

**YANGON UNIVERSITY OF ECONOMICS  
DEPARTMENT OF COMMERCE  
MASTER OF BANKING AND FINANCE PROGRAMME**

**OPERATIONAL RISK MANAGEMENT PRACTICES IN  
MYANMAR ORIENTAL BANK**

**PHYO THU HTWE  
(EMBF-6<sup>th</sup> BATCH)**

**DECEMBER, 2019**

**OPERATIONAL RISK MANAGEMENT PRACTICES IN  
MYANMAR ORIENTAL BANK**

A thesis submitted as a partial fulfillment towards the requirements for  
the degree of Master of Banking and Finance (MBF)

**Supervised by**

Prof. Dr. Daw Soe Thu  
Professor and Head  
Department of Commerce  
Yangon University of Economics

**Submitted by**

Phyo Thu Htwe  
Roll No. 42  
EMBF 6<sup>th</sup> Batch

**DECEMBER, 2019**

## ACCEPTANCE

Accepted by the Board of Examiners of the Department of Commerce,  
Yangon University of Economics, in partial fulfillment for the requirements of  
the Master Degree, Executive Master of Banking and Finance.

## BOARD OF EXAMINERS

-----  
Prof. Dr. Tin Win  
(Chairman)  
Rector  
Yangon University of Economics

-----  
(Supervisor)  
Prof. Dr. Daw Soe Thu  
Professor and Head  
Department of Commerce  
Yangon University of Economics

-----  
(Examiner)  
Daw Yee Yee Thein  
Associate Professor  
Department of Commerce  
Yangon University of Economics

-----  
(Examiner)  
Dr. Mya Thett Oo  
Associate Professor  
Department of Commerce  
Yangon University of Economics

-----  
(Examiner)  
Daw Htike Htike Lin  
Lecturer  
Department of Commerce  
Yangon University of Economics

December, 2019

## **ABSTRACT**

The objective of the study is to identify the internal operational risk management practices in MOB. Samples are collected from front line to middle managers, to analyze internal operational risk management and selected top management level for the fundamental risk management at MOB bank. Samples are 70 numbers who are collected from both front line to middle managers, to analyze internal operational risk management and, 20 numbers who are from top management level for the fundamental risk management at MOB bank by means of convenient random sampling method. In this study, survey found that the higher mean values are indicating that MOB has strong fundamental principles relating to operation risk cultures and framework, i.e., thus senior management has already identified well governance structures which will be used to manage operational risk at all level of bank organization, and thus, MOB Bank has found as strong fundamental principles of operational risk management culture behavior. It would also like to suggest the front line and middle management personal, to improve behavior in the staff to comply more with risk management policy because they have sometimes failed to comply with policy requirement of the bank. It would like to suggest to front line and middle management personal to record witnessed cases of design weakness in some its processes. So that, there would be lesson-learn to improve process risk management at MOB Bank. The study does not cover the whole MOB branches around the country. To understand more operational risk management practices in banking sector, further studies are needed to extend to other private commercial financial associations as well as to extend to public national banks in Myanmar.

## ACKNOWLEDGEMENTS

Upon completion of this paper, I would like to convey my heartiest Thanks to all of those who have contributed much and assisted me in various ways in all times-before, during and after the preparation of this paper.

First of all, I would like to express my sincere gratitude to Prof. Dr. Tin Win, Rector, Yangon University of Economics and Prof. Dr. Nilar Myint Htoo, Pro-rector, Yangon University of Economics for their concern and good academic guidance to the participants of the MBF Programme.

I would like to express my thankfulness to my supervisor Prof. Dr. Soe Thu, Head of Department of Commerce for her kind effort, good contribution and great encouragements to our program, master of banking and finance.

I would like to express my thankfulness to our respected Professors, Associate Professors, Lecturers and all the teachers from department of Commerce, who imparted their time and valuable knowledge during the course of my study at the Yangon University of Economics.

Furthermore, thanks to Senior Executive Management of Myanmar Oriental Bank and all the MOB team members who contributed to this paper, without their helping hands, this study would have not been completed in time.

Last, but not the least, I would like to say deepest thanks, all my family members, friends, and colleagues who give me the strength and encouragement to accomplish my academic goal. This study would not have been achieved without the encouragement, support and assistance of a number of people and organizations.

# TABLE OF CONTENTS

**ABSTRACT**

**ACKNOWLEDGEMENT**

**TABLE OF CONTENTS**

**LIST OF TABLES**

**LIST OF FIGURES**

<b>CHAPTER I</b>	<b>INTRODUCTION</b>	1
1.1	Rational of the Study	2
1.2	Objectives of the Study	4
1.3	Scope and Method of the Study	4
1.4	Organization of the Study	4
<b>CHAPTER II</b>	<b>THEORITICAL BACKGROUND</b>	5
2.1	Risk and Risk Management	5
2.2	Operational Risk Management Functions of the Bank	7
2.3	Operational Risk Management in Bank	9
2.4	Effectiveness of Internal Operational Risk Management Practices	11
2.5	Fundamental Principles of Operational Risk management	16
<b>CHAPTER III</b>	<b>OVERVIEW OF OPERATIONAL RISK MANAGEMENT IN MOB</b>	20
3.1	Background	20
3.2	Principle Business Activities of MOB	21
3.3	MOB Organization Structure	23
3.4	MOB Corporate Governance	25
<b>CHAPTER IV</b>	<b>ANALYSIS ON OPERATIONAL RISK MANAGEMENT OF MOB</b>	42
4.1	Survey Design	42
4.2	Internal Operation Risk Management (Process, People, Systems)	42

	4.3	Fundamental Principles of Operational Risk Management by Senior Management Level Respondents (Principle 1 & 2)	48
<b>CHAPTER</b>	<b>V</b>	<b>CONCLUSION</b>	<b>53</b>
	5.1	Findings and Discussions	53
	5.2	Recommendations and Suggestions	54
	5.3	Needs for Further Studies	55

**REFERENCES**

**APPENDICES**

## LIST OF TABLES

<b>Table No.</b>	<b>Particular</b>	<b>Page</b>
3.1	MOB Bank Branch Network	24
4.1	Demographic Profiles of Respondents	43
4.2	People Risk Management	45
4.3	Process Risk Management	46
4.4	Systems Risk Management	47
4.5	Three lines of defense Risk Management	48
4.6	Profiles of Management Level Respondents	49
4.7	Fundamental Principles of Operational Risk Management (P-1)	50
4.8	Operational risk management framework (P-2)	51

## LIST OF FIGURES

<b>Figure No.</b>	<b>Particular</b>	<b>Page</b>
2.1	Risk Management	7
2.2	Principles of Operational Risk Management	17
3.1	MOB Bank Organization Structure	24

# **CHAPTER I**

## **INTRODUCTION**

Risk ever exist and depend upon the uncertainties and the potential consequences. Operational risk management in banks has been increasingly emphasized in the past decade. Banks have continuously undergone changes in the business environment and this has been fostered by the increasing customer expectations, change in regulatory requirements, rise in technological innovation and stiff competition. As a result, this may lead to an increased chance of failure or errors from operations and result in increased operational risks.

Generally, significant risks in banking are credit risks, market risks, liquidity risks, operational risks, compliance risks, legal risks, financial crime risks, cyber risks and others. Operational risk is a kind of Non-Financial Risks in Banking. Most banks are taking cognizance of the qualitative and quantitative criteria for operational risk management advocated by the Basel Committee on banking supervision (2003). For international settlement, mechanisms have been developed to deal with risk problem through Basel II. According to Basel II (2004), operational risk is the risk resulting, from the inadequate or failed internal processes, people and systems or from external events.

The term operational risk became widely known in mid 1990s after the creation of proposals such as the Basel II in June 1999 and this was in perspective to rising scandals in the financial sector such as Nicholas Leeson, unscrupulous destruction of Barings bank in 1995 (Khan, 2008). The impact of operational risk on an organization is illustrated in the form of direct financial loss, earning volatility, financial distress, and non-financial effects on the future earnings capacity of the organization. Basel II want to address this issue through requiring banks to adopt mechanisms or standards. Basel II required banks to hold capital to deal with operational risk. Operational risk is inherent to all products, activities, process and systems and is generated in all business and support areas. For this reason, all employees are responsible for managing and controlling the operational risks generated in their sphere of action. Operational risk management process is subject to common procedure and strategies to risk management process such as identification,

assessment/measurement, monitoring/control, reporting/communication and decision making (IFC FIG RISK ADVISORY- Operational Risk 2018).

The Central Bank of Myanmar (CBM) expects all banks to develop effective frameworks and practices to manage their money Laundering/ terrorist financing risks(ML/TF). The effective management of risks is a requirement of the Basel Core Principles (BCP) for Effective Banking Supervision and the Financial Action Task Force (FATF) 40 Recommendations. Thus, CBM issued the guidance related to Bank required to establish operational Risk management framework and practices to effectively mitigate such risks. The CBM expects banks to establish effective systems for the on-going monitoring of their risk exposures and effectiveness of associated risk management systems and practices.

Most of Myanmar Banks are implementing Core Banking System and provide financial services on line and digital platform. Among private banks in Myanmar, Myanmar Oriental Bank Limited (MOB) is establishing effective risk management. MOB was established in November 18, 1993 and it expanded 46 branches across Myanmar. MOB was long term partnership with International Finance Corporation (IFC) since 2014 and providing advisory service project. MOB successfully implemented Core Banking System in 2018 for all MOB network bank branches.

Myanmar Oriental Bank's business activities involve the use of financial instruments. These activities expose the Bank to a variety of financial risks including operational risk. MOB, one of private banks in Myanmar, is carrying out transformation stage to digital bank and therefore it needs to have sound operational risk management. Thus, this study explores operational risk practices in Myanmar Oriental Bank.

## **1.1 Rationale of the Study**

The operational risk is complex in nature compared to other risks such as credit and market risk. Since financial sector plays a vital role in a country's economy, it is important for financial institutions and banks to monitor the risks associated with their products and services. In fact, traditional risk management practices have normally focused on protection of the tangible assets reported on company's financial matters. Thus, managing risk is at the core of managing any financial organization.

These day risk management has become the most useful tool to be used especially in banks in order to get assurance concerning the reliability of the

operations, and procedures to being followed. Banks in financial sector are taking part in the major role for economic development and stability of country.

In Myanmar, the banking sector has already undergone tremendous changes. According to the financial Institutions of Myanmar Law (1990), the Central Bank of Myanmar allows license financial institutions, Currently, there are four specialized state own banks and 27 privately owned banks. Moreover, 13 foreign own banks, 244 microfinance and 12 insurance companies are licensed. These financial institutions provide various bank products and services compatibly and the common types of risks can be faced with private banks.

The Central Bank of Myanmar (CBM) behave as a regulatory body by issuing guidance and directives. Therefore, banks need to proceed and implement to improve the banking and financial sector stability. CBM issued AML/CFT Risk Based Management Guidance Note on January 27, 2015.

The Risk Management Process consists of identification, measuring, controlling, monitoring and mitigating. according to the guidance of the Central Bank of Myanmar, banks shall establish the Risk Management Framework that encompasses with Corporate Governance, the Risk Management Functions, Policies and Procedures, Internal controls, the Compliance Function, Risk Monitoring and Reporting and Training.

In January 2019, the Central Bank of Myanmar issued directive that allows foreign banks and financial institution to be able to invest up to 35% in the equity of local banks. Assessment on Operational Risk Management framework is one of the crucial criteria of check list for foreign investor.

Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management program.

In June 2011 the Basel Committee on Banking Supervision published its "Principles for the Sound Management of Operational Risk" ("The Principles") to provide guidance to banks on the management of operational risk. The eleven principles incorporate the lessons from the financial crisis and the evolution of sound practice for management of operational risk.

Myanmar Oriental Bank (MOB) is a private limited bank and started its operations on 18th November 1993. It has now banking network of 46 branches across the country. MOB has signed a partnership agreement with Western Union

through which customers can transfer funds using its affiliated network in 111 countries from/to the bank. Due to MOB's market reputation for transparency and reliability, the bank continues to receive direct technical support from foreign financial institutions. The International Finance Corporation (a member of the World Bank Group) has helped MOB enhance its corporate governance, risk management, credit assessment, asset and liability management, trade finance and IT management. This study intends to find out the Sound Management of Operational Risk Practices in Myanmar Oriental Bank.

## **1.2 Objectives of the Study**

The objectives of the study are:

1. To identify the operational risk practices in Myanmar Oriental Bank
2. To analyze the internal operational risk management practices and compliance of the fundamental principles of operational risk management in Myanmar Oriental Bank.

