ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS AND ECONOMICS
DEPARTMENT OF MANAGEMENT

Operational Risk Management Practices

(The Case of Commercial Bank of Ethiopia)

By Hana Berhe Araya

June 2016

Addis Ababa

Ethiopia

Operational Risk Management Practices

(The Case of Commercial Bank of Ethiopia)

A thesis submitted to Addis Ababa University, College of Business and Economics, Department of Management in partial fulfillment of the requirements for degree in Executive Masters of Business Administration (EMBA)

By Hana Berhe Araya

Supervised by:

Abebaw Kassie (PhD)

June 2016

Addis Ababa

Ethiopia

DECLARATION

I, Hana Berhe Araya, declare that this thesis entitled "Operational Risk Management Practices - The Case of Commercial Bank of Ethiopia" is my original work and has not been submitted to Addis Ababa University or any other institution of higher learning as a thesis and all sources of information have been duly acknowledged.

I have carried out the research independently under the supervision of the research advisor, Dr. Abebaw Kassie.

_____

Hana Berhe Araya

June 2016

Addis Ababa University

Addis Ababa, Ethiopia

CONFIRMATION

This is to confirm the thesis entitled “Operational Risk Management Practices - The Case of Commercial Bank of Ethiopia” is conducted by Mrs. Hana Berhe Araya under my supervision.

The work is original in nature and is appropriate for submission for the award of the Masters of Executive Business Administration (EMBA) degree.

_____

Dr. Abebaw Kassie

June 2016

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

Operational Risk Management Practices

(The Case of Commercial Bank of Ethiopia)

By

Hana Berhe Araya

Approval of Board of Examiners

External Examiner	Internal Examiner
Name _____	**Name** _____
Signature _____	**Signature** _____
Date _____	**Date** _____

Confirmation

Chairperson, Department Graduate Committee

Name _____

Signature _____

Date _____

ACKNOWLEDGEMENT

First of all I would like to thank God for helping me to finalize this thesis.

I would like to express my deepest and sincere gratitude to my research advisor Dr. Abebaw Kassie, who tirelessly provided me with all the necessary advice, guidance and comments throughout this study.

I am grateful to the Commercial Bank of Ethiopia's Management and staff members for providing me with the relevant information for this study.

Lastly I am thankful to all friends and family for their ideas, advices, unlimited support and encouragement.

Contents

List of Tables

List of Figures

Acronyms

AMA - Advanced Measurement Approach

BCBS - Basel Committee on Banking Supervision

BIS - Basic Indicator Approach

CBE – Commercial Bank of Ethiopia

CORMF – Corporate Risk Management Function

COSO - The Committee of Sponsoring Organizations of the Treadway Commission

IT – Information Technology

KPIs – Key Performance Indicators

KRIs – Key Risk Indicators

NBE – National Bank of Ethiopia

ORM – Operational Risk Management

SWOT – Strengths, Weaknesses, Opportunities and Threats

Abstract

In doing business risk is inevitable and exposure to operational risk is inherent in banking activities, processes and systems. Banks therefore need to manage and keep this risk to an acceptable level. The objective of the study is to critically examine the operational risk management practices of banks in Ethiopia by taking Commercial Bank of Ethiopia (CBE) as a case. Managing Operational risk as an integrated process is a recent phenomenon especially in Ethiopian context and this study aims to examine the extent of operational risk management practices of CBE. The study was made through the combination of theory and empirical work. To achieve the study objectives survey research method was employed involving the use of both standardized questionnaire and personal interviews. Respondents were from various departments of the bank selected on the basis of their responsibilities for operational risk management. Statistical analysis in the form of percentages, means and standard deviations was employed to interpret the study findings. Effective Operational Risk Management should take into account the Risk Management Environment, Internal control and the Risk Culture of the bank. The outcome of the study revealed that the bank has an established framework to manage its operational risks, though some of its components are not always adhered to and need improvement. The bank needs to allocate adequate resources, create awareness and build the capacity of concerned staff, strengthen the risk culture, employ appropriate mechanisms for measurement and reporting of operational risk. As operational risk management practice is evolving, the bank is expected to continuously improve its approaches.

Key words: *Risk Management, Operational Risk, Operational Risk Management, Operational Risk management Environment, Internal Control, Risk Culture*

CHAPTER ONE

INTRODUCTION

1.1. Background

All businesses face uncertainty, but banking by its very nature is a business of risk (Hussein and Faris, 2007). Banks in the present-day volatile environment are facing a large number of risks such as credit risk, liquidity risk, foreign exchange risk, market risk, interest rate risk and operational risk, which may threaten a bank's survival and success. Until the Basel II reforms to banking supervision, operational risk was largely a residual category for risks and uncertainties which were difficult to quantify, insure and manage in traditional ways (Michael 2003).

Financial activity is subject to internal and external environmental factors, so a high degree of uncertainty, in other words, a high degree of risk. The increase in the degree of risk became evident during the last decade in the light of technological developments with the introduction of innovative products and delivery channels, increasing deregulation and the rising global competition where the vast world converges and becomes a small village sharing an open economy and therefore becomes subject to the internationalization of risks (Kayed and Mohamed, 2009).

Banking risks can be classified under two categories: Financial and Non-financial risks. Financial risk is an umbrella term for multiple types of risks associated with financing and directly affects the financial performance of a bank. Credit, Liquidity, Market risks are the three types of financial risks. Non-Financial Risk is a risk which indirectly affects the financial performance of a bank. It is associated with the internal and external environmental factors, macroeconomic and policy concerns, regulatory factors, the overall financial sector infrastructure and payment systems of the jurisdictions in which a bank operates. It incorporates Operational and Environmental risks.

