YANGON UNIVERSITY OF ECONOMICS

DEPARTMENT OF COMMERCE

MASTER OF BANKING AND FINANCE PROGRAMME

OPERATIONAL RISKS PRACTICES IN UNITED AMARA BANK

MYAT THUZAR NWE

ROLL NO-66

MBF- 4TH BATCH

DECEMBER, 2018

OPERATIONAL RISKS PRACTICES

IN UNITED AMARA BANK

A thesis submitted to the Boards of Examiners in partial fulfillment of the requirements for the degree of Master of Banking and Finance (MBF)

Supervised By:

Daw Yee Yee Thein

Associate Professor

Department of Commerce

Yangon University of Economics

Submitted By:

Ma Myat Thuzar Nwe

MBF (4TH Batch)- 66

Master of Banking and Finance

2016 - 2018

ABSTRACT

The purpose of this study is to investigate the operational risks practices in UAB Bank. The study was guided by the following objectives which is to identify the risk management practices in United Amara Bank and to analyze the extent types of operational risk practices in UAB Bank. The target population of this study was UAB employees in the 20 UAB Bank branches in Yangon. The descriptive analysis method was used. The structured 140 questionnaires are distributed among those branches. The finding showed that UAB Bank have in place of contingency and business continuity plans to ensure their ability to operate as going concerns and minimize losses in the event of severe business disruption. Internal controls are typically embedded in a bank's day to day business and also designed to ensure, to the extent possible that bank activities are efficient and effective. Therefore, internal control is among the core principles of managing risks and the bank needs to get it right. As a result of analyzing the extent of the types of operational risk practices, there is a need for an effective monitoring process to maintain high standards of ethics for effective corporate governance and regular staff training as a measure to control operational risk exposure. The institution should seek an innovative team capable of creating products and making the firm a market leader in product innovation. There is a need for the institution to establish communication channels to enable employees become aware of any cases of losses resulting from deliberate employee actions and dishonesty.

ACKNOWLEDGMENTS

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, for his concern and good academic guidance to the participants of the MBF Programme.

My sincere appreciation is extended to Prof. Dr. Daw Soe Thu, Head of Department of Commerce and Program Director of Master of Banking and Finance for her kind effort, good contribution and great encouragements to MBF program.

My special deepest thanks to Supervisor Daw Yee Yee Thein, Assistant Professor, Department of Commerce, Yangon University of Economics for her great effort and guidance to successfully finished this paper.

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 Executive Directors (Support), UAB Bank and all the UAB Bank members who contributed to this paper, without their helping hands, this report 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

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Nowadays, rapid innovations in financial markets and the internationalization of financial flows have changed the face of banking sector. Technological progress and deregulation have both provided new opportunities for and increased competitive pressures among banks and non-banks alike. Banks have responded to these new challenges with vigor. The growth in international financial markets and a greater diversity of financial instruments have allowed banks wider across to funds. At the same time, market have expended, and opportunities to design new products and provides more services have appeared. While the pace of these changes appears to be quicker in some countries than in others, banks everywhere are generally becoming more involved in developing new instruments, products and services and techniques.

These developments have increased the need for and complicated the function of risk measurement, management and control. In the banking industry, the new banking environment and increased market volatility have necessitated an integrated approach to asset-liability and risk management techniques.

Risk is the fundamental element that drives financial behavior. In general, 8 types of banking risks such as Credit Risk, Market Risk, Operational Risk, Liquidity Risk, Business Risk, Reputational Risk, Moral Hazard Risk. Among them, three risks are major risks for the bank. They are Credit Risk, Market Risk and Operational Risk. Credit risk is the probable risk of loss resulting from a borrower's failure to repay a loan or meet contractual obligations. Traditionally, it refers to the risk that a lender may not receive the owed principal and interest, which results in an interruption of cash flows and increased costs for collection. Market risk is the possibility of an investor experiencing losses due to factors that affect the overall performance of the financial markets in which he or she is involved. Operational risk is defined by the Basel Committee on Banking Supervision (2006) as: “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk”

Operational risks are related to a bank’s overall organization and functioning of internal systems, including computer-related and other technologies and bank policies and

procedures. The administration of operational risk is a noteworthy part of key risk administration process for businesses. The acknowledgement of operational danger as a particular class beside other risks (market and credit) by the Basel Committee on banking supervision signifies its developing significance. While the management of operational risk is the essential obligation of every business sector. (Rippel & Teply, 2011)**1.1 Rationale of the Study**

In the banking industry, the senior management will prevent all risks for organization's benefit. Especially financial risk and operation risk are important to protect. If banks do not protect the risks properly, their operation may experience losses. And that is the reason why so many banks today establish risk management committee and risk department just to prevent and manage risks so that they can reduce their losses. A good financial risk management process helps to uphold stability and continuity in revenue and earnings growth. The operational risk is complex in nature compared to credit and market risk as it is largely internal and vary across banks which makes it difficult to assess as well as to manage. A survey of operational risks management practices by commercial banks revealed that commercial banks in any country have suffered not only human risk and process risk but also external risk. (Idarus, 2005)

Practicing risk management become one of the biggest challenges for banks in Myanmar. Banks need operational risk management so as to perform all their operation with internal control and internal check regularly done by senior management. The success of banks is therefore resulted from how effective and systematic of its risk management practices. In Myanmar, there are 4 state own banks and 27 privately owned banks at the present. United Amara Bank is one of the top ten banks and well known in Myanmar. In this time of high competition, it is more important to be sustainable than to be profitable. In order to stand still in the banking industry, United Amara Bank should identify and efficiently control the risks especially operational risk. This study looks at the risk management practices of United Amara Bank and focuses on operational risk management.

1.2 Objectives of the Study

There are two main objectives in this study. These are

1. To identify the risk management practices in United Amara Bank.
2. To analyze the extent of types of operational risk practices in United Amara Bank.

1.3 Scope and Method of the Study

This study is to analyse the operational risk management in United Amara Bank. This study will use the descriptive research method. There are 78 branches all over the country. Primary data was collected from 140 respondents from 20 branches in Yangon which are randomly selected that included Executive Directors, members of Risk Management Committee and Risk Managers of United Amara Bank by using structured questionnaires and conducting in-depth personal interview and general field observation. Secondary data was collected from profile and previous record of United Amara Bank, internet websites and other relevant journals and texts.

1.4 Organization of the Study

There are total of five chapters in this study. Chapter one is the introduction of the paper and includes the rational of study; objective of the study; methods, scope and limitation of the study, and organization of the paper. Chapter two discusses theoretical background and presents the Risk and Risk Management and the Risk-Based of Banks. Chapter three details Profile of the United Amara Bank including the background of the United Amara Bank, the objectives of the company, the organization structure of the United Amara Bank and the functions of Risk Management Committee. Chapter four consists of the analysis on extent of types of Operational Risk Practices in United Amara Bank. Chapter five concludes the study with finding and discussion, suggestions, and need for future research.

CHAPTER II

THEORICAL BACKGROUND

This chapter provides further explanation about the theoretical base of the thesis with four different parts. The first part is the definitions and determinants of risk and risk management including different types of risk. The second part explains the influencing factors for effective risk management. The third part is about operational risk management practices in banks and the final part of the chapter describe the assessment of operational risk management practices in banks and their effectiveness in details.

2.1 Risk and Risk Management

Risk is the potential of gaining or losing something of value. Values (such as physical health, social status, emotional well-being, or financial wealth) can be gained or lost when taking risk resulting from a given action or inaction, foreseen or unforeseen (planned or not planned). Risk can also be defined as the intentional interaction with uncertainty. Uncertainty is a potential, unpredictable, and uncontrollable outcome; risk is a consequence of action taken in spite of uncertainty.

Banks are literally exposed to many different types of risks. A successful banker is one that can mitigate these risks and create significant returns for the shareholders on a consistent basis. Mitigation of risks begins by first correctly identifying the risks, why they arise and what damage can they cause. There are 8 types of major risks that are faced by every bank (Gangreddiwar, 2015). They are as follows:

Credit Risk is the risk that arises from the possibility of non-payment of loans by the borrowers. Although credit risk is largely defined as risk of not receiving payments, banks also include the risk of delayed payments within this category. The profitability of a bank is extremely sensitive to credit risks. Therefore, to deal with such risk banks have come up with a wide variety of measures. For instance, banks always hold a certain amount of funds in reserves to mitigate such risks.

Market Risk is defined by Bank for International Settlements (BIS) that the risk of losses in on-or off-balance sheet positions that arise from movement in market prices. Market risk is prevalent mostly amongst banks that are into investment banking since they are active in capital markets.