## **1.3 Scope and Method of the Study**

This study only focus on operational risk practices in Myanmar Oriental Bank. The descriptive statistics methods is used to analyze the operational risk practices in Myanmar Oriental Bank. Primary data collected from 70 respondents, 20 senior management level and 70 middle management level of Myanmar Oriental Bank. The study will be done at MOB Head Office and Yangon branches. The primary data are collected with structured questionnaires and the secondary data are obtained from relevant departments, audited annual reports, research papers, relevant microfinance text book, MOB official website and CBM instructions.

## **1.4 Organization of the Study**

This thesis consists of five chapters. Chapter I is the introduction of the study and it also includes the rational of study, objective of the study, scope and method of the study, and organization of the paper. Chapter II discusses theoretical background and chapter III details Profile of Myanmar Oriental Bank. Chapter IV includes analysis of Operational Risk Practices in Myanmar Oriental Bank. Chapter V concludes the study with conclusions and recommendations.

## **CHAPTER II**

### **THEORETICAL BACKGROUND**

This chapter summarizes the formation from the available literature on operational risk management in performance of financial institutions. This chapter focus on the relationship between operational risk management against business disruption and system failures, employment practice and workspace safety, and financial performance. This chapter is formed of five portions, such as defining risk and risk management in financial sector, including the eight types of risk and critical success factors of risk management in financial sector. After this part explained the operational risk management in Banks and then the fundamental principles of sound operational risk management in banks are explained.

#### **2.1 Risk and Risk Management**

The risks to which a bank is particularly exposed in its operations are: liquidity risk, credit risk, market risks (interest rate risk, foreign exchange risk and risk from change in market price of securities, financial derivatives and commodities), exposure risks, investment risks, risks relating to the country of origin of the entity to which a bank is exposed, operational risk, legal risk, reputational risk and strategic risk.

There are eight types of risk in financial sector: (1) Credit risk, (2) Market risk, (3) Operational risk, (4) Liquidity risk, (5) Business risk, (6) Reputation risk, (7) System risk and (8) Moral hazard risk.

**Credit risk** is the risk of negative effects on the financial result and capital of the bank caused by borrower's default on its obligations to the bank.

**Market risk** includes interest rate and foreign exchange risk.

**Interest rate risk** is the risk of negative effects on the financial result and capital of the bank caused by changes in interest rates.

**Foreign exchange risk** is the risk of negative effects on the financial result and capital of the bank caused by changes in exchange rates.

**Operational risk** is the risk of negative effects on the financial result and capital of the bank caused by omissions in the work of employees, inadequate internal

procedures and processes, inadequate management of information and other systems, and unforeseeable external events.

**Liquidity risk** is the risk of negative effects on the financial result and capital of the bank caused by the bank's inability to meet all its due obligations.

**Business risk** is the risk associated with the failure of a bank's long term strategy, estimated forecasts of revenue and number of other things related to profitability. To be avoided, business risk demands flexibility and adaptability to market conditions. Long term strategies are good for banks but they should be subject to change. The entire banking industry is unpredictable. Long term strategies must have backup plans to avoid business risks.

**Reputational risk** is the risk of loss caused by a negative impact on the market positioning of the bank.

**System risk** is the risk that doesn't affect a single bank or financial institution but it affects the whole industry. Systemic risks are associated with cascading failures where the failure of a big entity can cause the failure of all the others in the industry.

**Moral hazard risk** is a risk that occurs when a big bank or large financial institution takes risks, knowing that someone else will have to face the burden of those risks.

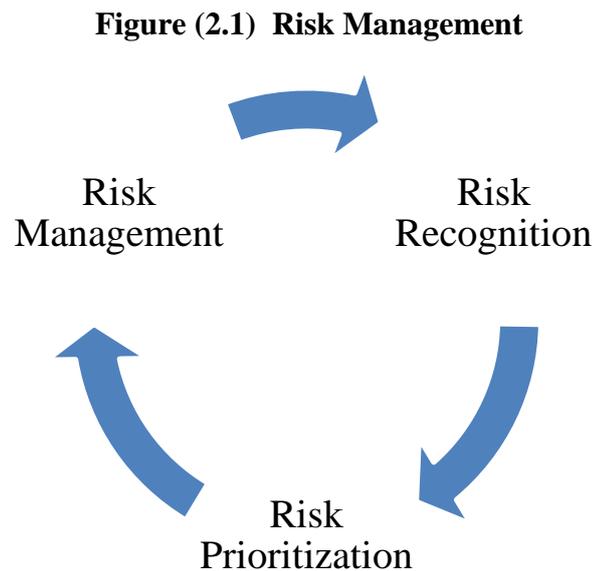
Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters.

**Risk management** is a process aslo a task which can be resemble or transmit with other management functions and also faces difficulties in allocating resources. Resources spent on risk management could have been spent on more profitable activities. An ideal operational risk management can proactively help in overcoming the possibilities which can cause any type of business failures because it is an integral part of the decision-making process. The approach used to managing operational risk differs from that approach which applied to other types of risk, because it is not used to generate profit.

**Risk management** involves four stages: risk identification, measurement, monitoring, and management. Operational risk and control assessments are often the first process that a firm uses to carry out operational risk management. Frequently the assessment is carried out without an operational risk management framework in place

and without much thought being given to high-quality corporate governance around the multiple interlocking processes of operational risk management. Operational risk management provides us with a set of tools that will allow us to attain even greater and more consistent results by using a systemic method to approach issues rather than relying on experience. Risks have to be assessed against benefit, the purpose of ORM is to loosen risk and thus improve the ratio of benefit to cost.

Whenever any risk arises first it recognizes, then it is prioritized according to the importance then it is managed, as shown in the following diagram.



Risk management must be integrated part of planning and executing any operation, routinely applied by management, not a way of reacting when some unforeseen problem occurs. Managers are responsible for the routine use of risk management at every level of activity, preliminary with the planning

## **2.2 Operational Risk Management Function of the Bank**

The Basel Committee on Banking Supervision defines operational risk as: “ The risk of loss resulting from inadequate or failed internal processes, people and systems or external events.” Sound operational risk management practices cover governance, the risk management environment, and the role of disclosure. Operational risk management must be fully integrated into the overall risk management processes of the bank.

The three common “lines of defense” model employed by firms to control operational risks are:

1. Business line management is the first line of defense. Banks now, more than ever, have multiple lines of business, all with varying degrees of operational risk. Risks must be identified and managed within the various products, activities and processes of the bank.
2. An independent operational risk management function.
3. Independent reviews of operational risks and risk management.

The review may be conducted internally with personnel independent of the process under review or externally.

### **2.2.1 Corporate Operational Risk Function (CORF)**

The bank’s specific business lines monitor, measure, report, and manage operational and other risks. The corporate operational risk function (CORF), also known as the cooperate operational risk management function, is a functionally independent group that complements the business line’ risk management operations.

The CORF is responsible for designing, implementing, and maintaining the bank’s operational risk framework. Responsibilities of the CORF may include:

- Measurement of operational risks.
- Establishing reporting processes for operational risks.
- Establishing risk committees to measure and monitor operational risks.
- Reporting operational risk issues to the board of directors.

Larger, more complex banking institutions will typically have a more formalized approach to the implementation of the lines of defense against operational risks, including the implementation of the CORF.

### **2.2.2 Benefits of Operational Risk Management**

The benefits which can be got from operational risk management are:

1. Reduction of operational loss.
2. Lower compliance/ auditing costs.
3. Early detection of unlawful activities.
4. Reduced exposure to future risks.

### **2.3 Operational Risk Management in Banks**

The bank must determine its risk bearing capacity and tailor its risk profile being aware of it. The risk management got an important role in the bank organization and ways business conduct. There are strong relations between risk management, the business strategy, corporate governance and internal control system.

It is important to state that each bank's operational risk profile is unique and requires a tailored risk management approach appropriate for the scale and materiality of the risks, and the size of the organization. Risk must be well managed and for the banking institutions this task has become much more difficult and complex being proved the changing nature of risk in banking industry and its new implications for bankers and bank supervisors.

Operational risk is determined by a multitude of factors as for example the complexity of the bank structure, the geographical dispersion of its activities and units, the complexity, range of products and services, number of staff and its professional skills, experience and training and risk management culture as it develops its operational risk management. The complexity of the activity and its geographical extend are extremely important.

In the same time, the number of the employees and their professionalism is determinant being proved by the statistics that an important number of operational loss events were determined by human error caused by the lack of competence, experience, overload or insufficient training? Corporate culture is decisive in the fight with risks, operational risk inclusively. Senior management is responsible to ensure the corporate culture development on continuous bases and imbedding the risk awareness in the bank's culture. Of all the different types of risk that can affect firms, Operational Risk can be among the most devastating and the most difficult to anticipate.

Management of operating risks is a key component of our financial and risk management discipline that drives net income results, capital management and customer satisfaction. Rigorously controlled and well-managed risk frees up resources and capital for revenue generating opportunities. Operational risk is determined by a multitude of factors as for example the complexity of the bank structure, the geographical dispersion of its activities and units, the complexity, range of products and services, number of staff and its professional skills, experience and training and risk management culture as it develops its operational risk management.

As long as this awareness related to risks is not ensured, the risk control and management will not attend the desired consistence. An effective operational risk management system should identify both the internal and external factors that could influence the accomplishment of its bank's objectives either positively or negatively. Internal risks arise from the bank's structure, the nature of the bank's activities, the quality of the bank's human resources and organizational changes while external risk result from changes in industry and technological progress.

From the Bank's perspective, operational risk is classified as the risk of loss resulting due to inadequate or failed internal processes, people and systems or external events. The frequent appearance of financial scandals in the financial industry has increased attention on operational risk. While the risk of fraud and external events has been in existence since the beginning of banking, the chance that operational risk might arise has increased due to recent technological advances.

Hiwarashi (2002) mentioned that operational risk has increased its importance and is being looked at by various banks due to deregulation, improvements in technology and increased international competition. Similarly the increase in the number of mergers and acquisition has expanded operational risk in banks. According to Hiwatashi, banks strive to measure operational risk for a number of reasons.

1. A bank is better able to develop objective measures in order to examine the adequacy of internal risk control processes.
2. The increase in the viability of the methods used to calculate operational risk

has induced banks to allocate economic capital to operational risk.

Robert J. Chapman, (2011), supported Hiwarashi's finding that due to the increased complexity in bank's operations, the need for effective risk management has also increased. Robert J. Chapman (2011) identified as the operational risk management affords a business benefits by: Improving the ability to achieve its business objectives , Providing management opportunity to focus on revenue generating activities rather than fire -fighting one crisis after another, Minimizing day-to-day-losses, Providing more robust enterprise risk management system, Contributing to the establishment of a system which enables the correlation of different classes of risk to be understood and, where appropriate, modelled. Those at the very top of the organization have to focus on operational risks and their management. The board of directors and senior management must establish, and then

periodically review, an operational risk framework for the firm. That framework should make clear the range of risks to be covered by the program and outline how they are to be identified, assessed, monitored and controlled across the various lines of business within the firm.

## **2.4 Effectiveness of Internal Operational Risk Management Practices**

The top management is answerable for all the risks of the bank; planning and implementing its risk strategy. One amongst the foremost vital prerequisites for establishing an efficient operational risk management system is the support of the top management right from the beginning (Mikes, 2009). The management should therefore assign necessary budget funds and human resources to operational risk management as their support has a substantial influence on the risk management and control surroundings (Kioko, 2014).

In larger banks, risk committee that specializes in the management of the bank's risks, and internal control system is set up for the role of observation of the risk, state of affairs and approaches taken for comprehensive risk identification, and maintenance of an efficient internal control system. Such a centralized risk-controlling unit has the authority to lay down pointers and strategies of risk management (Bank for International Settlement, 2011).

The forms of internal operational risks involve issues of human error in processing, fraud, missing a control step, disruption or system failures (software, hardware, telecommunications), act of sabotage or vandalism, noncompliance with law and regulatory requirements, external dispute with employee as a result of discrimination or harassment, new service or change in the current processes (Weber, 2014).

### **2.4.1 People Risk**

All human actions have the risk of error, the more complex an activity is the higher the risk. As a result, the danger of harm because of mistakes is extremely varied. The spectrum includes cases like incorrect processing due to inadequate skills, clerical mistakes, and wrong inputs in IT systems, omissions, or errors owing to work-related or personal stress, etc. In distinction to criminal acts, these mistakes do not involve any intent to create personal gain or cause injury to the organization or third parties (Cornalba & Giudici, 2004).

Employees need the necessary skills to perform their work effectively and these skills are a critical for individuals, businesses, and societies. The benefits of skills are more pronounced in this changing, globalized nation (Certo, 2015). Building the necessary skills early in childhood stages, is important however, it very important to make sure that skills taught are the relevant ones for the working world and used by employers and employees in the labour market (Armstrong & Taylor, 2014).