Operational Risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events defined by Bales Committee. This definition includes legal risk but excludes strategic and reputational risk. Operational risk occurs as the result of a failed business processes in the bank's day to day activities. This risk may be increased by poor training, inadequate controls, poor staffing resources, or other factors.

Liquidity Risk is another kind of risk that is inherent in the banking business. Liquidity risk is the risk that the bank will not be able to meet its obligations if the depositors come in to withdraw their money. This risk is inherent in the fractional reserve banking system. Therefore, in this system, only a percentage of the deposits received are held back as reserves, the rest are used to create loans.

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 an extremely important intangible asset in the banking business. Customers like their money to be deposited at places which they believe follow safe and sound business practices. Hence, if there is any news in the media which projects a given bank in a negative light, such news negatively impacts the banks business. Also, banks need to continuously ensure that their public relations efforts project them as a friendly and honest bank.

Systemic 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 by which a business seeks to reduce or mitigate the possibility of loss or damage inherent in the industry. Risk management process in

banks may take many different forms, including lending and investing strategies, employee training, or security. A key factor of risk management in any bank is the means to identify sources of risk and enact efficient plans to counteract it.

Risk management plays an important role in any bank and ways of business conduct. There are strong relations between risk management, the business strategy, corporate governance and internal control system. Risk management system comprises:

1) Risk management strategy and policies, as well as procedures for risk identification and measurement, i.e. for risk assessment and risk management;

2) Appropriate internal organization, i.e. bank's organizational structure;

3) Effective and efficient risk management process covering all risks the bank is exposed to or may potentially be exposed to in its operations;

4) Adequate internal controls system;

5) Appropriate information system;

6) Adequate process of internal capital adequacy assessment.

Risk Management Identification

The first step of managing operational risk is to identify it. According to Muermann and Oktem (2002), identifying operational risk is especially challenging in banking industry because the operational factors are not well defined. Geiger (2000) suggested using a risk identification matrix (RIM) to identify and segregate operational risk. The causes are used to differentiate the operational from other risks. Operational risks are all unexpected losses, which have their origin in internal errors, or staff related deficiencies in the processes and systems and also in external events.

Risk Management Approaches

Bloom and Galloway (2000) and Allen and Saunders (2002) all agreed that many banks currently adopt a top-down approach, that is using a percentage of their non-interest expenses to calculate their operational risk capital. Fung (2006) indicated that there are a number of drawbacks of this approach. This approach does not truly reflect a bank's risk profile against which the capital is required. It is only a rough estimate of the amount of insurance the bank should be carrying to mitigate the effects of potential exposure to operational risk. It is clear that this top-down approach could no longer meet the real

business needs of banks, which increasingly require a more sophisticated means of assessing and mitigating operational risk. For this reason, some of the banks are switching to a bottom-up approach, which can provide a better approach to risk management. A bottom-up approach evaluates operational risk from the perspective of individual business unit that make up an organization's production process. The advantage of this approach is that it creates a loop so that banks can avoid the worst repercussions of operational failures, such as crisis management and management shake-ups.

Risk Management Measures

When the term operational risk management first came on the scene, there were two distinct schools of thought. One school held the idea that it was not possible to manage something which one could not measure and therefore, they stressed on quantitative tools such as loss distributions, risk indicators and economic models. The other school believed that operational risk could not be quantified effectively and therefore they focused more on humanistic, qualitative approaches, such as self-assessments, risk maps and audit findings. However, very soon, people realized the problems of using only one approach but without the others. The scope of operational risk is measured by the probability and impact of the unexpected losses from a lack of internal control to external event occurrences. Geiger (1999), Muermann and Oktem (2002).

2.2 Operational Risk

The definition of operational risk covers a narrow term of operational failures in processes to an extensive term stating all risks other than credit or market risk. The definition proposed by the Basel committee mainly focused on core business risk of the bank. It specifically categorizes the operational risk based on causing factors such as people, process, system and external. However, many institutions adopted their own definition by accepting Basel definition as base. BCBS (Basel Committee for Banking Supervision) defined that the operational risk is the risk of 'direct and indirect loss' resulting from inadequate or failed internal processes, people or systems or from external events (BCBS Jan 2001). Operational risk is the potential for failure (include the legal component) in relation to employees, contractual specifications and documentations, technology, infrastructure failure and disasters, external influences and customer relationship. (Deutsche bank 2011)

Determinants of Operational Risk Management in Commercial Banks

Operational risk management in banks has been increasingly emphasized in the past decade. Big financial scandals, frauds and information technology system failures are important drivers for the greater attention both inside and outside banking institutions to their exposures to and internal handling of such risk. The exposure to different kinds of operational risk is nothing new for the individual bank. For banks, the occurrence of an extreme and major "one-off event in its daily operations may even be more damaging than its credit losses in connection to the current collapse of the financial markets. However, the ability of the bank to properly assess and control, or hedge itself against, the negative economic consequences of such events seems to be less developed than its management of credit and market risks,(Flores, Ponte & Rodríguez 2006). It is important to indicate that the objective of this sub-section is to consider the current operational risk management practice and related issues in the banking industry and not to any recommendation on which best practices to adopt on managing operational risk within the banking industry.

Managing Operational Risk

Each bank should define their own approach, the extent of the analysis, and which method, either quantitative or qualitative, will be used in the analysis, Davies and Haubenstock (2002). Croupy, Galai and Mark (2001) stated that it was important for a bank to set a clear guiding principle for the operational risk management process which should ensure that it provided an appropriate measure of operational risk across all lines of business throughout the bank.

The process of implementing a sound operational risk management should contain certain stage of development. Davies and Haubenstock (2002) mentioned that good operational risk management needed the support and involvement of senior management who could decide that operational risk was important and deserved attention and the most important point was to allocate resources accordingly. Without their support, operational risk management will be ranked on the last on the list or will be only carry out with the minimum requirement of regulatory body. One important point is that the senior management should play an important role in establishing a corporate environment in which operational risk management can flourish (Croupy, Gala and Mark, 2001).

2.3 Sources of Operational Risk

The fundamental origin of operational risk lies in the conscious and unconscious process. A collective representation of all contributing risk factors helps to achieve the objective of risk management successfully. The sources of risk classification can be done on the basis of direct and indirect losses. Once the main origin of the incident is identified, it is very easy to manage and control any risk.

The primary factors of operational risk are internal (people, process, system) and external factors. Indirect losses are permanent losses of future business due to the events, for example, customers who switch over from an existing one to a rival one. Without any knowledge of the root cause of the operational failure, appropriate control mechanism cannot be placed to reduce the risk. When possible causes of losses are once reviewed and analyzed, it helps to address the issues in a cost effective way. In particular, core areas of operations which may be exposed to business threatening events, which ultimately result in a drastic impact on financial institution as a whole. Effective management of risk resolves the issues and enables an organization to establish sound measures that ensures the benefits and opportunities to be achieved from its operation.

Primary sources of operational risk are people risk, processes risk, systems risks, and external risks. People risks include employee fraud, unauthorized activity misdeed, employment law, workforce disruption and loss or lack of key personnel. Payment, settlement, delivery risk, documentations or contract risk, valuation and pricing, internal and external reporting, compliance, project risk and change management and selling risks are included in processes risks. Systems risk involves technology investment risk, systems development and implementation, system failures, systems security breach and systems capacity. External factors consists of legal, regulatory risk, public liability, criminal activities, outsourcing, supplier risks, insourcing risks, disaster and infrastructural utilities failures, political and government risks.

Operational Risk Events

The above described drivers can be classified on the basis of front of office and back office risk in banks. The intensity and frequency of emergency of risk differ according to size, location, structural complexity and control mechanism of the organization. The primary and secondary sources cause certain events, in that some are controllable and some events are uncontrollable.

Internal fraud - Employees stealing from their company or from company clients are typical internal frauds. This could range from the taking off the office stapler to the misuse of company or client funds. Other forms include employee corruption, deliberate embezzlement of company property, intentional false pricing of inventory or intentionally divulge of security position.

External fraud - This could range from simple robbery to forgery and to the most deceitful computer hacking, identity pilfering and also leaving companies and their prosperous clients to face ill- fated threats.

Processing errors - Losses can occur due to poor or failed transaction processing or poor management of the process. These losses could be due to individual mistakes or due to a poor process itself. Examples of such processing errors are: data entry errors, accounting errors, delivery failures, incomplete legal documentation, illegal access given to client accounts, incomplete or inaccurate client records, client errors, poor communications with clients, vendor or trade supplier errors, incomplete or inaccurate vendor or supplier records etc.