According to Klosters (2014), it is necessary to ensure that necessary skills are matched to the jobs although skills mismatches take place when staffs either have less or more skills than required by the jobs require. He further adds that such high and persistent mismatch may turn to be costly for the organization and the industry at large. Armstrong and Taylor, (2014), explain that many of these shortages can be addressed by altering the current training and recruitment practices, while promoting labour mobility. According to Institute of Bankers Malaysia (2014), study done in Malaysia to investigate talent and skills requirements for the banking sector revealed that a (62%) of respondents agree that the tightening of risk management skills influences banks in many ways. Institute of Bankers Malaysia (2014), further highlight that talent needed in investment banks requires employees to have the ability to interpret various risks, while organizing products and steering daily operations.

The rise of globalization and technology has been blamed for the increased rate of fraud related activities. These fraud activities have however been very difficult to detect due to advanced technology (Zagaris, 2010). In such conditions, the banking industry are forced to put up significant amount of resources to recognize and fight fraud (Kranacher, Riley, Wells, 2011). The other challenge has been political meddling in the bank's operations, inadequate laws for prosecution of fraudsters, and frail institutional structures in the courts and police force (Akelola, 2015).

Within any organization there is a need for existence of involvements, and connections between people. This fosters leader/follower relationship through interaction and connectivity within a firm (Banks, 2008). Managers in firms have power which enables individuals and groups to achieve objectives and satisfy needs. A manager's power gives him/her the right to sway and issue orders to the follower's. Power becomes abusive to subordinates when it results in violation to their dignity or result in a dysfunctional performance (Irungu, 2011). A workplace may be inhabitable if performance weakness cases are rewarded over merit-based output; employees avoid confrontations with senior management for fear of payback; personal plans take

superiority over the firms well-being; new managers and employee turnover is very common; and employees are not treated like company assets, and superiors routinely cause disruption of business, by making unreasonable demands. In such environments, staffs are always overloaded with work, and unlikely to maintain work-life balance due to the tight deadlines and superiors' demands (Colligan & Higgins, 2006).

Despite the mentioned challenges, the increasing globalization calls for more interaction among individuals from varied backgrounds. Employees are now a portion of a universal economy and have to compete effectively within a global context. For this reason, firms should adopt diversity to remain competitive although at the same time, managing diversity possesses a significant challenge that managers must adapt skills to accommodate in the work environs (Kelli, Mayra, & Allen, 2016).

#### **2.4.2 IT System Risk**

In an advanced commercial society, a corporation's operations are relatively structured on the integrity of its IT structures, and success relies heavily upon its capability to use increasingly more rich databases, and make well timed decisions connected to industry modifications. An economic organization's overall performance is negatively impacted if it experiences device interruptions, errors, or even if it lags behind competition regarding the information system used (Comalba & Giudici, 2004). Every company needs to be devoted to upgrading, improving, and checking out its systems, to meet the sophisticated user wants, market requirement, regulatory adjustments, and internal needs for records management (Khan, 2008). Barakat (2014) explains that records generation risks consist of the failure to respond to the correct data, as well as many different issues they are: human blunders, internal fraud through software manipulation, outside fraud with the aid of intruders, obsolesce in programs and machines, reliability issues, mismanagement, and effect of natural failures.

Natural failures of technological systems are realistic, however it takes long to do it, and perhaps the maximum essential component is that a robust group is needed, during the implementation of (IT) policies. Once a minor issue of operation becomes a threat, it is necessary for the corporations to become aware, and control it to minimize risks related to security breach, availability, and overall performance and compliance factors (Lopez, 2002). Information technology risk has a capacity to harm

an organization's reputation, ensuing from insufficient adaptation to procedures, bad configuration, sabotage of information or structures, malicious software, updating antivirus and antispyware packages, access to confidential statistics, and unauthorized entry by unauthorized employees (Lopez, 2002). Identification, analysis, measuring and control of IT risk requires specialized know-how and skill. IT risk management has to be executed in every division, and each corporation has its personal unique IT management process. (IT) risks need to be labeled consistent with their impact as either security risk, availability risk, performance risk or compliance risk (Bebbington, Larrinaga, & Moneva, 2008).

In security risk, the data can be altered, accessed, or used by unauthorized events. Such security risk can be in form of: external attacks, malicious code, bodily destruction, unhappy workers, type of platform and messaging types. The effects related to them include corruption of information, outside fraud, identification theft, robbery of financial assets, and damage to reputation and harm to assets (Bank for International Settlements, 2008). An availability risk on the other hand involves those risks that result into records or packages being inaccessible due to device failure or natural catastrophe, together with any repair time. Causes of such risks include hardware crash, network outages, data Centre failures, pressure majeure. Capability influences related with them are: abandoned transactions and lost income, reduced customer, reduced worker confidence, interruption or delay of commercial enterprise essential procedures, reduced IT staff productivity (Cornalba & Giudici, 2004).

Performance risk results into overall under performance of systems, applications, or employees and sources of this risk include negative machine architectures, network crowding, ineffectual code, insufficient capability. Potential effects associated with them are; reduced client pleasure and loyalty, interruption or delay of business dire process, lost IT efficiency (Bek, 2014). Compliance risk are those that involve failing of data processing to meet regulatory, IT or enterprise policy requirements. Commonly, it entails fines, penalty, or loss of recognition from failure to conform to legal guidelines or rules, or effects of non-compliance with the guidelines.

Resources of compliance risk are: rules precise to every jurisdiction, legal actions, and inner IT safeguards supporting compliance. Possible effects related to them are: harm to reputation, breach of customer confidentiality, legal action (Bank For International Settlement, 2011).

### **2.4.3 Process Risk**

Bank's operations are reinforced through variety of systems and processes, like IT systems, human resource, market, credit, and insurance and liquidity risk management systems. These systems may possess different mechanisms, and each requires the process of various apparatus. Multifaceted or ill designed systems and processes can lead to operational losses, due to their improper fit or malfunction, this result into problems during settlement, fraud and information security failures and processing errors. In addition, the increased automation also has the prospect of transforming risks from manual processing errors to systematic failures which may be drastic (Bank for International Settlements, 2008).

When addressing operational dangers on account of business processes, the first step is to distinguish if the danger is due to the organization system failure or human errors. Accordingly, the subsequent instances can be diagnosed. Methods with a faulty normal design involve a notable capacity of operational dangers these instances are typically discovered in regions where in techniques are historically grown without a corresponding development of procedural enterprise (Advisen Insurance Intelligence, 2014). Business Process management (BPM) is a disciplined method to discover, design, execute, file, degree, display, and control both automatic and non-automated commercial enterprise procedures to attain regular, targeted effects aligned with an employer's strategic desires. BPM enables an organization to align its business processes to its enterprise method, main to powerful typical company performance thru upgrades of unique work activities both within a specific department, throughout the organization, or among groups (Bank For International Settlement, 2011).

People are continually core to any agency, and it's the company's human capital that facilitates to make sure strategies function efficiently and effectively irrespective of how a good deal they may be computerized. That's why "human capital" is the primary and most important pillar in the middle of Excellence. Unluckily, many firms make the error of hiring those who lack an appropriate understanding, or they move people around internally with the hope that they will learn the discipline on the fly (Bek, 2014). According to Getter (2014), governance, specifically is a key element of procedure management and is of the very best importance to get actual cost out of reference models, BPM governance includes defining roles and responsibilities for method stakeholders, policies for accessing and

modifying reference models and their organization-specific versions and hints for the adoption of recent or additional reference models. Furthermore, powerful governance can provide businesses with centralized coordination, preservation, and management of their BPM competencies, even when the execution of system management is scattered throughout the company. A robust governance technique will ensure the consistency of reference fashions, even though decentralized organizational units alter them primarily based on unique desires (Bek, 2014).

## **2.5 Developing Effective Operational Risk Management**

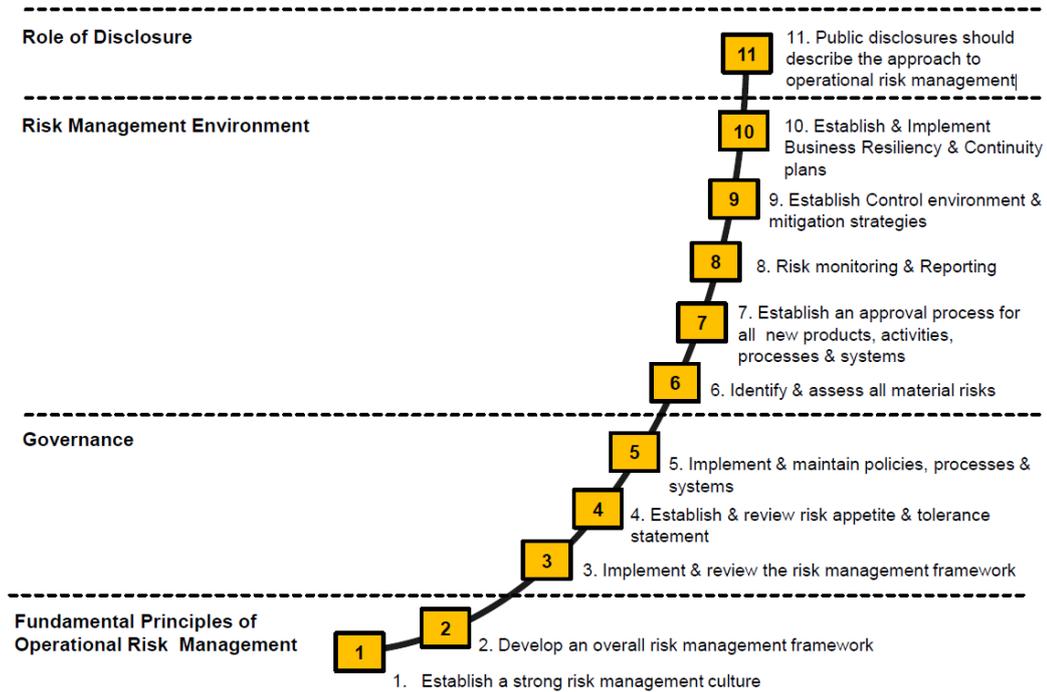
In developing sound practices for effective Operational Risk Management Framework, operational risk to mean the identification, assessment, monitoring and control/ mitigation” of risk. The Basel Committee has suggested eleven principles for effective Operational Risk Management Framework. (Basel 2011)

### **2.5.1 Eleven Principles of Operational Risk Management**

1. The maintenance of a strong risk management culture led by the bank’s board of directors and senior managers.
2. The operational risk framework must be developed and fully integrated into the overall risk management processes of the bank.
3. The board should approve the periodically review the framework.
4. The board must identify the types and levels of operational risks the bank is willing to assume as well as approve risk appetite and risk tolerance statements.
5. Consistent with the bank’s risk appetite and risk tolerance, senior management must develop a well-defined governance structure within the bank.
6. Senior management must understand the risks, and the incentives related to those risks, inherent in the bank’s business lines and processes.
7. New lines of business, products, processes, and systems should require an approval process that assesses the potential operational risks.
8. A process for monitoring operational risks and material exposures to losses should be put in place by senior management and supported by senior management, the board of directors and business line employees.
9. Banks must put strong internal controls, risk mitigation, and risk transfer strategies in place to manage operational risks.

10. Banks must have plans in place to survive in the event of a major business disruption. Business operations must be resilient.
11. Banks should make disclosures that are clear enough that outside stakeholders can assess the bank's approach to operational risk management.

**Figure (2.2) Principles of Operational Risk Management**



Source: IFC, Advisory Services, Senior Management Awareness Workshop

### 2.5.2 Fundamental Principles of Operational Risk Management

This study focus on two fundamental principles of operational risk management practiced by MOB. Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behavior. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organization.

- Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with this events that do occur. The actions

of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.

- The board should establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behavior convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes. Compensation policies should be aligned to the bank's statement of risk appetite and tolerance long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.
- Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organization. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

The fundamental premise of sound risk management is that the board of directors and bank management understand the nature and complexity of the risks inherent in the portfolio of the bank products, services and activities. This is particularly important for operational risk, given that operational risk is inherent in all business products, activities, processes and systems.

A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organization including those at the group and business line levels, as well as into new business initiatives products, activities, processes and systems. In addition, results of the

bank's operational risk assessment should be incorporated into the overall bank business strategy development processes.

The Framework should be comprehensively and appropriately documented in board of directors approved policies and should include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their Framework.

Framework documentation should clearly:

- Identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
- Describe the risk assessment tools and how they are used;
- Describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;
- Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;
- Establish risk reporting and Management Information Systems (MIS);
- Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;
- Provide for appropriate independent review and assessment of operational risk; and
- Require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

## **CHAPTER III**

### **OVERVIEW OF OPERATIONAL RISK MANAGEMENT IN MYANMAR ORIENTAL BANK**

#### **3.1 Background**

Myanmar Oriental Bank Limited was incorporated as a private limited bank under the Financial Institutions of Myanmar Law and started its operations on 18<sup>th</sup> November 1993. Its founding members were prominent bankers retired from state-owned banks, family members holding the majority of shares, their close friends and relatives from the business circle.