Physical security breaches – Safety in the workplace has become a vital part of both employees and clients. Banks should be properly secured to prevent theft or to prevent unwanted intruders from entering its premises and potentially harming the physical assets or its employees and clients.

System failures - Losses could result from failures in computer hardware, software, telecommunications equipment, etc. Failures of systems that support sales to clients, processing of client or employee transactions, corporate functions, such as accounting, human resources, control and relations with investors or regulators could have a significant effect on its operations.

Disaster recovery and business continuity –Failures like power outages, could produce material losses to an institution. Risk management should be deeply concerned with the institutions ability towards quick and complete recovery from these disasters and ensure continuity of the business front - office and back - office operations.

Inappropriate business practice – The conduct of business affected by any defective products, market manipulation, false publicity and improper sales or trading. Along with that, an organizational failure to develop, execute and conduct basic and sound business practice severely endangers the reputation of a company (Dickstein and Flast, 2008).

2.4 Operational Risk Management in Banks

In the decade since the global financial crisis, banks and their regulators have become increasingly mindful of the need to manage risk. Especially to financial risk and operational risk. Financial risk includes credit risk (the likelihood that borrowers will pay back their loans), market risk (the likelihood that a security will fluctuate in value) and liquidity risk (the ability of a bank to meet its obligations to its depositors and counterparties). Operational risk is the risk of loss due to errors, breaches, interruptions or damages—either intentional or accidental—caused by people, internal processes, systems or external events. Although banks have developed sophisticated systems for controlling financial risk, they still have struggled to deal effectively with operational risk.

Losses from these operational risk episodes can be catastrophic, not just in a strictly monetary sense, but in terms of the impact on the bank's overall business and reputation, sometimes even threatening its very existence. In recent years, banks around the world have been caught up in headline-generating scandals triggered by failures to contain operational risk. From 2011 to 2016, major banks suffered nearly $210 billion in losses from operational risk. Most of these losses stemmed from preventable mistakes made when employees and systems interacted with clients, flaws in the way transactions were processed or outright fraud.

Risk management is not an end in itself, but a key instrument supporting the management in achieving corporate objectives. This applies, in particular, to the management of operational risk. There is a close relation between a company's mission, vision and general strategic orientation, and its willingness to take risk (risk appetite, risk tolerance), risk policy and risk strategy, on the other hand. All these elements have a strong impact on corporate culture, values, opinions and attitudes of employees. It is decisive for the well-balanced interaction of those elements whether the focus is on formal compliance with regulatory requirements or expectations of the capital markets or whether operational risk management is fully embraced by the management and all employees in their day-to-day work.

The top management is responsible for all the risks of the bank as well as for designing and implementing its risk strategy, roles and responsibilities for everyone involves. The clear assignment and definition of roles and responsibilities is important and frequently part of operational risk frameworks. This distribution very strongly depends on the concrete situation in a bank or group and should therefore be carefully coordinated. It

should be reviewed regularly and adjusted to changed circumstances. One of the most important prerequisites for establishing an effective operational risk management system is the support of the top management right from the start. In part, the top management itself takes the initiative in launching a project on operational risk management.

Managing a multitude of internal and external risks is one of the most significant challenges facing any bank. Increasing transaction volumes, and the globalization of business, extended reliance on technology, have introduced higher complexity and uncertainty to banks. In order to maintain a competitive advantage and to improve overall performance, banks are seeking a way to understand and proactively manage the risks that can impact their business. In this respect, it is essential to clearly define the relationship between operational risk processes and the overall control environment.

Banks survive and prosper by accepting risks. 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.

People Risk

People as a source of operational risk. Retail banks on average have more employees than large corporate banks. Main characteristics of operational risk events that are driven from employees' behavior or their work in retail banking include: higher possibility of unintentional errors caused by overtime or tiredness due to the large number of everyday transactions in order to serve large number of clients. During the period of expansion, accompanied with growing number of employees, risk of insufficient training of employees and consequently higher percentage of accidental errors increases.

According to the proposed Basel II matrix, which is adopted by National bank of Serbia, this type of risk event would be categorized as execution, delivery & process management, within business line retail banking, originated by human factor. Inadequate level of control large amount of transactions as it requires high expenses, which can open a room for internal frauds, but also for unintentional errors or failure to meet a professional obligation. In order to mitigate this risk, empirical data shows that banks usually implement following:

1) Determination of time intervals when number of orders reaches peaks;
2) Determination of adequate number of employees for execution volume of transactions;
3) Procedure implementation control;

IT System Risk

Information technology risk, IT risk, IT-related risk, or Cyber Risk is any risk related to information technology. While information has long been appreciated as a valuable and important asset, the rise of the knowledge economy and the Digital Revolution has led to organizations becoming increasingly dependent on information, information processing and especially IT. Various events or incidents that compromise IT in some way can therefore cause adverse impacts on the organization's business processes or mission, ranging from inconsequential to catastrophic in scale.

It is becoming increasingly apparent that information systems and technologies significantly influence business processes in the banking industry. The value of Information System (IS)/ Information Technology (IT) depends widely on the way IS/IT are implemented and related to the banking activities. The IS/IT as such represent an important factor of competitiveness and commercial success of individual financial institutions. IS/IT affect the banking business and its economic results in the following ways:

1) contribution of IS/IT to the business productivity
2) making use of IS/IT as a tool for banking innovations
3) IS/IT as a banking risk mitigating (increasing) factor.

IS/IT risk within a bank's risk management framework should logically result from this definition and from the fact that IS/IT risk forms a significant subset of operational risk, which is attributed in particular to an increasing IS/IT penetration into the banking processes. A large portion of the whole operational risk which falls under IS/IT risk and involves:

1. the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and
2. the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to:
    i) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
    ii) Unintentional errors and omissions
    iii) IT disruptions due to natural or man-made disasters
    iv) Failure to exercise due care and diligence in the implementation and operation of the IT system.

Process Risk

Process risk or internal control risk is the potential for losses related to a business process. It is usually considered a type of operational risk as most processes are part of the day-to-day operations of a business. Operational risk in the banking sector are inherent to the internal processes, and sometimes it can be difficult to differentiate the risk caused by people and those that are due to the failure of the internal processes. Knežević (2013) notes that failures and omissions in the bank's internal operations can be unintentional due to a minor misunderstanding of the process or intentional with the aim of gaining more profits by exposing the institution to higher risks.

A system of effective internal controls is a critical component of bank management and a foundation for the safe and sound operation of banking organizations. A system of strong internal controls can help to ensure that the goals and objectives of a banking organization will be met, that the bank will achieve long-term profitability targets, and maintain reliable financial and managerial reporting. Such a system can also help to ensure that the bank will comply with laws and regulations as well as policies, plans, internal rules and procedures, and decrease the risk of unexpected losses or damage to the bank's reputation.

Overlapping of responsibilities with the bank can lead to a failure in the internal processes. When the employees are not set adequately and adequately, overlapping of duties can happen, and this often leads to omissions and inefficiency during work (Rahim et al., 2017). Other than the unintentional failures within the process, sometimes bank procedures can have loopholes that allow individuals to make personal gains or expose the bank to higher risks than what is expected. If the bank procedures do no cover all aspects of the internal process, there is a high chance of breaches of responsibility by the employees.

The biggest threat in internal processes comes from moral hazard problem, but still it is not identified in that manner. Apart from these, internal processes inadequateness could be present in other processes. Systems of internal and external control are the first measure in mitigating risk inherent in bank processes. Contribution to it comes also from regular monitoring of bank management by shareholders, and monitoring of decentralized organizational structures from top management applying restrictive covenants. By this measure investors can define areas and projects that are prohibited for financing; set rules and conditions for loans disbursements, determine acceptable ratios of liquidity, solvency and loan portfolio quality. Existence of independent operational risk unit within the bank

is of crucial importance for identifying these kinds of risks. Process of risk identification should be more concentrated on analyzing these hidden risks instead of countable high frequency, low severity risk events.

External Risk

External factors, as a source of operational risk are not under bank control. If we exclude catastrophic and events that cause physical damage on bank assets, in retail banking higher exposure to operational risk comes from higher possibilities of clients' frauds and forgeries. In the working environment characterized by high level of corruption, it is easier to forge documentation on clients' financial results as well as issuance of false certificates on their property. In entrepreneurial segment, moral hazard problem is more present in comparison to large enterprises. In addition, entrepreneurs, managers, owners and entrepreneurial personal income is directly dependent on company's income. That is the reason why there is a higher chance that entrepreneur would misuse borrowed funds from the bank and invest them in more risky ventures in order to maximize their own fortune.