Over the past 26 years, the bank has played an important role with stability and success of domestic banking in Myanmar by contributing its efficient and reliable banking services and promoting financial intermediation in the country. The bank accepts foreign currencies (USD, EUR, SGD, THB) as current accounts and Myanmar Kyat as current, call, savings and fixed deposits within its present banking network of 47 branches across the country. In addition, the bank also provides banking facilities and other financial assistance to its customers in the form of commercial loans, trustee and remittance services.

Upon approval from the Central Bank of Myanmar, the bank was among the first few selected financial institutions that were allowed to deal in foreign currencies and international banking. It was among the first batch of six private banks to be permitted to open currency exchange counters in the country. The bank has now opened 20 currency exchange counters in the commercial cities has introduced ATM and POS debit card and credit card facilities for the promotion of electronic payment systems in the country. The bank has developed an overseas network by establishing corresponding banking relationships with 60 banks worldwide. The bank has also signed a partnership agreement with Western Union through which customers could transfer funds using its affiliated network in over a hundred countries from/to the bank.

Apart from its core banking business, MOB established the Oriental Leasing Company Limited (OLCL), as a subsidiary, extending financial assistance to its customers in acquiring their household and other durable consumer items. The bank owns 99% of the company's share capital.

In foreseeing the future needs, the bank inked a Memorandum of Understanding with IFC on joining their Global Trade Finance Program (GTFP) which has provided MOB with a USD 5 million trade finance facility and allows the bank to establish working partnerships with a vast number of major international banks through the GTFP bank network. Additionally, under the framework agreement, IFC is helping the bank to strengthen its corporate governance and improve its trade finance operations. IFC disbursed MMK 8.98 billion, equivalent of USD 7 million, to MOB as a convertible loan.

### 3.1.1 MOB Bank Branch Network

There are six regional zones, 47 branches across the Myanmar.

**Table (3.1) MOB Branch Network**

<b>Zone</b>	<b>Number of Branch</b>
Zone 1 (Yangon)	15
Zone 2 (Mandalay)	5
Zone 3 (Monywar)	6
Zone 4 (Pyay)	9
Zone 5 (Pathein)	7
Zone 6 (Mawlamyaing)	5
Total	47

Source : MOB Annual Report (2018-2019)

### 3.2 Principal Business Activities

**Deposit taking in the forms of current, fixed, saving deposit and call deposit** – The bank offers an interest rate of 8.25% p.a. on saving deposit, 8.50% p.a. on 1-month, 9.25% p.a. on 3-months, 9.5% p.a. on 6-months, 9.75% p.a. on 9-months and 10% p.a. on 12-months fixed deposit and 2% p.a. on call deposit daily balance. The bank does not allow any interest on current deposits. By the end of FY 2018/2019, the amount of deposit reached MMK 553.38 billion, achieving an increase of 24.44% from previous year.

**University Education Saving Scheme (UESS)** – UESS was introduced on 2nd May, 2002 to promote saving habits among the people in Myanmar. The goal of

the product is to support advance planning on the tertiary education for a child currently under the age of 12. A parent or guardian, who wants his or her child to benefit from this scheme, can open a saving account with the bank and regularly save in multiples of MMK 5,000 per month -the minimum amount to be saved monthly must not be less than MMK 5,000. By joining the scheme, customers will receive an additional 3% interest contribution on the account's yearly balances. The customer can pay annual school fees out of his/her account by producing documents certifying his/her admission to a college or university.

**Extension of commercial loan to business borrowers** – The bank's credit committee is composed of CM and members of senior management. The committee strictly observes its prudential loan policy by reviewing the prospective borrower's credibility, business performance and collateral before it grants its approval. Currently the bank is extending commercial loans for a term of not more than one year. The loans are disbursed mainly for the borrower's working capital. Interest on loans charged by the bank is based on the Central Bank's interest rate policy and current rate is set at 12% p.a. and 1% service charges on loan. The bank's total outstanding loans and advances amounted to MMK 439.57 billion, equivalent to 79.43% of total deposits, at the end of September 2019. There has been an increase of 33.13% over last year. Most of the current account holders and loan customers are business entities and private entrepreneurs, the rest are household individuals.

**Trustee, telephone and electricity bill payment services-** The trustee service which started its operation on 1st February, 2001, and has experienced significant growth since its introduction. It has become one of the bank's major sources for generating income, providing considerable funds to OLCL. In FY 2018/2019, the number of trust deeds was increased from 277 to 369 and the amount growing from MMK 7.85 billion to MMK 12.37 billion.

**Bill payment services** were launched on 2nd October, 2001. The bank is collecting service charges 300 MMK on electricity and 500 MMK on phone bill at per settlement. All these bills are paid by the bank on behalf of its customers out of their designated current account.

**Domestic remittance services** – MOB uses its network of 47 branches across the country and collaboration with other 11 domestic private banks (Co-operatives Bank, Myawaddy Bank, Global Treasure Bank, Myanmar Citizen Bank, Ayeyarwaddy Bank, Rural Development Bank, Innwa Bank, Myanmar Microfinance

Bank, Shwe Bank, Small & Medium Enterprise Development Bank and Mineral Development Bank) to provide remittance services. MOB also provides Customer Credit Transfer (CCT) service in collaboration with other domestic banks and online tax payment through CBM NET.

**International money transfer services** – In partnership with Western Union, an internationally renowned money transfer company, MOB is the first financial institution in Myanmar to deliver inbound & outbound money transfer services.

**ATM and POS debit card & credit card facilities** – As a leading member of the Myanmar Payment Union, MOB has been issuing debit and credit cards to its customers and installing POS terminals at various merchants like shopping centers, restaurants, hotels, airlines etc. The bank is also setting up ATMs at various public places to be more accessible for customers. MOB notably received the Member Service and Trademark License Agreement from Union Payment International (UPI).

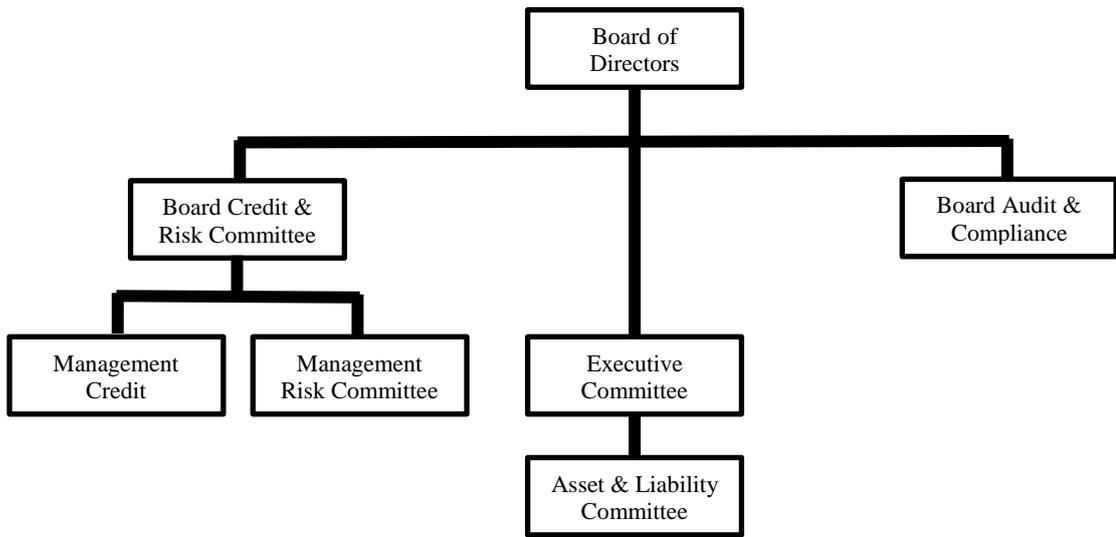
**International banking services** – MOB was one of the few privileged banks granted with Authorized Dealer License for international banking services from the Central Bank of Myanmar on 25th November 2011. Taking this opportunity, the bank had installed SWIFT communication system and started setting up international network of correspondent banks for its operations. Supported by international organizations and reputed global financial institutions, the bank has been able to expand its foreign banking services with higher standard of practice for overseas remittances, trade financing and treasury operations.

### **3.3 MOB Bank Organization Structure**

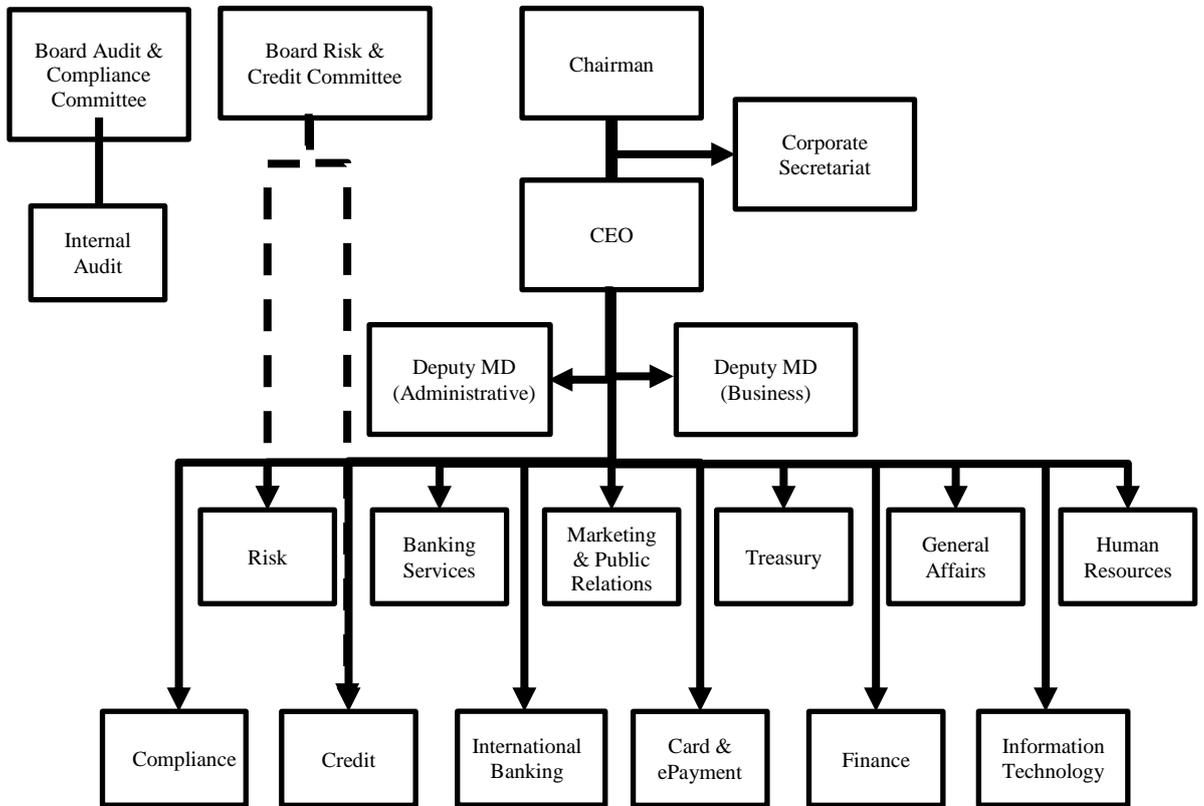
The organization structure of MOB is shown in figure (3.1). It can be seen into two parts: (a) Governance Committee and (b) Management organization.

**Figure (3.1) MOB Management Board**

**(a) Governance Committees**



**(b) Management Organization**



Source: [www.mobmyanmar.com](http://www.mobmyanmar.com)

### 3.3.1 Departments of MOB bank

Myanmar Oriental Bank Head Office was formed 15 departments

1. Banking Services Department
2. Credit Department
3. Card & e-payment Department
4. International Banking Department
5. Internal Audit Department
6. Compliance Department
7. Finance Department
8. Treasury Department
9. Information Technology Department
10. Human Resources Department
11. General Affairs Department
12. Marketing & Public Relations
13. Relationship Management Department
14. Corporate Secretariat
15. Risk Management Department

### 3.4 MOB Corporate Governance

The purpose of Myanmar Oriental Bank's Corporate Governance Policies (or Manual) is to summarize MOB's (the Company) key corporate governance policies and provisions. MOB defines corporate governance the structures and processes that provide strategic direction and oversight control of the company. It includes the relationships between the Bank's shareholder, Board of Director and executive bodies. MOB's corporate governance framework is broadly based on the OECD principles of;

- **Accountability:** These Policies establish MOB's accountability to all shareholders and guides the Bank's Board in setting strategy, and guiding and monitoring the Bank's management.
- **Fairness :** MOB obligates itself to protect shareholder rights and ensure the equitable treatment of all shareholders, including minority shareholders. All shareholders are to be granted effective redress for violation of their rights through the Board.

- **Transparency** : MOB will ensure that timely and accurate disclosure is made on all material matters regarding the corporation including the financial situation, performance share ownership and governance of the company in a manner easily accessible to interested parties.
- **Responsibility** : MOB recognizes the rights of other stakeholders as established by law and regulations and encourages co-operation between the company and stakeholders in creating in creating sustainable and financially sound enterprises.

**These Policies have been developed in adherence with:**

- (1) The Financial Institutions Law (No.20/2016)
- (2) The Myanmar's Companies Law (No.29/2017)
- (3) Articles of Association of MOB

The MOB Board of Directors will ensure these Policies are adhered to throughout the organization further the Board will review and update these Policies as needed. Any changes to these Policies must be approved by the Board of Directors. By adopting these Policies, MOB confirms its ongoing commitment to good corporate governance.

**3.4.1 Board Roles and Director Policies**

The board is elected by and is accountable to the MOB shareholders. Except for decisions explicitly reserved for shareholders, the board has full authority to carry out all activities necessary to provide effective strategic guidance and sound oversight of the company. Its ultimate goal is to create long-term shareholder value, while taking into account the interest of its stakeholders. Following are the primary roles and responsibilities of the Board:

- Reviewing approving and monitoring the Bank's long-term strategic objectives and business plans of management, including any performance indicators and targets to be used in relation to the strategy.
- Setting the risk appetite for the Company, including specific targets, caps, or indicators related to the risk appetite.
- Monitoring the overall performance of the Bank's and progress towards its strategic objectives and in line with its defined risk appetite.
- Assessing the major risks facing the Company and the steps taken by management to monitor and control such risks.

- Overseeing and approving the risk management framework and associated policies and procedures used by management to effectively manage risk.
- At the recommendations of the CEO, approving the appointment and dismissal of the Chief Risk Officer and Internal Auditor.
- Overseeing the integrity of the financial statements, the compliance with legal and regulatory requirements, the performance, qualifications, and independence of the external auditor and the performance of the internal audit function.
- Overseeing the internal control framework used by management and ensuring it is efficient and effective.
- Overseeing and approving the human resource policies and framework of the Company.
- Taking decisions on major business matters and credit applications as per the defined authority matrix in this Policy Manual.
- Appointing and as necessary dismissing the CEO of the Company.
- Determining the remuneration and incentive schemes, including key performance indicators for senior executives.
- Evaluating the overall performance of key senior executives and taking corrective actions as needed.
- Developing succession plans and developmental objectives for senior executive positions.
- Identifying and recommending potential new board members for election by Shareholders.
- Recommending the board remuneration policy, for approval by the Shareholders.
- Evaluating the overall performance and effectiveness of the Board and its members and taking corrective actions as needed.
- Overseeing the Bank's corporate governance framework and ensuring compliance with approved policies.

### **3.4.2 Audit and Compliance Committee Policies**

The following Audit and Compliance Committee policies are complementary to the policies of the Board of Directors, the Articles of Association of MOB and any

other provisions required of it by Myanmar Companies Law and the Financial Institutions Law (No.20/2016).

### **Roles and Responsibilities**

In particular the Committee shall have the following specific roles and responsibilities (in addition to any other authority that the Board may from time to time delegate the Committee).

#### **1. Inspection and Investigation**

The Audit and Compliance Committee shall be authorized to:

- Investigate any within its authority as outlined in its Articles of Association; and
- Seek any information that it requires from any employee of the Company, and all employees are directed to cooperate with any request made by the Committee.

#### **2. Internal Audit**

The Audit and Compliance Committee shall:

- Monitor and review the effectiveness and organizational structure of the Bank's internal audit function;
- Approve the appointment and removal of the head of the internal audit function review the qualifications and effectiveness of internal audit personnel;
- Ensure the internal audit function has adequate resources and appropriate access to information to enable it to perform its function effectively and in accordance with relevant professional standards;
- Review and assess the annual internal audit plan;
- Review all internal audit report and take or instruct necessary action;
- Ensure the internal audit function remains independent from management to ensure objective reporting;
- Review and monitor management's responsiveness to the findings and recommendations of the internal auditor;

### **3. External Auditors**

The Bank's external auditor shall work closely with the Board of Directors, especially the Audit and Compliance Committee, and report directly to shareholders through the General Meeting of Shareholders (AGM). The Audit and Compliance Committee shall consider and make recommendations to the Board, to be put to shareholders for approval, in relation to the appointment, re-appointment and removal of the Bank's auditing board or external auditors. The Audit and Compliance Committee shall oversee the selection process for new members of auditing board or auditors and if a member of auditing board or an auditor resigns the Audit and Compliance Committee shall investigate the issues leading to this and decide whether any action is required by the Board of Directors.

The Audit and Compliance Committee shall work closely with the Bank's external auditors and shall:

- Oversee the relationship with the external auditor and ensure adherence to the Bank's External Audit policy.
- Recommend to the board for approval of their remuneration, whether fees for audit or non-audit services and that the level of fees is appropriate to enable an adequate audit to be conducted.
- Recommend to the board for approval of their terms of engagement, including any engagement letter issued at the start of each audit and the scope of the audit.
- Assess annually their independence and objectivity taking into account relevant professional and regulatory requirements and the relationship with the auditor as a whole, including the provision of any non-audit services. These regulations are based on the principles that:
  1. The External Auditor must be independent from the client audited, both in mind as in appearance;
  2. An External Auditor is someone who is able, in the light of all relevant facts and circumstances, to form an objective and all impartial opinion on all matters that fall within the scope of his assignment.
- Satisfy itself that there are no relationships (such as family, employment, investment, financial or business) between the auditor and the Bank (other than in the ordinary course of business).

- Monitor the auditor's compliance with relevant ethical and professional guidance on the rotation of audit partners, the level of fees paid by the Bank compared to the overall fee income of the firm, office and partner and other related requirements.
- Assess annually their qualifications, expertise and resources and the effectiveness of the audit process which shall include a report from the external auditor on their own internal quality procedures.
- Ensure adherence with the Bank's policies on supply of non-audit service by external auditor, taking into account relevant ethical guidance and legal requirements regarding the matter. In general, MOB stipulates that the appointed External Auditor shall not provide any other service to the Bank beyond the scope of the financial audit, unless otherwise explicitly approved by the Board of Directors. No exceptions shall be granted if they are deemed to compromise the independence of the External Auditor in any way (e.g., consulting services, tax services, other). Any exceptions to this provision should be disclosed to shareholders along with an explanation as to why this was granted and what assurances exist to safeguard the auditor's independence.
- Consider whether, in order to assure the continuing independence of the external auditors and prevent the External Auditor and the Bank becoming too close, there should be regular rotation of the lead audit partner, ideally, every five (05) years after the start of their involvement. The partner of the audit team of the Company charged with essential tasks who have been replaced are not allowed to work on a new assignment for the Company until at least two years have expired from the date of their replacement.
- Review and discuss with the Board, external auditors and the Bank's internal auditors the performance and adequacy of the Bank's internal audit function, including its responsibilities, budget, staffing, and any proposed changes in the scope or procedures of the internal audit year on year.
- Monitor and review management's responses to recommendations of the external auditor, including those in the Management Letter.

### **3.4.3 Financial Reporting and Financial statements**

The Audit and Compliance Committee shall:

- Monitor, review and assess the integrity of the financial statements of the Bank, including the monthly financial reports required by the regulator, and any other formal announcements relating to the Bank's financial performance, and review any significant reporting issues and judgments contained therein.
- Discuss with management and the external auditors on a regular basis and review and approve the annual financial statements and other disclosures required by laws and regulations, including announcements of a sensitive nature, prior to board approval and public disclosure.
- Review the findings of the audit with the external auditor. This shall include but not be limited to, the following;
  1. A discussion of any major issues which arose during the audit,
  2. Any accounting and audit judgments, and
  3. Levels of errors identified during the audit.
- Review and challenge where necessary:
  1. The consistency of, and any changes to, accounting policies both on a year basis and across the company/group;
  2. The methods used to account for significant or unusual transactions where different approaches are possible;
  3. Whether the company has followed appropriate accounting standards and made appropriate estimates and judgments, taking into account the views of the external auditor;
  4. The clarity of disclosure in the Bank's financial reports and the completeness of the accompanying financial statement notes;
  5. All material information presented with the financial statement, including both financial and non-financial information, such as the business review and the corporate governance statement.
- Review with the internal auditors and the external auditors their annual audit plans and the degree of coordination of such plans and ensure that it is consistent with the scope of the audit engagement.

## **5. Internal Controls**

The Audit and Compliance Committee shall:

- Monitor and review the framework for internal controls and risk management of the Bank to ensure its effectiveness. This includes ensuring the internal auditor conducts adequate testing of the internal controls, per its plan, to attest to the Bank's control effectiveness.
- Discuss any significant internal control deficiencies or material weaknesses and monitor changes needed to mitigate the issues.
- Discuss with management the internal auditors and the external auditors the Bank's policies with respect to risk assessment and risk management. This discussion should cover the Bank's major financial and non-financial risk exposures in close collaboration with the Risk Oversight Committee and the steps management has taken to monitor and control these exposures.

## **6. Compliance**

The Audit and Compliance Committee shall:

- Ensure the Bank has an effective compliance function in place to ensure compliance with external laws and regulations and internal codes and policies, particularly the Code of Conduct.
- Review the findings of any examinations by regulatory and supervisory agencies and respond as needed.
- Review with the Bank's legal counsel, the internal auditors and other appropriate parties, legal matters that may have a material impact on MOB's financial statements and compliance procedures, and any material reports received from or communications with regulators or government agencies.
- Oversee the procedures for
  1. The receipt and treatment of complaints received by MOB regarding financial reporting, accounting and auditing, internal controls, or conduct or conflict matters; and
  2. The confidential, anonymous submission by the Bank's employees of concerns regarding questionable financial reporting, accounting, auditing or other matters. The Committee's objective shall be to ensure that arrangements are in place for the proportionate and independent investigation of such matters and for appropriate follow-up action.

### **3.4.4 Code of Conduct**

The purpose of this Code of Conduct is to:

- Demonstrate MOB' commitment to the highest standards of ethical behavior.
- Encourage proper ethical conduct and sanction misconduct within the bank.
- Develop an ethical culture based on such standards and conduct, led by MOB's shareholders, directors and management, and followed by all employees.

By adopting, following and updating this Code of Conduct on a regular basis, together with the Bank's corporate governance manual, MOB confirms its desire to demonstrably lead and promote good ethical behavior and corporate governance. This Code of Conduct is reviewed and updated on an annual basis.

### **MOB's Ethical Principles**

The Bank is committed to act ethically in all aspects of its business. The Bank's ethical standards are based on the following principles;

- Honesty
- Integrity
- Fairness
- Transparency

Similarly, the Bank expects the same in its relationship with all those with whom it does business.

The Bank's ethical standards focus on the following areas: employees, customers, relations with its business partners, government, society and the wider community. These ethical standards shall also apply to all business areas for all subsidiaries and dependent companies both within and outside of Myanmar.

All of the Bank's ethical standards are based on:

- Respecting the rule of law, Myanmar laws and regulations, and showing respect for human rights;
- Managing the Bank's financial and operational performance to maximize the long-term value for its shareholders;
- Conducting business with integrity and fairness, renouncing bribery and corruption or similar unacceptable business practices, and not giving or accepting gifts and entertainment unless they fall under business custom, are immaterial and infrequent;

- Creating mutual advantage in all the Bank's relationships to build and foster trust; and
- Demonstrating respect for the community the Bank operates in , as well as for the natural environment.

The Bank's business plan will include specific, measurable targets for improving ethical behavior.

### **3.4.5 Ethical Standards for the Bank's Relationship with its Stakeholders**

#### **1. Employees, Officers and Directors**

- The Bank is committed to treating all employees with dignity, trust and respect, and to building a long-term relationship based on Myanmar's labor law and the respect of human rights. The Bank will not employ child labor.
- It is the Bank's policy to provide for and regularly improve upon a healthy, safe and secure working environment for its employees.
- Conflicts of interests can, or appear to, compromise the judgment or objectivity of the Bank's employees and officers. An appropriate conflict policy and disclosure there has been adopted by the Bank.
- The Bank's is an equal opportunity employer. Its recruitment, promotion and compensation policy is based on merit and free of discrimination. Clear and transparent policies to this extent have been developed and put into practice.
- Any kind of discrimination or harassment at the workplace will not be tolerated and contrary behavior properly investigated and dealt with through the Bank's human resources manager and/or MOB's Board of Directors.
- Employees are recognized and rewarded for their performance based on performance objectives, and constructive and regular feedback, through face-to face meeting. The Bank has in place a program, accessible to all employees, which encourages individuals to formulate personal development plans and provides for coaching mentoring and formal skill-enhancing trainings.
- Under the authority of this Code, it is incumbent upon Employees to speak up or report any breaches identified or witnessed per the procedures under this Code.
- The company sanctions the illegal use of confidential and insider information by all officers and employees, and has developed a detailed procedure to effectively deal with this matter.