Furthermore, entrepreneur tendency to misuse borrowed funds in order to increase own fortune is directly dependent on the companies financing choices [Wu Yan, 2008] and it is higher within those that finance their activity primarily using banking loans i.e. capital structure with higher share of debt to equity ratio. Entrepreneurs follow the well-known economic principle that marginal benefits of effort should equal its marginal cost. Higher debt share in finance structure assumes lower marginal benefit of invested effort of the entrepreneur. And thus, entrepreneurs' motivation for further efforts is reduced and they are more prone to misuse borrowed funds leading to higher indebtedness that increases moral hazard risk to banks even at very high-risk exposure. In this case moral hazard problem is negatively correlated with chosen financing model.

CHAPTER III

OVERVIEW OF RISK MANAGEMENT IN UNITED AMARA BANK

This chapter contains four different parts. The first part describes the profile of United Amara Bank Limited (UAB) including mission, vision, objectives and core value. The second part is about products and services provided by UAB. The third part mentions organization structure of UAB, and the final part explains its established corporate governance practices and procedures.

3.1 Overview of United Amara Bank Limited

United Amara Bank (UAB) was established in 2010 as a fully-fledged Domestic private bank. On 16thAugust 2010, it opened its very first branch in Nay Pyi Taw and the branch network has since grown to 78 branches across Myanmar under five different zones as of August 2018. It is envisaged that the network will further expand to 100 branches by the end of 2020.

A year after its first opening, an Authorized Dealer License was obtained in 2011 allowing the bank to do foreign exchange transactions through its Money Changer Counters, and subsequently on 9th July 2012, a Foreign Banking License was also obtained which enabled the bank to perform foreign banking transactions. UAB is now fully licensed to make International money transfers as well as to issue Letters of Credit (LC). UAB now operates a fully-fledged banking business both in domestic and foreign currencies serving its customers through its branches and electronic platform across Myanmar. As a reflection, UAB received a number of awards during the year 2016 and 2017 recognizing its growing maturity in both domestically and internationally. The mission, vision and objectives of UAB Bank are as follow

Mission

The missions are UAB to become the bank of choice for customers who value personalized high-quality service, building strong customer relationships and trustworthiness as the base of UAB. The bank will also keep on strengthening and building on our customers, stakeholders and partners trust by building relationships giving those sound solutions that combine the highest level of banking expertise, technology and financial security.

Vision

The name of United Amara Bank Limited represents the bank's vision, which is to be the leading customer centric bank built on safe, sound and trustworthy principles.

Objectives

The objectives of the United Amara Bank Limited are:

1. To provide excellent professional services and improve its position as a leader in the field of financial related services
2. To build and maintain a team of motivated and committed workforce with high work ethos
3. To use the latest technology aimed at customer satisfaction and act as an effective catalyst for socio-economic developments

Products and Services Provided by United Amara Bank

United Amara Bank (UAB) is one of the top ten banks in Myanmar Banking Industry. The bank aim is to provide as many financial services as possible for the convenience and satisfaction of bank's customers. Followings are the list of the products and services provided by the bank:

1. Corporate Banking Services
2. Retail Banking Services
3. Trade Finance Services
4. Electronic Services
5. The corporate banking services
6. Retail banking services
7. Foreign exchange services

Organizational Structure of United Amara Bank Limited

UAB has a proper organization structure which is started below. The Board of Directors sits on the very top of the organization chart which directly appointed to Advisor of the Chairman. Advisor of Chairman is supported by one Deputy Chief Executive Officer and one Executive Director in second tier who are in-charge of different departments. The bank's Management Board contain of (10 – 16) members.

The bank Chairman is U Nay Aung, Four Board of Directors, six committees, one advisor to Chairman, one Deputy Chief Executive Officer, and eleven head of departments, such as: Corporate Banking Department, UAB Securities, Trade Finance Department,

Treasury & FI Department, Retail Banking Department, Internal Audit Department, Finance Department, Credit Management Department, Human Resource Department, Risk and Compliance Department, and Administration Department. The numbers of Bank's staff reached total of over (2500) at the end of March 2018.

In East Yangon Zone, there are twenty-one branches which are located in East of Yangon region. West Yangon zone, there are twenty-four branches which are residence in West of Yangon. Mandalay zone has sixteen branches. Upper Myanmar zone has twelve branches and lower Myanmar zone has five branches. The detail list of the branches by zone-wise will show in (Table 3.1).

Table (3.1) Zone-wise by Branch Total

Sr	Zone	Branches
1	East Yangon Zone	21
2	West Yangon Zone	24
3	Mandalay	16
4	Upper Myanmar	12
5	Lower Myanmar	5

Source: www.unitedamarabank.com

Head of the departments such as Treasury department, finance department, credit management department, Internal Audit department and legal department involved in Assets Liability Management Committee, Audit Committee, and Credit Management Committee which are holding the meeting weekly to monitoring the ongoing activities such as liquidity surplus or deficit as well as ongoing loan cases.

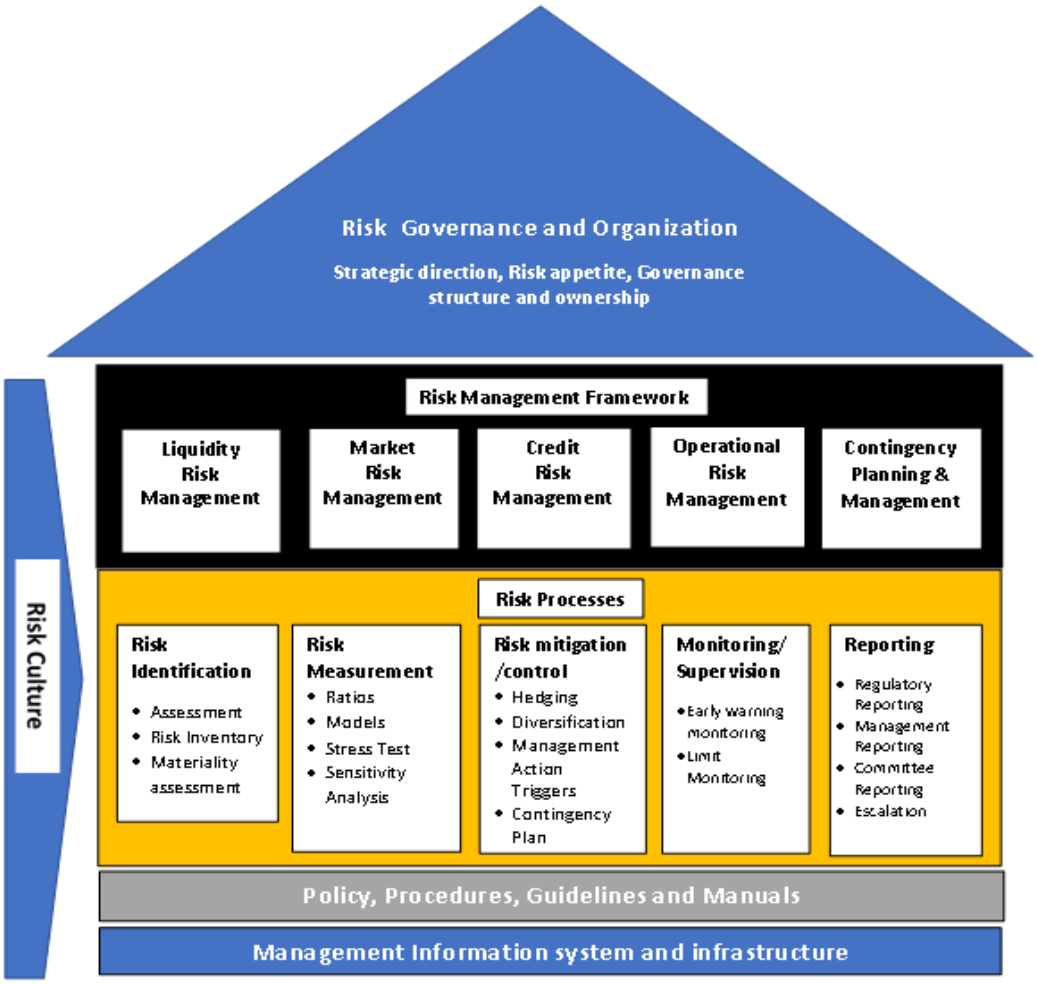
3.2 Risk Management in United Amara Bank

UAB's risk governance and management structure is illustrated in the following diagram and it is designed to ensure that appropriate risk management and governance is accorded to the bank.