- A regular consultation process between the Bank's employees and managers has been put in place to effectively deal with employment conditions and other issues that affect the employees work environment
- These principles do not limit the right of the company to enforce discipline or the discipline or issues that affect the employees work environment.
- These principles do not limit the right of the company to enforce discipline or to terminate workers in accordance with Myanmar legislation.
- MOB directors and officers shall be of good reputation and good standing, shall not be individuals, or individuals representing a company or person that is deemed a 'Restricted Person' and shall not have committed any crime or sanctionable practice. (i.e practice that involve corruption, fraud, coercion, collusion, or obstruction) or representing a company or a person that has, such as practices that involve corruption, fraud, coercion, collusion, or obstruction. If a Director or officer ceases to meet such qualification, that person shall resign or be dismissed.

## **2. Customers**

Customer satisfaction is tantamount to the company. Safe and quality products and services, fair pricing and appropriate after-sales service shall define the Bank's relations with its customers.

The company always seeks to deliver what it promises.

## **3. Relations with its Business Partners**

- The Bank will put forth its best effort to only cooperate with business partners that share the same ethical standards as MOB.
- The Bank will respect the sanctity of contracts and business relations.
- The company is committed to complying fully with the Myanmar law on anti-money laundering and only conducts business with reputable suppliers, business customers and other partners who are involved in legitimate business activities and whose funds are derived from legitimate sources.

## **4. Government**

- The Bank seeks to build and manage a sound relationship with governmental authorities on an arm's length basis. No attempts to improperly influence

governmental decisions shall be made, and the Bank will not offer, pay, solicit or accept bribes in any form or shape, either directly or indirectly, in its dealings with the government, administration or counts. Transparent procedures regarding transactions engaged in by the Bank with any government agency or official , or in dealings with any company owned or controlled by a government agency or official , shall be established to this end.

- The Bank will never make political contributions whether in cash or in kind.

## **5. Society, Environment and the Wider Community**

- The Bank's views itself as an integral part of the community in which it operates and is committed to a sound relationship built on respect, trust honesty and fairness.
- The preservation of the environment is of the utmost importance to the Bank. The company thus strives to minimize any disruption to the environment arising from its activities by reducing waste, emissions and discharges, and by using energy efficiently.
- Non-governmental organizations (NGOs) are a key element to any society and the company seeks to build constructive relationships with such organizations in building a better society and environment in an economically sustainable matter.

### **Board Level – Credit & Risk Committee (Bcrc)**

The proposed roles and responsibilities of the Board Level Credit & Risk Committee is summarized below:

The Board Credit/Risk Committee shall be formulated to ensure a continuous Board level formal oversight of the risks embedded in the Bank's operations .It shall assist the Board of Directors in determining the strategic direction of the Bank by providing them inputs on credit & risk management.

### **Roles and Responsibilities**

#### **Policy Review / Approval**

- Setting the Bank's broad credit parameters/limits and establishing overall Credit/lending strategy and principles.

- Oversee the establishment, implementation, review and monitoring of Credit Policies, Procedures, rating methodology, credit risk appetite , portfolio strategy and new credit products.
- Review and approve management’s recommended lending objectives, policies and guidelines that direct the loan portfolio.
- Reviewing the proposed modifications to the credit management policies.

### **Approvals**

- Reviewing and approving individual credit and investment decisions, that falls under the Board Credit Committee’s purview and pose material risk to the Bank’s business strategy or reputation.
- On an annual basis define and delegate sufficient credit / lending and investment authorities of the Bank at various levels of Management (through Credit Committee) to enable implementation of the Credit and Investment Strategy / Policy.
- Seek ratification of approvals provided by them at the quarterly Board Meeting.
- Review and approve credit risk policy exceptions.

### **Management Level – Credit Committee (MCC)**

The proposed roles and responsibilities of the Management Level Credit Committee are summarized below:

- The purpose of the MCC is to support the BOD to:
- Approve all Credit falling within the approval authority of the committee and the overall delegation of approval authority structure of the Bank

### **Roles and Responsibilities**

- Consider credit proposals in accordance with the Delegation Matrix for loans as per the stated policies and approve exceptional credits.
- Decide on new and review/renewal of Credit Applications for borrowers and counterparties up to the approval authorities as delegated to the Committee and within approved policies.
- Seek ratification of approvals provided by them on a quarterly basis from BCRC.

- The Committee shall also review the broad credit portfolio, group exposures, NPL status and other credit risk related issues within the Bank.
- Establish and maintain loans strategy and policies.
- Monitor compliance with both external regulation and the Policy governing the Bank's loans and categories of loans, including requirements relating to composition, diversification, credit risk and yield.
- Deliberate as required to approve or disapprove any matters subject to the Committee's approval authority, as called for by the Credit Policy or Board resolution.
- Consider whether a proposed loan is a related party transaction.
- Monitor the performance of loans.
- Provide the Board with timely assessment of the aggregate credit risk profile concerning risk concentration, portfolio composition and quality.
- Approve target market criteria in line with approved risk strategy and risk appetite of the bank.
- Review and approve delegation of financial approval authority to various officials of the Bank with respect to credit within the overall parameters approval by the Board.
- Approve risk limits proposed i.e credit risk limits.
- Delegation of approval authority structure.
- Approve industry and Country concentration limits.
- Conduct periodic portfolio reviews to ensure that the portfolio risk is within the acceptable risk parameters.
- Propose credit risk strategy and risk appetite of the bank for approval by Board.
- Setting up guidelines for identifying credit risk in all new products, processes and activities.

### **Management Level – Risk Committee (MRC)**

The proposed roles and responsibilities of the Management Level Risk Committee is summarized below:

The MRC will be responsible for assisting the Board of Directors to fulfill their oversight responsibilities for the risks that the Bank is exposed to. The purpose of the MRC is to support the BOD to initially focus on

- Portfolio quality review.
- Asset Liability Management.
- Key Risk Indicators.

### **Roles and Responsibilities**

MRC will provide oversight and monitor all the issues relating to risk policies and procedures and to analyses, manage and control risks on a Bank wide basis. MRC will have the following roles, responsibilities with respect to risk management

- Primary responsibility for managing bank's Credit, Market, Operational Risk and other material risks as required under Pillar II i.e.
- Liquidity Risk, Interest Rate Risk in Banking Book etc.
- Review and approve risk management policies, including policies related to credit, market and operational risks etc.
- Review and approve capital framework and risk aggregation policies and methodologies across the bank.
- Approve significant changes to the Risk Organization.
- Provide the Board with timely assessment of the aggregate credit risk profile concerning risk concentrations, portfolio composition and quality.
- Approve target market criteria in line with approved risk strategy and risk appetite of the bank.
- Review and approve delegation of financial approval authority to various officials of the bank with respect to credit within the overall parameters approved by the Board.
- Approve risk limits proposed i.e. credit risk limits.
- Delegation of approval authority structure.
- Approve Industry concentration limits.
- Conduct periodic portfolio reviews to ensure that the portfolio risk is within the acceptable risk parameters.
- Propose credit risk strategy and risk appetite of the bank for approval by Board.
- Periodically review the risk strategy and appetite of the bank especially with respect to credit portfolio.
- Review and approve the portfolio management strategies.
- Review business asset quality results versus planned asset quality.

- Review the adequacy of the provision for the risk losses.
- Approve the new risk measurement methodologies risk assessment criteria, rating model & score cards adopted by the bank in the credit risk management area.

### **Management Level – Executive Committee (EXCO)**

To approve major business matters within the authority delegated by the Board of Directors, to review and propose significant investment / strategic plans / policies, etc. to the Board of Directors for approval, and to review and monitor the overall financial and risk performance of the Bank.

### **Roles and Responsibilities**

#### **Approve**

- To approve expenses and investments within its authority as delegated by the Board of Directors.
- To approve major business matters in line with the approved strategic objectives and within its authority as delegated by the Board of Directors.

#### **Review and Propose for Board Approval**

- To review and propose the annual collective agenda, budget, and strategic objectives.
- To review and propose expenses and investments requiring Board approval.
- To review and propose the risk appetite for the Bank.
- To review and propose the human resource policies and framework of the Bank.
- To review and propose the launch of new products and services.
- To review and approve the bank's remuneration policy.

#### **Review and Monitor**

- To review and monitor the business financial performance and propose corrective action as needed to align with the agreed objectives.
- To review and monitor the credit and portfolio performance and propose corrective action as needed to align with the agreed objectives.

- To review and monitor progress on projects with significant impact on the bank's financial performance and/or operational efficiency, and to take corrective action as needed to ensure the projects are completed on time, within budget, and achieve the agreed objectives.
- To review and monitor emerging risks in the market, up-and-coming changes in the regulatory environment, and trends in the banking industry.
- To manager matters related to remuneration.

### **Management Level – Asset & Liability Committee (ALCO)**

The Executive Committee establishes Asset Liability Committee (ALCO) to ensure effective implementation of asset liability management policy of the Bank. The Committee shall make oversight of capital planning, balance sheet management, performance management, liquidity and asset liability risk management and investments in the financial markets.

### **Roles and Responsibilities**

#### **Policy Review/Approvals**

- Establish suitable policies for asset liability management and investment operations that would set out proper organization, workflow, methodologies, and controls.
- Maintain effective ALM organizational structure, coordinate respective activities of the Bank's structural divisions and evaluate their performance.
- Determine pricing policy for the main banking products and maintain the market competitiveness through approval of new banking products.

## **CHAPTER IV**

### **ANALYSIS ON THE INTERNAL OPERATION RISK MANAGEMENT AND FUNDAMENTAL PRINCIPLE OF OPERATIONAL RISK MANAGEMENT IN MOB BANK**

This chapter includes the analysis of the data regarding internal operation risk management of front line and middle level respondents and fundamental principle of operational risk management are presented with two parts. It starts with research design and detailed information of respondents, and by the use of descriptive statistics to calculate means and frequency relating to the extent on their agreeable on current operational risk management practices, as follows.

#### **4.1 Survey Design**

This is the study on the internal operational risk management and fundamental principle of operational risk management in Myanmar Oriental Bank, in Yangon. Study mainly focused on primary data. Samples are collected from front line to middle managers, to analyze internal operational risk management and selected top management level for the fundamental risk management at MOB bank. Samples are 70 numbers who are collected from both front line to middle managers, to analyze internal operational risk management and, 20 numbers who are from top management level for the fundamental risk management at MOB bank by means of convenient random sampling method. Study finds out how aware of the Bank is undertaking operational risk management area regarding process risk, people risk, and system risk area. Samples are convenient random sampling method by the assistants of department head of MOB Bank. Survey questionnaire was developed as survey instrument to gather required information.

#### **4.2 Internal Operation Risk Management (Process, People, Systems)**

In the analysis on the internal operational risk management practices, the first part is the analysis on the demographic profiles of the respondents of front line and middle management people, as follows.

#### 4.2.1 Demographic Profiles of Front Line & Middle Level Respondents

In the analysis of the demographic profiles of front line and middle respondents, it is analysis on gender composing, education level, years of service to the MOB Bank, and respondents' aware on the utilization of operation risk management at bank. Table (4, 1) shows the demographic profiles analysis as follows.

**Table (4.1) Demographic Profiles of Respondents**

Sr. No.	Particular	Total Respondents	Percent
		70	100%
<b>Gender of Respondents</b>			
1	Female	43	61%
2	Male	27	39%
	Total 70 of 70 % of staff		
<b>Education of Respondents</b>			
1	University Graduate	37	53%
2	Diploma	26	37%
3	Master Degree	7	10%
	Total	70	100%
<b>Year of Services at Bank Respondents</b>			
1	Less than 1 year	3	4%
2	1 to 3 year	11	16%
3	4 to 7 years	34	49%
4	8 to 10 years	10	14%
5	above 10 years	12	17%
<b>Utilization of operation risk management</b>			
1	Strongly Disagree	0	0%
2	Disagree	0	0%
3	Neutral	21	30%
4	Agree	28	40%
5	Strongly agree	21	30%

Source: Survey data, 2019

By the Table (4.1), 43 numbers or 61% are female respondents and 27 number or 39% is male. In this study, female respondents are more than male composition. Educations of respondents are analyzed. Survey shows that 37 are University Graduate, 26 are post graduate diploma, and 7 are master degree level. Survey shows that only educated people are involved in the study.

Year of Services at Bank Respondents are analyzed. Their working service are grouped into Less than 1 year, 1 to 3 year, 4 to 7 years, 8 to 10 years, and above 10 years. In the analysis, 80 percent or the most percentage of respondents are found as over 4 years' experience, in current MOB company.

Utilization of operation risk management is analyzed. Respondents are asked to rate their agreeable extent from 1=Strongly Disagree, 2 Disagree, 3= Neutral, 4= Agree, and 5= Strongly agree, respectively. By the analysis, Table (4.1) showing that 21 out of 70 reply that normal operation risk management practices, 28 reply that their organization is practicing operational practices, and the rest 21 respondents strongly agreed on that of their bank strongly emphasis on operation risk management. By the survey, most of front line and middle managers' agreeable on that of their organization has well operational-risks management practice regularly.

#### **4.2.2 Analysis on Internal Operation Risk Management Culture at Front Line and Middle Level Respondents**

Saul McLeod, (2019) have explained on A Likert scale definition with examples (<https://www.simplypsychology.org/>) and he assumes that the strength/intensity of an attitude is linear, i.e. on a continuum from strongly agree to strongly disagree, and makes the assumption that attitudes can be measured 5= Always or very great extent, 4= often or great extent, 3=sometime, 2=little extent or rarely, 1= never.

In the analysis on the operation risk management practices, the first analysis is on the people risk at bank. Survey is made on required employees' skills to perform their work effectively, possess ethical behavior necessary to mitigate the bank against people risk, staff have sometimes forget to stay comply with policy requirement of the bank, keeping recorded has recorded cases of dishonesty among its employees, unethical of some officials with a supervisory responsibility misuse it for their personal benefits, bank wide diversity of employees in the working environment, and for the senior management ensuring establishment of specific and formal operational risk management committees, which are examined. Table (4.2) shows the respondents' agreeable of their bank well management at people risk management, as follows.

**Table (4.2) People Risk Management**

<b>Sr.</b>	<b>People risk</b>	<b>Mean</b>	<b>Standard Deviation</b>
1	Employees at MOB bank have the necessary skills to perform their work effectively	3.76	0.77
2	Employees at MOB bank possess ethical behavior necessary to mitigate the bank against people risk	3.67	0.81
3	Staff have sometimes failed to comply with policy requirement of the bank	3.51	0.70
4	The bank has recorded cases of dishonesty among its employees	3.97	0.95
5	Some officials with a supervisory responsibility abuse it for their personal benefits	3.57	0.83
6	MOB bank has a wide diversity of employees in the working environment	3.40	0.62
7	Senior management ensures establishment of specific and formal operational risk management committees	4.03	0.87
	Overall mean	3.70	

Source: Survey data, 2019

By the Table (4.2), the higher overall mean value of People Risk Management is 3.70. The higher mean value is indicating that of well practicing of the front line and middle management personal at people risk management practices. The highest mean value 4.03 is showing that the commitment of front line and middle management to their senior management, with which very great extent at ensuring establishment of specific and formal operational risk management committees. The lowest mean value is 3.40, and thus they all agreed that there is high level of people risk from a wide diversity of employees in the working environment at MOB Bank.

#### **4.2.3 Analysis on Process Risk Management**

Table (4.3) is the analysis on the process risk management. It is a continual cyclic process at which assessment, decision making, and implementation of risk controls, this aims at acceptance, mitigation, or avoidance of risk (Wikipedia). In this process risk management, total five statements is used and the analysis is shown in Table (4.3), as follows.

**Table (4.3) Process Risk Management**

Sr. No.	Process	Mean	St Dev
1	MOB bank has witnessed cases of design weakness in some its processes	3.37	0.64
2	MOB bank has experienced underlinable hardware and software issues	3.93	0.82
3	MOB bank has had dependent processes not integrating to the degree for a business unit to achieve its objectives	3.50	0.78
4	MOB bank has no clear acceptance of accentuality or responsibility for business process	3.50	0.59
5	The evaluation of new processes or changes to existing processes are not done at the development phase	3.57	0.60
	Overall mean	3.57	

Source: Survey data, 2019

By the Table (4.3), the higher overall mean value of process risk management is 3.57. The higher mean value is indicating that of well practicing of process risk management by the middle and front-line management team. The highest mean value 3.93 is showing that front & middle management have MOB bank has experienced underlinable hardware and software issues to manage process risk. The lowest mean value is 3.37, which is also greater than 3, and thus middle and front-line management team are strong experiences of process risk like witnessed cases of design weakness in some its processes.

#### **4.2.4 Analysis on Systems Risk Management**

Table (4.4) is the third form of operation risk management at systems risk management practices. In this analysis, total eight statements: bank has experiences system disruptions, having reasonable security measures for system risk management, good practice guidance on password security, has experienced from financial losses from acts of IT related risks, Internal Audit Department regularly systems audit, facing the volume of transactions consistently exceeds the technology's ability to deliver, functionally of systems aligned with organizational objectives, and bank has experienced cases of disastrous events that have caused damage to the bank resources, which all are tested to the middle and front-line management people.

**Table (4.4) Systems Risk Management**

Sr. No.	Systems	Mean	St Dev
1	MOB bank has experienced system disruptions which have interrupted business	3.54	0.85
2	Reasonable security measures have been put in place to prevent unauthorized access to the banks network	3.54	0.74
3	Staffs are given good practice guidance on password security	3.51	0.74
4	MOB bank has suffered financial losses from acts of IT related risks	3.53	0.70
5	Internal Audit Department regularly conducts systems audit	3.40	0.79
6	The volume of transactions consistently exceeds the technology's ability to deliver	3.51	0.72
7	Functionally of systems have been aligned with business objectives	3.60	0.71
8	MOB bank has experienced cases of disastrous events that have caused damage to the bank resources.	3.41	0.81
	Overall mean	3.51	

Source: Survey data, 2019

By the Table (4.4), the higher overall mean value of system risk management is 3.51. The higher mean value is indicating that of well-prepared system risk management to the middle and front-line management team. The highest mean value 3.60 is showing that the beliefs of front & middle management in that of the functionality of system, aligned with bank's objectives. The lowest mean value is 3.40, which is also greater than 3, and thus Internal Audit Department regularly conducts systems audit as per scheduled by internal auditing department.

#### **4.2.5 Summary of Risk Management**

Overall mean values of people risk, process risk and system risk are 3.7, 3.57 and 3.51 respectively. According to the survey results, the respondents agreed with operational risk practices conducting in MOB.

#### 4.2.6 Three Lines of Defense Risk Management

Table (4.5) is the analysis on the three lines of defense Risk Management by means of well-established roles and responsibilities for the three lines of defense, more refined approach to assigning specific roles and responsibilities, and strong risk culture and good communication between the three lines of defense, which are tested to ensure good operational risk governance at MOB Bank, as follows.

**Table (4.5) Three lines of defense Risk Management**

Sr. No.	Three lines of defense	Mean	Standard Deviation
1	Established roles and responsibilities for the three lines of defense	3.99	0.99
2	Implemented a more refined approach to assigning specific roles and responsibilities for the three lines of defense	3.77	1.00
3	Strong risk culture and good communication between the three lines of defense to ensure good operational risk governance	3.46	0.79
	Overall Mean	3.74	

Source: Survey data, 2019

By the Table (4.5), the higher overall mean value of three-lines of defense's risk management is 3.74. The higher mean value is indicating that of well-prepared system risk management to the middle and front-line management team. Established roles and responsibilities for the three lines of defense is the important and highest risk management among these three lines of defense by the highest mean value 3.99. The lowest mean value is 3.46, which is showing strong risk culture and good communication between the three lines of defense which are important to ensure good operational risk governance, and thus study finds out there has strong risk management culture at these three-lines of defenses.

#### 4.3 Fundamental Principles of Operational Risk Management by Senior Management Level Respondents (Principle 1 & 2)

In this part, operational risk management is tested which is done by senior management level respondents. It starts with the profiles of management level respondents who are involving in this study, and followed by their operational risk

management regarding to risk culture management shown in principle (1) of fundamental principles of operational risk management, and then, makes an analysis on risk management framework according to principle (2) of Fundamental Principles operational risk management, which are stated as follows.

#### 4.3.1 Profiles of Management Level Respondents

In the analysis of the demographic profiles of senior-management level respondents, it is also focused analysis on their gender, education level, years of service to the Myanmar Oriental Bank, and the extent to awareness at utilizing of operation risk management at bank. Table (4.6) shows the senior management demographic profiles analysis as follows.

**Table (4.6) Profiles of Management Level Respondents**

Sr. No.	Particular	Total Respondents	Percent
		20	100%
Gender of Respondents			
1	Female	12	60%
2	Male	8	40%
Education of Respondents			
1	University Graduate	0	0%
2	Diploma	15	75%
3	Master Degree	5	25%
Year of Services at Bank Respondents			
1	4 to 7 years	4	20%
2	8 to 10 years	9	45%
3	above 10 years	7	35%
Utilization of operation risk management			
1	Agree	9	45%
2	Strongly agree	11	55%

Source: Survey data, 2019

By the Table (4.6), 12 numbers or 60% are female respondents and 2 numbers or 40% is male. In this study, female respondents are more than male composition. Education of respondents are also studied. Survey shows that no one are University Graduate, however 15 or the most respondents are post graduate diploma, and 5 are master degree level. Survey shows that more educated senior management person are involved in the study.

Year of services of senior management respondents are analyzed. Their working service are grouped into Less than 1 year, 1 to 3 year, 4 to 7 years, 8 to 10 years, and above 10 years. In the analysis, 80 percent or the most percentage of respondents are found as more than eight-year working experience, in current MOB.

#### **4.3.2 Analysis on Fundamental Principles of Operational Risk Management by Senior Management (Principle 1 & 2)**

To understand people judgment in extent of agreeable to a variable, Likert scale measurement is practiced, assuming that the strength/intensity of an attitude is linear, i.e. strongly agree to strongly disagree, and makes the assumption that attitudes can be measured 5= Always or very great extent, 4= often or great extent, 3=sometime, 2=little extent or rarely, 1= never. In that analysis at fundamental principles of operational risk management practices is shown, below.

#### **4.3.3 Fundamental Principles of Operational Risk Culture**

Table (4.7) shows the fundamental Principles of Operational Risk Culture practice at senior management.

**Table (4.7) Fundamental Principles of Operational Risk Culture**

<b>Sr. No.</b>	<b>Operational risk culture (Principle-1)</b>	<b>Mean</b>	<b>St. Dev.</b>
1	Code of conduct or ethics policy	4.15	0.81
2	Compensation policies aligned with the bank's statement of risk appetite and tolerance	3.70	1.03
3	Compensation policies that balance risk and reward	3.65	0.88
4	Operational risk training available throughout the organization	3.65	0.81
	Overall mean	3.79	

Source: Survey data, 2019

By the Table (4.7), the higher overall mean value of fundamental principles of operational risk culture is 3.79. The higher mean value is indicating that MOB has strong fundamental principles relating to operation risk cultures. The highest mean value is found as code of conduct or ethics policy at MOB bank which is a guide for operational risk management with mean value 4.15. The lowest mean value is found in operational risk training available throughout the organization, with mean value 3.65 and lower standard deviation value 0.81. And thus, study finds out MOB Bank has strong fundamental principles of operational risk management culture behavior.

#### 4.3.4 Study on Operational risk management framework

Table (4.8) is the analysis on the fundamental principles relating to operational risk management framework, as follows.

**Table (4.8) Fundamental Principles Operational risk management framework**

Sr. No.	Operational risk management framework (P-2)	Mean	St. Dev.
1	Integration of ORMF into overall risk management process	4.00	0.92
2	Documented in board of directors-approved policies and governance structures used to manage operational risk	3.85	0.93
3	Identifies the governance structures used to manage operational risk	3.55	0.83
4	Establishes risk reporting and MIS	4.10	1.07
5	Describes the roles and responsibilities of each of the three lines of defense	3.95	1.15
6	Requires the policies to be reviewed whenever a material change occurs	4.25	0.64
	Overall mean	3.95	

Source: Survey data, 2019

By the Table (4.8), the higher overall mean value of fundamental principles relating to operational risk management framework is 3.95. The higher mean value is indicating that of well fundamental principle of operational risk management framework set up by the senior management team. The highest mean value 4.25 is showing that senior management are flexible to frequent reviews as required on the policies whenever a material change occurs. The lowest mean value is 3.55, which is

also greater than 3, and thus senior management has already identified well governance structures which will be used to manage operational risk at all level of bank organization.

## **CHAPTER V**

### **CONCLUSION**

In this section, it states the findings and discussion of the study, along with the recommendation, and the needs for further studies.

#### **5.1 Findings and Discussions**

The objective of the study focus on the internal operational risk management and fundamental principle of operational risk management in Myanmar Oriental Bank, in Yangon Region. 70 numbers of respondents are collected from both front line to middle managers, to analyze internal operational risk management and, 20 numbers of samples are selected from top management level for the fundamental risk management at MOB bank by means of convenient random sampling method. Focusing area includes how aware of the Bank is undertaking operational risk management area regarding process risk, people risk, and system risk area. And for the analysis on fundamental risk management principles in terms of operational risk cultures and operational risk management framework. Samples are convenient random sampling method by the assistants of department head of MOB Bank. Survey questionnaire was developed as survey instrument to gather required information. Findings of the study is shown as follows.