According to Figure (3.1), risk is managed within the levels established by the Senior Management and approved by the Board of Directors. Various sub-committees

within the bank govern and monitor the risk levels at the bank and ensure that it operates within the levels established. Within the Risk Management Framework, the bank ensures that all key risk elements are categorized and sufficiently robust contingency planning is appropriated. Processes are put in place to identify, measure, mitigate and monitor risk. Reports are made to various management and board committees and a process for escalation is available where risk levels require such escalation. Policies, procedures, guidelines and manuals are issued and a Management Information System which is sufficiently robust provides support to risk governance. The overarching influence within the Risk Management Framework is the Risk Culture and this is the set of encouraged and accepted behavior towards taking and managing risk. The Board and Management sets the tone for UAB's risk culture in its deliberations, managers' conferences, training programs and written statements.

Figure (3.1) Structure of Risk Governance and Organization of UAB Bank



Source : United Amara Bank Website

UAB bank are literally exposed to many different types of risks. A successful banker is one that can mitigate these risks and create significant returns for the shareholders on a consistent basis. Mitigation of risks begins by first correctly identifying the risks, why they arise and what damage can they cause. There are five types of major risks that are faced by UAB bank. They are liquidity risk management, market risk management, credit risk management, operational risk management, operational risk management, contingency planning and management.

Liquidity Risk Management

Liquidity risk management is the risk that arises from funding of long-term assets by short-term liabilities, thereby making the liabilities subject to rollover or refinancing risk. Liquidity risk is usually of an individual nature, but in certain situations may compromise the liquidity of the financial system. As in overall terms it is about a situation that is very dependent on the individual characteristics of each financial institution, defining the liquidity policy is the primary responsibility of each bank, in terms of the way it operates and its specialization. Liquidity is the ability to efficiently accommodate deposit as also reduction in liabilities and to fund the loan growth and possible funding of the off-balance sheet claims.

Liquidity risk can be sub-divided into funding liquidity risk and asset liquidity risk. Asset liquidity risk designates the exposure to loss consequent upon being unable to effect a transaction at current market prices due to either relative position size or a temporary drying up of markets. Funding liquidity risk designates the exposure to loss if an institution is unable to meet its cash needs. This can create various problems, such as failure to meet margin calls or capital withdrawal requests, comply with collateral requirements or achieve rollover of debt.

Market Risk Management

Market risk refers to the risk of losses in the bank's trading book due to changes in equity prices, interest rates, credit spreads, foreign-exchange rates, commodity prices, and other indicators whose values are set in a public market. To manage market risk, banks deploy a number of highly sophisticated mathematical and statistical techniques. Chief among these is value-at-risk (VAR) analysis, which over the past 15 years has become established as the industry and regulatory standard in measuring market risk. To set up limits, various factors are taken into account, including business strategies, historical limit

usage ratios, risk–bearing capacity (profits, equity capital, and risk management framework), profit targets and the market liquidity of the products involved. The limits are discussed and coordinated by the Risk Management Committee, discussed further by the Risk Management Committee and then determined by top level management. To provide a system of mutual checks and balances in market operations, UAB has established middle offices specializing in risk management that are independent of front offices which engage in market transactions and of back offices which are responsible for book entries and settlements.

Credit Risk Management

In general, when UAB Bank grants loans to individuals and legal entities, the credit risk involved is characterized by the following quantitative parameters: risk as the probability of the borrower's failure to repay the loan; acceptable risk; average risk; possible losses given loan default; the average value of losses; the maximum allowable losses; the number of loans given by the bank; the possible number of different loans the bank can give; the number of problem loans. The management of credit risk of credit portfolios is therefore one the most important tasks for the financial liquidity and stability of banking sector in connection with increased sensitivity of banks to the credit risks and changes in the development of prices of financial instruments (Kiseľáková and Kiseľák, 2013). The most significant impact on performance of the enterprise has just financial risk. The unsystematic risks have a higher impact on performance of the enterprise as systematic risks (Kiseľáková et al., 2015).

Operational Risk Management

Operational risk is the risk of possible adverse effects on the bank's financial result and capital caused by omissions (unintentional and intentional) in employees' work, inadequate internal procedures and processes, inadequate management of information and other systems, as well as by unforeseeable external events. Operational risk also includes legal risk which is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events defined by Bales Committee. This definition includes legal risk but excludes strategic and reputational risk. Operational risk occurs as the result of a failed business processes in the bank's day to day activities. This risk may be increased by poor training, inadequate controls, poor staffing resources, or other factors.

Contingency Planning and Management

UAB Bank have in place contingency and business continuity plans to ensure their ability to operate as going concerns and minimize losses in the event of severe business disruption. Institutions should have a mechanism to identify stress situations ahead of time and plans to deal with such unusual situations in a timely and effective manner. Stress situations to which this principle applies include all risks of all types. For instance contingency planning activities include disaster recovery planning, public relations damage control, litigation strategy, responding to regulatory criticism etc. Contingency plans should be reviewed regularly to ensure they encompass reasonably probable events that could impact the organization. Plans should be tested as to the appropriateness of responses, escalation and communication channels and the impact on other parts of the institution. In order to develop a comprehensive liquidity risk management framework, institutions should have way out plans for stress scenarios.

Contingency Funding Plan (CFP) is a set of policies and procedures that serves as a blue print for a timely manner and at a reasonable cost. A CFP is a projection of future cash flows and funding sources of a bank under market scenarios including aggressive asset growth or rapid liability erosion. To be effective it is important that a CFP should represent management's best estimate of balance sheet changes that may result from a liquidity or credit event. A CFP can provide a useful framework for managing liquidity risk both short term and in the long term. Further it helps ensure that a financial institution can prudently and efficiently manage routine and extraordinary fluctuations in liquidity. The scope of the CFP is discussed in more detail below.

3.3 Risk Management Committee in United Amara Bank

The success and growth of banking business mainly depends on the issue of qualified credit on the deposits lodged with the Banks. It is also considered single biggest revenue contributor toward the bank. The committee's prudent practices are on accessing and analyzing credit has led the bank to withstand the bank crises over the last two decades. It is the duty of this committee to monitor the risk exposure, profile against risk limits and risk strategy in accordance with approved risk appetite.

The committee regularly schedules board meetings to discuss sizable credit applications and set our guidelines to mitigate potential risks. Additionally, the committee closely monitors market development, such as macroeconomic, credit industry risk in order to well position the bank of these developments. Risk management generally encompasses

the process of identifying risks to the bank, measuring exposures to those risks, ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions.

Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. The committee is seeing sound operational risk governance practices adopted in an increasing number of banks. Common industry practice for sound operational risk governance often relies on three lines of defense

(1) business line management

(2) an independent corporate operational risk management function and

(3) an independent review.

In all cases, a bank's operational risk governance function should be fully integrated into the bank's overall risk management governance structure. Organizations need to utilize risk management and control to mitigate any unexpected losses that may arise from unwanted events. The management should be aware of the procedures for identification and management of risks. Internal control is among the core principals of managing risks and companies need to get it right. (Zheng, 2012)

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 professionals 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 should develop implement and maintain a framework that is fully integrated into the bank's overall risk management processes.

3.4 Influencing Factors on Operational Risk Management in United Amara Bank

Definitions of operational risk goes from the broadest that describe it as all risks that are not originated by market or credit risk to the most used Basel II definition. According to it, operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems and from external events.

People Risk

In UAB Bank, main characteristics of operational risk events that are driven from employees' behavior or their work in retail banking. In order to mitigate this risk, empirical data shows that banks usually implement following:

1. Determination of time intervals when number of orders reaches peaks;
2. Determination of adequate number of employees for execution volume of transactions;
3. Procedure implementation control;
4. Individual productivity control;
5. Promoting e-banking transactions.

One of the methods for mitigation risk of internal frauds is more strict internal controls which have benefits both for detecting internal as well as external frauds and forgeries from clients. It includes checking of credit documentation, client visits and rechecking their financial performances.

Process Risk

In UAB Bank, processes risk which includes internal and external processes and procedures are the most difficult driver of operational risk. Operational risk inherent to internal processes and procedures is hard to distinguish from the risks that result from people because they actually create them. Failures and omissions in processes could be unintentional due to misunderstanding of process essence or intentional with the aim of acquiring more profit by exposing institution to higher risks which is the result of moral hazard.

Systems of internal and external control are the first measure in mitigating risk inherent in bank processes. These are controlled by following factors:

1. Regular monitoring of bank management by shareholders, and monitoring of decentralized organizational structures from top management;
2. Applying restrictive covenants. By this measure investor can define areas and projects that are prohibited for financing; set rules and conditions for loans disbursements, determine acceptable ratios of liquidity, solvency and loan portfolio quality. It is important that proscribed covenants do not include short term profitability requirements, but the ones that support long-term sustainable stable business results of the institution. Profitability indicators directly support moral hazard problem. Faced with high profit targets, managers could be more prone to more risky activities in order to achieve personal gains.

3. Existence of independent operational risk unit within the bank is of crucial importance for identifying these kinds of risks. Process of risk identification should be more concentrated on analyzing these hidden risks instead of countable high frequency, low severity risk events.

Technology Risk

There are four fundamental forces involved in risk management of UAB Bank, which also apply to cyber security. These are assets, impact, threats, and likelihood. UAB Bank has internal knowledge of and a fair amount of control over assets, which are tangible and intangible things that have value. UAB Bank also have some control over impact, which refers to loss of, or damage to, an asset. However, threats that represent adversaries and their methods of attack are external to UAB Bank's control. Likelihood is the wild card in the bunch. Likelihoods determine if and when a threat will materialize, succeed, and do damage. While never fully under bank control, likelihoods can be shaped and influenced to manage the risk.

The implementation of IT in banks can lead to challenges in the workflow, policies or procedures and this ultimately led to risks. IT system problems are majorly caused by Cyber- attacks, viruses and other failures and this result in significant issues that affect the whole system. Because of this, technology and system risk can be classified as the risk of loss due to imperfect systems in banks. Moreover, such imperfection includes inappropriate data processing, lack of system capacity, and poor quality of data or using low technology. Therefore, UAB assumed that using an effecting IT system together with- IT security leads to successful management of IT-related risks in an organization.

External Risk

There are three steps to control external event risks in UAB bank. These are as follows.

1. To build an effective operational risk management (ORM) capability which is required to fully assess the bank's existing risk profile
2. To construct a database
3. To construct a map of all internal and external OR risk events.

Purely external risk events include natural hazards, both environmental and weather influenced. A natural disaster is a grave event caused by the components in the terrestrial, atmospheric, or terrestrial atmosphere affecting the business operation that is capable of causing losses to human life and or property and which, due to the extent of damage, is improbable to be fully accomplished by the enterprise itself. Nevertheless, it is likely and

necessary to design measures in this field to ensure safety of employees and clients affected by the risk.

For the time being, the highest threats are coming from external events that are not controllable. However, single institutions cannot do much in mitigating these risks. In order to mitigate them, joint actions of all participants in the market are needed. One of the possible solutions could be exchange of risk events data between banks within the same system and forming so called black lists of clients. As banks are not reluctant to share in house information, of key importance is the role of regulator that could be kind of intermediary, at least in first phases.

CHAPTER IV
ANALYSIS ON EXTENT OF TYPES OF OPERATIONAL RISK PRACTICES IN UNITED AMARA BANK

In this chapter, findings from analysis of data from survey are presented with thee sub-sections. The first one is to ask about demographic information, the second are include 19 statement questionnaires which ask UAB Bank organization. Three levels top-level, middle level and staff level, third one ask UAB bank organization include 6 statement questionnaires which ask internal operation risk management, which item was rated on a 5-point Likert scale, ranging from "1" indicated "strongly disagree to "5" indicated "strongly agree".

4.1 Demographic Information

Demographic information of the respondents consists of gender, age, education, occupation, income level, job experience and utilizes risk management practices.

4.1.1 Gender of Respondents

The selected sample of the 140 UAB employees are categorized by their gender and this is shown in the following table (4.1).

Table (4.1) Gender of Respondents

Gender	No. of Respondents	Percent
Male	40	28.6
Female	100	71.4
Total	140	100.0

Source: Survey Data (2018)

In table (4.1) shows a gender profile of the respondents as a percentage of totals. It should be noted that the gender of the respondents is 71.4% of the replies being from female and 28.6% respondent by males. Therefore, it found during the distribution of the questionnaires which female respondents tend to be more concerned about survey and interested in the UAB bank.

4.1.2 Age Group Respondents

The age of the UAB's employees are grouped into three classes which are under 20 years, 20 years to 39 years, and 40 years to 59 years. These data are shown in the following table (4.2).

According to the table (4.2), respondents in the age group 20-29 years of age category represent 67.86% which is the largest age group of the all replies. The 40-59 years of age grouping respondents at 31.43%, the age group of the under 20 years old represents the smallest number of replies at 0.01%. So based on the sample data, it can say that majority staff of society in UAB bank.

Table (4.2) Age Group Respondents

Age	No. of Respondents	Percent
Under 20	1	0.01
20-39	95	67.86
40-59	44	31.43
Total	140	100.00

Source: Survey Data (2018)

4.1.3 Education Level of Respondents

The selected sample of UAB bank employees are asked about their educational level of attainment and the results are classified in the table (4.3).

Table (4.3) Education Level of Respondents

Education Level	No. of Respondents	Percent
Graduate	108	77.1
Post Graduate	18	12.9
Master Degree	14	10.0
Total	140	100.0

Source: Survey Data (2018)

With regard to the level of education as table (4.3) provides the largest segment of the respondents at 77.1% have graduate, followed by post graduate of the respondents at 12.9% and master degree of the respondents is 10%, which is the smallest group. So that most of the UAB employees are graduate.

4.1.4 Level of Management Respondents

There are four level of management of the respondents such as staff, middle level and top level. These data are described in the table (4.4).

From the level of management respondents classified by three categories, the largest proportion were employees in the staff level about 55%, middle level about 32.1%, and top level management of 12.9%.

Table (4.4) Level of Management Respondents

Level Of Management	No. of Respondents	Percent
Staff	77	55.0
Middle Level	45	32.1
Top Level	18	12.9
Total	140	100.0

Source: Survey Data (2018)

4.1.5 Monthly Income Level of Respondents

There are three levels of monthly income described in the table (4.5).

Table (4.5) Monthly Income Level of Respondents

Money Income	No. of Respondents	Percent
200,000-500,000	65	46.4
500,000-1,000,000	57	40.7
Above 1,000,000	18	12.9
Total	140	100.0

Source: Survey Data (2018)

The data on level of income show in table (4.5) indicates that the respondents whose monthly earning Kyats 200,000-500,000 income represent the largest group respondents of 46.4%, monthly earning Kyats 500,000-1,000,000 income are second largest of 40.7% and Kyats above 1,000,000 incomes are smallest which represents 12.9%.

4.1.6 Experiences of Respondents

There are three level of experiences respondents work at UAB

Table (4.6) Experiences of Respondents

Experiences	No. of Respondents	Percent
1 to 3 years	21	15.0
4 to 6 years	60	42.9
7 years and over	59	42.1
Total	140	100.0

Source: Survey Data (2018)

As shown in table (4.6), respondents in the 4 to 6 years of experience segment represent 42.9% which is the largest sample group of respondents. The second largest group of respondents is 7 years and over, holding 42.1% and the smallest group of respondents is

1 to 3 years experiences at 15%. Therefore UAB bank has well experience staffs in their organization.

4.2 Operational Risk Management Practices Utilization

In this section, the utilization of practices on operational risk management were asked with Likert scale with five level of agreements and the result is as shown in Table (4.7).

Table (4.7) Operational Risk Management Practices Utilization

Operational Risk Management Practices	No. of Respondents	Percent
Strongly Disagree	1	0.7
Disagree	6	4.3
Agree	107	76.4
Strongly Agree	26	18.6
Total	140	100.0

Source: Survey Data (2018)

According to the Table (4.7), operational risk management practices are fairly utilized by 76.4% of respondents while 18.6% were fully utilized. However, the rest 4.3% of respondents were not really utilized such practices and the rest 0.7% were not utilized at all. As per the result in the Table (4.7), UAB bank fairly utilizes the practices on operational risk management.

4.3 Internal Operational Risk Management Practices

While the research obtained data relevant with internal risk management practices using a likert scale, the respondents were asked to indicate their perception on people risk, process enabler and system risk. Therefore, this sections analyzed on the source of risk such as process risk, people risk, system risk and external events risk.

Operational risk is the exposure of a bank to possible losses resulting from inadequacy and failure in the execution of its operations. This definition firstly comprises the main underlying operational risk factors namely people, processes and systems as internal operational risk management and the others are external risk management.

Internal risk management factors are based on people, process and system in UAB bank. The success of a business is dependent on the knowledge, skill and capability of the persons involved in all of the business processes. Operations manual includes policies and procedures for the concerned business and a support unit comprises of the key operational

controls to mitigate the key operational risks from the process/ function. Further, any proposed mitigation plans for key risks are reviewed by the Risk management division, the Human Resources Management Division, the Head of Audit and the Head of Compliance before escalation to the senior management and incorporating the same in the operations manual of the concerned business and support unit. Implementation of the existing and proposed policies and procedures are monitored by the operations group along with audit and compliance divisions.