Regarding the people risk management culture, survey finds out that there has well practicing of the front line and middle management personal at people risk management practices. There is found that high commitment of front line and middle management to their senior management, with which very great extent at ensuring establishment of specific and formal operational risk management committees.

Regarding the process risk management culture, survey finds out that there has strong practicing of the front line and middle management personal at process risk management practices. The highest mean value at process risk management is at front & middle management who have already experienced underlinable hardware and software issues to manage process risk successfully.

Third form of operation risk management at systems risk management practices. Survey result is indicating that of well-prepared system risk management to the middle and front-line management team. The highest mean value is found as the

beliefs of front & middle management in that of the functionality of system, aligned with bank's objectives.

Three lines of defense Risk Management by means of well-established roles and responsibilities for the three lines of defense, more refined approach to assigning specific roles and responsibilities, and strong risk culture and good communication between the three lines of defense, which are analyzed. The higher mean value finds out that of well-prepared system risk management to the middle and front-line management team.

In the analysis on the fundamental Principles of operational Risk culture and risk management framework undertaken by senior management team are analyzed. In this study, survey found that the higher mean values are indicating that MOB has strong fundamental principles relating to operation risk cultures and framework, i.e., thus senior management has already identified well governance structures which will be used to manage operational risk at all level of bank organization, and thus, MOB Bank has found as strong fundamental principles of operational risk management culture behavior.

## **5.2 Recommendations and Suggestions**

Regarding the people risk management culture, survey finds out that front line and middle management personal have well practicing of the at people risk management practices. By the survey result, it would like to recommend to continue to follow risk management practice to mitigate people risk. It would also like to suggest the front line and middle management personal, to improve behavior in the staff to comply more with risk management policy because they have sometimes failed to comply with policy requirement of the bank.

Regarding the process risk management culture, there has strong practicing of the front line and middle management personal at process risk management practices. And thus, it would also like to recommended to follow current process risk to have more compliance. It would like to suggest to front line and middle management personal to record witnessed cases of design weakness in some its processes. So that, there would be lesson-learn to improve process risk management at MOB Bank.

Regarding to systems risk management practices, survey result is showing that of well-prepared system risk management to the middle and front-line management team with the higher beliefs of front & middle management in that of the functionality

of system, aligned with bank's objectives. It would like to suggest to front line and middle management personal to have proper record keeping more at cases of disastrous events that have caused damage to the bank resources. It would also like to suggest to Internal Audit Department to review their regularly conducts systems audit because the obtained mean value is not too higher.

Regarding the three lines of defense risk management by means of well-established roles and responsibilities for the three lines of defense, more refined approach to assigning specific roles and responsibilities, and strong risk culture and good communication between the three lines of defense, which are analyzed. By the higher mean score, it is strongly recommended to front & middle management for the compliance of these three lines of defense for more risk mitigating at MOB Bank.

Regarding to the analysis on the fundamental principles of operational risk culture and risk management framework undertaken by senior management team are analyzed as well, it would like to recommended to senior management team for their systematic and very fundamental operational risk management culture and framework. It would like to suggest to senior management team, to improve more on that of other operational risk management principles and to follow to the implementation steps, so as the whole organization would be overwhelmed by systematic and building up internationalized standard risk management culture at MOB bank.

### **5.3 Needs for Further Studies**

This study only focuses on internal operational risk management practices and fundamental operational risk management practices in terms of risk culture and risk framework. There may be other operational risk management practices in bank sector, such as external operational risk management and many others. For that, further studies are needed to extend to study other operational risk management practices, which can fulfill the risk management of MOB. This study only focuses on MOB branches in Yangon. The study does not cover the whole MOB branches around the country. To understand more operational risk management practices in banking sector, further studies are needed to extend to other private commercial financial associations as well as to extend to public national banks in Myanmar.

## REFERENCES

1. Baxte R, J., Megone, C., Dempsey, J., & Lee, J. (2012). *Real Integrity: Practical solutionsfor organisations seeking to promote and encourage integrity. Research Report*. London, UK: The Institute of Chartered Accountants in England and Wales.
2. Cania, L. (2014). The Impact of Strategic Human Resource Management on Organizational Performance. *Economia. Seria Management*, 7(2), 373-384.
3. Certo, S. (2015). *Supervision: Concepts and skill-building*. New York, NY: McGraw-Hill Higher Education.
4. CFA Institute. (2013). *Global Market Sentiment Survey Report*. London, UK: CFA Institute.
5. DCIO. (2011). Standards of Sound Business and Financial Practices. *Enterprise Risk Management Practices*. Ontario, CA.
6. Deloitte. (2014). 2014 global survey on reputation Risk. London, UK: Deloitte.
7. GIZ, 20.16, Myanmar's Financial Sector, A Challenging Environment for Banks (3rd Edition,),
8. Klosters, D. (2014). *Matching Skills and Labour Market Needs*. Swiss, SW: World Economic Forum.
9. Maina, G., Alala, O., Wabwile, E., & Musiege, D. (2014).Effects of Operational Risks in the Lending Process of Commercial Banks Profitability in Kakamega Town. *International Journal of Business and Management Invention*, 3(31), 11-17.
10. McMillan, J., & Schumacher, S. (2001). Research in Education: A conceptual.
11. Mamontov, A. (2007),Internal control reports and financial reporting problems. *Accounting Horizons*, 10(25), 65-75.
12. Nanayakkara, W. (2012). Modern Challenges to the Principle of the Banker's Duty of Confidentiality: A Critical Analysis. Colombo, SR: University of Colombo
13. Zikmund, W., & Babin, B. (2012). *Essentials of marketing Research*. Boston, MA:

14. Bindya Kohli, Dr. (20.13). Basel I to Basel II to Basel III: Risk management journey of India Banks. Retrieve AIMA Journal of Management & Research, May 2013, Volume 7, Issue 2/4, ISSN 0974 497.  
Website: [https://apps.aima.inkjournal\\_new/articlesPDF/Dr.BindyaKohli.pdf](https://apps.aima.inkjournal_new/articlesPDF/Dr.BindyaKohli.pdf)
15. EY, 2012, Banking and financial services risk management survey, 2012. Progress in financial services risk management (PDF format). Retrieve website: [http://www.ey.com/Publication/vwLUAssets/Banking\\_and\\_financial\\_services\\_risk\\_managementsurvey\\_2012/\\$FILE/Progress\\_in\\_financial\\_services\\_risk\\_management.pdf](http://www.ey.com/Publication/vwLUAssets/Banking_and_financial_services_risk_managementsurvey_2012/$FILE/Progress_in_financial_services_risk_management.pdf)
16. FAA System Safety Handbook, Chapter 15: Operational Risk Management December 30,2000 (PDF format).Retrieve from online website:// [https://www.faa.gov/regulations\\_policies/handbooks\\_manuals/aviation/risk\\_management/ss\\_handbook/media/Chap15\\_1200.pdf](https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/media/Chap15_1200.pdf)
17. Metric stream. Operational Risk Management (ORM) Framework in Banks and Financial Institutions: retrieve from online website: [https://www.metricstream.com/solution\\_briefs/ORM.htm](https://www.metricstream.com/solution_briefs/ORM.htm)
18. Prokopenko, Yevgen, Banking Advisor and Bondarenko, Denis IFC Banking Expert in Tirana, Albania ,2010, (PDF format). Retrieve from online website : <https://www.ifc.org/wps/wcm/connect/e4f8ce004d6f9e3d85c8b548b49f4568/ECA-CROPRIKtraining.pdf?MOD=AJPERES>
19. Risk management in banks website : <https://www.educba.com/risk-management-in-bank>
20. Strachnyi, K. (2016). *Costs of Operational Risk Mismanagement*. Retrieved May 11, 2016, from Risk Article: <https://riskarticles.com/costs-of-operationalriskmanagement/>
21. Top 10 operational risks in 2017, risk.net. Retrieve from online website: <https://www.risk.net/risk-management/operational-risk/2480528/top-10-operational-risks-for-2017>
22. Corporate Governance of Myanmar Oriental Banks (<https://www.mobmyanmar.com>)
23. Review of the Principles for the Sound Management of Operational Risk, October 6, 2014, Basel Committee on Banking Supervision, Bank for International Settlements

24. Principles for the Sound Management of Operational Risk, FRM (Financial Risk Manager)
25. Operational Risk Management, Senior Management Awareness Workshop, IFC Financial Institutions Group, Advisory Services

# APPENDICES

## APPENDIX I

### Section (A) Demographic Profiles of Respondents

#### 1. Gender of Respondent

- Male
- Female

#### 2. Years of Working experience in this organization.

- 1 to 5 years
- 6 to 10 years
- Over 10 years

#### 3. Please state your role at the following management level.

- Top level
- Middle level
- Functional level

#### 4. Education Background

- Vocational Training
- University Student
- University graduate
- Post Diploma
- Master and above level

#### 5. Does your bank utilize operational risk management practices?

- Yes
- No

**Section (B) Effectiveness Of Internal Operational Risk Management Practices At Mob Bank (In A Scale Of 1-To-5 Where 1= Strongly Disagreed, 2= Disagreed, 3= Neutral, 4= Agreed, 5= Strongly Agreed)**

Sr.	People risk	1	2	3	4	5
1	Employees at MOB bank have the necessary skills to perform their work effectively	1	2	3	4	5
2	Employees at MOB bank possess ethical behavior necessary to mitigate the bank against people risk	1	2	3	4	5
3	Staff have sometimes failed to comply with policy requirement of the bank	1	2	3	4	5
4	The bank has recorded cases of dishonesty among its employees	1	2	3	4	5
5	Some officials with a supervisory responsibility abuse it for their personal benefits	1	2	3	4	5
6	MOB bank has a wide diversity of employees in the working environment	1	2	3	4	5
7	Senior management ensures establishment of specific and formal operational risk management committees	1	2	3	4	5
Sr.	Process	1	2	3	4	5
1	MOB bank has witnessed cases of design weakness in some its processes	1	2	3	4	5
2	MOB bank has experienced underlinable hardware and software issues	1	2	3	4	5
3	MOB bank has had dependent processes not integrating to the degree for a business unit to achieve its objectives	1	2	3	4	5
4	MOB bank has no clear acceptance of accentuality or responsibility for business process	1	2	3	4	5
5	The evaluation of new processes or changes to existing processes are not done at the development phase	1	2	3	4	5
Sr.	Systems	1	2	3	4	5
1	MOB bank has experienced system disruptions which have interrupted business	1	2	3	4	5
2	Reasonable security measures have been put in place to prevent unauthorized access to the banks network	1	2	3	4	5
3	Staff are given good practice guidance on password security	1	2	3	4	5
4	MOB bank has suffered financial losses from acts of IT related risks	1	2	3	4	5
5	Internal Audit Department regularly conducts systems audit	1	2	3	4	5

Sr.	<b>Systems</b>	1	2	3	4	5
6	The volume of transactions consistently exceeds the technology's ability to deliver	1	2	3	4	5
7	Functionally of systems have not been aligned with business objectives	1	2	3	4	5
8	MOB bank has experienced cases of disastrous events that have caused damage to the bank resources.	1	2	3	4	5
Sr. No.	<b>Three lines of defense</b>	1	2	3	4	5
1	Established roles and responsibilities for the three lines of defense	1	2	3	4	5
2	Implemented a more refined approach to assigning specific roles and responsibilities for the three lines of defense	1	2	3	4	5
3	Strong risk culture and good communication between the three lines of defense to ensure good operational risk governance	1	2	3	4	5

**Section (C) Compliance of the two Fundamental Principles of Operational Risk Management at MOB (In a scale of 1-to-5 where 1- Principle has not been implemented, 2- Principle is materially not compile with, 3- Not applicable, 4- Principle is largely compiled with, 5- Principle is fully complied with)**

<b>Sr. No.</b>	<b>Operational risk culture (Principle-1)</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
1	Code of conduct or ethics policy	1	2	3	4	5
2	Compensation policies aligned with the bank's statement of risk appetite and tolerance	1	2	3	4	5
3	Compensation policies that balance risk and reward	1	2	3	4	5
4	Operational risk training available throughout the organization	1	2	3	4	5
<b>Sr. No.</b>	<b>Operational risk management framework (Principle -2)</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
1	Integration of ORMF into overall risk management process	1	2	3	4	5
2	Documented in board of directors-approved policies and governance structures used to manage operational risk	1	2	3	4	5
3	Identifies the governance structures used to manage operational risk	1	2	3	4	5
4	Establishes risk reporting and MIS	1	2	3	4	5
5	Describes the roles and responsibilities of each of the three lines of defense	1	2	3	4	5
6	Requires the policies to be reviewed whenever a material change occurs	1	2	3	4	5

**Thank you for your kind participation.**