4.3.1 People Risk

This section analyzed the practices of respondents which could be the source of people risk. To control such risk, the employees of UAB bank must have necessary skills along with ethical behaviors. At the same time, they must comply bank policies accordingly and should not intended supervisory responsibility abuse. Moreover, the employee recording on their honesty and dishonesty attitudes is necessary and wide diversity of employee is important.

Table (4.8) People Risk

People Risk	Mean	Standard Deviation
Employees at UAB bank have the necessary skills to perform their work effectively	3.95	0.723
Employees at UAB bank possess ethical behavior necessary to mitigate the bank against people risk	3.74	0.792
Staffs comply with policy requirement of the bank	3.08	0.945
The bank has recorded cases of dishonesty and honesty among its employees	3.69	0.839
Some official with a supervisory responsibility abuse it for their personal benefit	3.10	0.999
UAB bank has a wide diversity of employees in the working environment	3.84	0.761
Average Mean Value	3.57	0.84

Source: Survey Data (2018)

In Table (4.8), people risk which relates to employees at UAB bank have the necessary skills to perform their work effectively was ranked as highest ranking (M=3.95)

while the questions that related to staffs who comply with policy requirement of the bank that leads people risk with sound ranking (M=3.08). However, as per survey result, all of the employees have necessary skills, ethical behavior for their work effectively and banks have recorded cases of dishonesty and honesty, supervisory responsibility abuse for their personal benefit and a wide diversity of employees in the working environment. Table (4.8) shows internal risk factor of people risk classified with six categories. The average mean value 3.57 and standard deviation 0.84 can be concluded that UAB bank's practices used to mitigate people risk are faired and they are neutral level for people risks factors of UAB bank. Therefore, UAB bank has to emphasis on policy requirement for staffs to comply with regulations.

4.3.2 Internal Risk Factors of Process Enabler

This section is aiming to analyze internal risk factors of process enabler by identifying five categories such as their procedural design, handling on hardware and software issue, business integration degree for respective objectives, acceptance of accountability and responsibility for business processes and evaluations of new and existing procedures at their development phase of UAB bank.

Table (4.9) Process Risk Factors of UAB Bank

Process Enabler	Mean	Standard Deviation
UAB bank has design weakness in some procedures.	3.25	0.711
UAB bank has experienced unreliable hardware and software issues	3.08	1.039
UAB bank had dependent processes not integrating to the degree for a business unit to achieve its objectives	3.04	0.821
UAB bank has clear acceptance of accountability or responsibility for business process	2.85	1.031
The evaluations of new processes or changes to existing processes are not exercised at the development phase	3.06	0.812
Average Mean Value	3.06	0.88

Source: Survey Data (2018)

According to Table (4.9), processes risk which relates to UAB bank has witnessed cases of design weakness in some of its processes was ranked as highest ranking (M=3.25)

while the questions that relates to reliable hardware and software, dependent processes which is not integrating to the degree to achieve its objectives and lack of evaluations of new processes to existing processes were ranked with ranking (M=3.08, M=3.04 and M=3.06) respectively. Although mean value for clear acceptance of accountability for business process was ranked at lowest M=2.85. Average mean value is 3.06 that are around the neutral level and UAB bank has to weight all risk categories by emphasizing more on clear acceptance of accountability and responsibility to mitigate process risk.

4.3.3 Internal Risk Management factors of system

The following Table (4.10) internal risk management factors of system classified by system disruption, security measures, Information Technology and system auditing, functionality and disastrous events of UAB bank.

Table (4.10) System Risk

System Risk	Mean	Standard Deviation
UAB bank experienced system disruptions which have interrupted business	3.17	0.905
Reasonable security measures have been put in place to prevent unauthorized access to the banks network	3.59	0.749
Staffs are given good practice guidance on password security	3.88	0.829
UAB bank has suffered financial losses from acts of IT related risks	3.11	0.990
Internal Audit Department regularly conducts IT system auditing.	3.65	0.856
The volume of transactions consistently operates with the technology's ability to deliver	3.46	0.781
Functionality of system has been aligned with business objectives	3.03	0.848
UAB bank has experienced cases of disastrous events that have caused damage to the bank resources	3.21	0.888
Average Mean Value	3.39	0.86

Source: Survey Data (2018)

From the table (4.10) shown, all of the mean values are greater than norm mean 3.0. Especially staffs are given good practice guidance on pass word security mean value is 3.88 and standard deviation is 0.829. The average mean value is 3.39 and standard deviation is 0.06. As per Table (4.10), system risk which relates to employees at UAB bank have good practice guidance on password security was ranked as highest ranking (M=3.88) while the questions that relates to system which functionality of system have not been aligned with business objective was ranked with lowest ranking (M=3.03).

However, according to above table, all IT system from UAB have well-experienced system developer, well-controlled financial losses from acts of IT related risks, reasonable security system, systematic internal audit department, well-controlled for transactions volume and well-planned disastrous events that have caused damage to the bank resources. Due to the inappropriate functionality of system with business objectives, UAB bank need to consider to align system function to match with their business objectives.

The following Table (4.11) shows internal risk factors of people risk, system risk and process risk analysis. Total average mean value is 3.34 and standard deviation is 0.86 greater than norm mean 3.0. Overall internal risk management in employees of UAB bank are faired.

Table (4.11) Analysis of Internal Risk Management Factors

Factor	Mean	Standard Deviation
People	3.57	0.84
Process	3.06	0.86
System	3.39	0.88
Average	3.34	0.86

Source: Survey Data (2018)

4.4 External Operational Risk Management Practices

The research obtained data on the effectiveness of external operational risk management practices using a likert scale, the respondents were asked to indicate their perception about effectiveness of external operational risk management practices.

The external operational risk management practices are considered based on: Regulatory requirement, customer preferences, external factors and business growth.

Table (4.12) External Risk

External Risk	Mean	Standard Deviation
Some cooperating banks' clients comply with contractual arrangements	2.96	1.045
UAB bank clients and counterparties deliver to the expected or contracted level of service	2.92	0.823
Changes/restrictions in the regulatory environment have a significant impact on the bank	3.55	0.916
UAB bank has suffered financial losses from acts of regulatory body	3.04	1.062
Some Actions of countries or governments impacts on the business directly or indirectly	3.76	0.836
Developments in the economy & financial markets have had a negative impact on the company	3.08	1.194
Average Mean Value	3.22	0.97

Source: Survey Data (2018)

As regards with Table (4.12), external risk that influences on operational risk is delivery of clients and counterparties of the bank to expected contractual level of services as lowest ranking (M=2.92) while the questions that relates to government actions which can impacts on the business was ranked with highest ranking (M=3.76). As per result in Table (4.12), overall mean score is 3.22 and some regulatory restriction environment changes and development in the economy and financial market are uncontrollable factors and which can influence to the business in a way of negative or positive impact.

CHAPTER V

CONCLUSION

This chapter presents the summary and discussions on the findings of this study as well as explanations and importance to related literature. This chapter dissects the practices of the results to the field of risk management, the conclusion and the recommendation sections are presented as per the research questions.

5.1 Findings and Discussions

The purpose of this study was to investigate operational risk practices at United Amara Bank (UAB). The research was guide by the following objectives: To identify the risk management practices in United Amara Bank, to analyze the extent of the types of operational risk practices in United Amara Bank. The target population of this study was UAB employees in the 20 UAB Bank branches in Yangon. The data obtained was analyzed through SPSS. Both qualitative and quantitative were analyzed and the results presented in percentages, means, standard deviations and frequencies.

The researcher distributed 140 questionnaires and on analysis of the demographic factors, majority of the respondents have been working at UAB Bank in duration between 4-6 years. Most of the respondents were staff and most of the employees have already finished their bachelor graduation.in addition, most of the respondents agree that they utilize operation risk management.

The first objective of the study was to identify the risk management practices in UAB Bank. The finding established that UAB Bank have in place contingency and business continuity plans to ensure their ability to operate as going concerns and minimize losses in the event of severe business disruption. The committee of UAB Bank regularly schedules board meetings to discuss sizable credit applications and set their guidelines to mitigate potential risks. Internal controls are typically embedded in a bank's day to day business and also designed to ensure, to the extent possible that bank activities are efficient and effective. Therefore, internal control is among the core principles of managing risks and companies need to get it right.

The second objective of the study was to analyze the extent of the types of operational risk practices at UAB Bank. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems and external factors. Therefore, the internal and external factors effect on operational risk. First for the internal factors,

people risk is the most influencing factor on operational risk because the mean score is the highest ranking among three factors. The findings established that most employees have the necessary skills to perform their work effectively and have a wide diversity of employees in the working environment. Most of the respondents sometimes denied to comply with policy requirement of the bank that leads people risk with lowest ranking.

For the external factors, most clients comply with contractual arrangements while most of the respondents are uncertain whether clients and counterparties do not deliver to the expected or contracted level of service. Most of the respondents agree that changes/restrictions in the significant impact on the bank. However, most of the respondents were uncertain of UAB Bank having experienced negative reposting and that negative effects of developments in the economy and financial markets have been experienced. For the influencing factors on operational risk, internal factors are more influencing on operational risk.

The four important factors of on operational risk practices are organizational structuring and design, communication, organizational culture and trust. These factors are managed based upon these factors including people, process, system and external to achieve the organizational goals. The respondents replied all factors which are essential to achieve the operational risk management system internally and externally. Based on the questionnaires, the majority of respondents accept commitment and support from top level management is the most significant facts of critical success factors of operational risk management. Without top management commitment, the policies are not improved.

5.2 Suggestion and Recommendation

For any organization to perform well, there need to be a sufficient work force to deliver the objectives. The study established that most of the respondents agree that UAB Bank utilize operational risk management.

The study established that most of the employees at UAB Bank have the necessary skills, and ethical behaviors to perform their work effectively. Very few employees of the institutions are aware of any deliberate actions taken that have resulted in losses. Despite this, the bank has experienced system risk interruptions. However, reasonable security measures and good practices guidance have been put in place and are aligned with business objectives. Just like any business the changes and restrictions in the regulatory environment, initiatives of competitors, country policies and governments have an impact on the financial sector.

The effective management practices of risk is critical for the bank's survival. The risk management goal is to maximize the operational capability of the bank, ensuring an efficient use of resources, valuating the existing opportunities and maximizing the gain. To reach this goal it is necessary to have a good and profound understanding of the existing risks, to implement an efficient internal control system in order to prevent or mitigate the risks.

People are as a source of operational risk. Retail banks on average have more employees than large corporate banks. In order to mitigate this risk, UAB Bank should determine adequate number of employees for execution volume of transactions, support sufficient training for employees. Therefore, employees will have more skills to perform the work effectively. Process risk, day-to-day operations of a business, is the potential for losses related to business process. Therefore, a system of effective internal controls can help to ensure the goals and objectives of a banking organization will be met, achieve long-term profitability targets, maintain reliable financial and managerial reporting.

It is becoming increasingly apparent that information systems and technologies significantly influence business process in the banking industry. Overall, for the internal factors on operation risk, at UAB Bank there is a need for the institution to establish communication channels to enable employees become aware of any cases of losses resulting from deliberate employee actions and dishonesty. For the external factors, from the finding, majority of the respondents agree that changes/ restrictions in the regulatory environment affect UAB Bank, it is therefore important for the firm to adhere to the set rules by the governing body. In addition, the institution should seek an innovative team capable of creating products and making the firm a market leader in product innovation.

5.3 Needs for Further Research

The study only focused on the evaluation of the banks operational risk practices in restriction internal and external operational risk. It is recommended that other studies should be done to determine how operational risk management affect liquidity of the organization. The study also only focused on one bank and therefore these results are skewed towards the perception and data from UAB Bank. It is suggested therefore that such a study should be done in other banks to increase the statistical power of the study and make the results more reliable.

REFERENCES

1. Albania.Tirana : Operational Risk Management-Best Practice Overview and Implementation (Sep 2012)
2. Aloqab.Abdullah : Operational Risk Management in Financial Institutions (Feb 2018)
3. Blunden.Tony : Operational Risk (Jan 2018)
4. Chalupka.Radovan, Teplý.Petr : Operational Risk Management and Implications for Bank's Economic Capital (Sep 2008)
5. Cole.Roger, Christine.Cumming : Operational Risk Management (Sep 1998)
6. Coleman.Rodney : Operational Risk (Jan 2011)
7. Gangreddiwar.Aboli : 8 Risks in the Banking Industry Faced by Every Bank (Sep 2015)
8. Ghosh.Amalendu : Managing Risks in Commercial and Retail Banking (Feb 2012)
9. Huber.J.Alex, Funaro.D (Jul 2018) : How Banks Can Manage Operagtional Risk?
10. Hussiny.Shaima Al : A study of Risk Management in the United Arab Emirates Banking Industry
11. Marija1.Knežević : Operational Risk – Challenges for Banking Industry (May 2013)
12. Mundra.S S : Information technology and cyber risk in banking sector - the emerging fault lines (Sep 2016)
13. Na Ranong.Prapawadee, Phuenngam.Wariya (May 2009) : Critical Success Factors for effective risk management procedures in financial industries
14. Risk Management Operation Procedure from National Bank of Serbia : Risk Management in Banking
15. Srinivas.Val : Bank board risk governance
16. Stanciu.Victoria : Managing Operational Risk in Banks
17. Svat'a.Vlasta, Fleischman.Martin : IS/ IT Risk Management in Banking Industry (Mar 2011)
18. Vienna (Aug 2006) : Operational Risk Management
19. Willis New Zealand Ltd : People Risk (https://www.willisgroup.co.nz)

Yangon University of Economics

Department of Commerce

Master of Banking and Finance Programme

Questionnaire for Operational Risk Practices in UAB Bank

This questionnaire is for my MBF Thesis about Operational Risk Practices in UAB Bank, please kindly answer the following questions. Thank you very much for your valuable time.

SECTION A: DEMOGRAPHIC INFORMATION

Please tick "√" a mark to indicate your answer.

1. Gender

Male ☐ Female ☐

2. Age

Under 20 years ☐ 40 – 59 years ☐

20 – 39 years ☐ 60 years and above ☐

3. Education

Graduate ☐ Post Graduate ☐

Others ☐ Master Degree ☐

4. Occupation

Staff ☐ Top level ☐

Middle level

5. Monthly income

Under 200,000 ☐ 500,000 – 1,000,000 ☐

200,000 – 500,000 ☐ Above 1,000,000 ☐

6. How long have you been employed in the organization?

a) 1 to 3 years ☐

b) 4 to 6 years ☐

c) 7 years and over ☐

7. UAB bank utilizes Operational Risk Management practices.

Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree ☐

SECTION B: EFFECTIVENESS OF INTERNAL OPERATIONAL RISK PRACTICES AT UAB BANK.

Five likert scale: 1: Strongly Disagree 2: Disagree 3: Neutral 4: Agree 5: Strongly Agree

	PEOPLE RISK	**1**	**2**	**3**	**4**	**5**
1	Employees at UAB Bank have the necessary skills to perform their work effectively.					
2	Employees at UAB Bank possess ethical behavior necessary to mitigate the bank against people risk.					
3	Staffs comply with policy requirement of the Bank.					
4	The bank has recorded cases of dishonesty and honesty among its employees.					
5	Some officials with a supervisory responsibility abuse it for their personal benefit.					
6	UAB bank has a wide diversity of employees in the working environment.					
	PROCESS ENABLERS	**1**	**2**	**3**	**4**	**5**
7	UAB bank has design weakness in some procedures.					
8	UAB Bank has experienced unreliable hardware and software issues.					
9	UAB bank had dependent processes not integrating to the degree for a business unit to achieve its objectives					
10	UAB Bank has clear acceptance of accountability or responsibility for business process.					
11	The evaluations of new processes or changes to existing processes are not exercised at the development phase					

	SYSTEM RISK	1	2	3	4	5
12	UAB Bank experienced system disruptions which have interrupted business.					
13	Reasonable security measures have been put in place to prevent unauthorized access to the banks network.					
14	Staffs are given good practice guidance on password security.					
15	UAB Bank has suffered financial losses from acts of IT related risks.					
16	Internal Audit Department regularly conducts IT system auditing.					
17	The volume of transactions consistently operates with the technology's ability to deliver					
18	Functionality of system have been aligned with business objectives					
19	UAB Bank has experienced cases of disastrous events that have caused damage to the bank resources.					

SECTION C: EFFECTIVENESS OF EXTERNAL OPERATIONAL RISK PRACTICES AT UAB BANK.

Five likert scale: 1: Strongly Disagree 2: Disagree 3: Neutral 4: Agree 5: Strongly Agree

	External Risk	1	2	3	4	5
20	Some cooperating banks' clients comply with contractual arrangements					
21	UAB bank clients and counterparties deliver to the expected or contracted level of service					
22	Changes/ restrictions in the regulatory environment have a significant impact on the bank.					
23	UAB bank has suffered financial losses from acts of regulatory body					
24	Some actions of countries or governments					

	impact on the business directly or indirectly.					
25	Developments in the economy & financial markets have had a negative impact on the company.					