Hence, simplifying business practices and minimizing activities that cause risk may help to avoid some kind of risks. However, some risks associated with activities which the bank is committed to proceed are inevitable and need to be properly managed. Inevitable risks are those too complex to separate from assets (Hussein and Faris, 2007). The residual risk is accepted by the bank as being crucial to its business; banks are specialized in dealing with this sort of risk, and reap the benefits.

Risk management has an essential role in one's decision-making, whether it is with regard to business start-up, strategy, exploiting opportunities, managing one's various projects or in one's day-to-day business operations (Osborne, 2012). Ability to measure the risks and take appropriate position will be the key to success. The important element in risk management is to create balance between risk and returns.

The management of credit, market and liquidity risks was long established, but operational risk management is a recent phenomenon that is getting wider acceptance by most banking industries worldwide. Operational Risk has more subjective elements and its scale is broad when compared to other risks. Studies have been conducted to reinforce the importance of paying attention to operational risk in spite of its measurement challenges.

In Ethiopia, commercial banks are playing an important role as financial intermediaries in the economic growth process, channeling funds from savers to borrowers for investment. As financial intermediaries, banks play an important role in the operation of an economy. In such away, commercial banks are key providers of funds and their stability is of paramount importance to the financial system (Birhanu, 2012).

Ethiopian banking system had not been given enough attention before 2010 especially regarding to the development of modern system of assessing, controlling and managing risk in banking operation in line with the changing environment and global financial standard (Atakelt, 2015). The National Bank of Ethiopia (NBE), which is the central bank, issued a risk management guideline in 2010 due to the need for development of sound risk management practices in the Ethiopian banking industry. In the guideline, it was stated that the recent growth in the banking system should be matched to strong risk management practices that is consistent with

international standards and best practices. The guideline provides the minimum risk management (risk identification, measurement, monitoring and control) standards for all banks operating in the country.

Operational risk is imbedded in all of the bank's operations, including those supporting the management of other risks. Managing operational risk is an important feature of sound risk management practice in any bank (NBE, 2010). The most important types of operational risk involve breakdowns in internal systems and controls and corporate governance. Other aspects of operational risk include major failure of information technology systems or events such as natural and other disasters. As banks become more reliant on technology to support various aspects of their operations, the potential failure of a technology based system is of growing concern in the context of the management of operational risk.

Operational risk cannot be confined to specific organizational units but remains largely the responsibility of line managers or owners of the core processes, and other support functions such as Information Communications Technology, Human Resource and Legal (NIB, 2015).

This study is about the Operational Risk Management practices of banks in Ethiopia by taking Commercial Bank of Ethiopia as a case.

1.2. Statement of the Problem

Banks and financial institutions are undergoing a huge change and face an environment marked by growing consolidation, rising customer expectations, increasing regulatory requirements, proliferating financial engineering, uprising technological innovation and mounting competition (Jeet and Preeti, 2013). This has increased their exposure to various risks and the need for effective risk management.

The importance of managing risk has grown over the years due to significant losses that have been experienced in the financial sector because of inadequate management of risk. The continued losses incurred by businesses due to inefficient controls has emphasized once again the need for continual review of regulatory requirements and increase in banks supervision and monitoring (Pulane, 2011).

The regulators of financial institutions and banks are demanding a far greater level of insight and awareness by directors about the risks they manage, and the effectiveness of the controls they have in place to reduce or mitigate these risks. Further, compliance regulations mandate financial institutions to identify, measure, evaluate, control and manage risks. Regulators have now become more firm and have formalized the implementation and assessment of risk management (Pulane, 2011). This has led to an increased emphasis on the importance of having a sound risk management practice in place.

The impact of operational risk on an organization is portrayed in the form of direct financial loss, earning volatility, financial distress, and non-financial effects on the future earnings capacity of the organization (Nabweteme, 2011). On the other hand effective management of this risk enhances profitability and competitiveness. Lessons learned by banks from the recent financial crisis forced radical changes in operational risk management structure. The rapid growth of Ethiopian banks calls for sound operational risk management to support this growth and continue in business maintaining their profitability (Fasika, 2012). Hence, the focus of this study is to examine operational risk management practices of Commercial Bank of Ethiopia.

Although different studies have made immense contributions to operational risk management, their focus in most cases is the banking industry in the developed world and little is done targeting banks in developing countries (Jacobus and Joseph, 2013). Existing studies didn't go beyond assessing awareness and effectiveness of overall risk management, identifying risk types and establishing relationships among risk factors and risk effect (Fasika, 2012; Tsion, 2015).

Fasika (2012) established relationships among risk factors and risk effect and identified whether each risk factor (loss event) has significance on risk effect. This study is different from Fasika (2012) in the sense that it focused on the management aspect of operational risk and assessed whether there existed effective operational risk management in the bank. This study therefore examines operational risk management practices of CBE against sound operational risk management principles.

The motivation of this study is to fill the gap in the literature by providing evidence on risk management practices of Ethiopian Banks based on case study of CBE. To the best of the researcher's knowledge, there is no study made that evaluates the operational risk management practices of banks in Ethiopia. The researcher is therefore motivated to contribute in enhancing understanding in this area.

1.3. Objectives of the Study

General Objective

The objective of this thesis is to assess the degree to which CBE is implementing sound operational risk management practices and techniques in dealing with operational risk. The study aims at identifying the challenges of operational risk management of the bank.

Specific objectives

In view of the above general objective and the problem statement, the study has the following specific objectives.

1. To examine the effectiveness of operational risk management environment of CBE,
2. To examine the adequacy of internal control processes in operational risk management of CBE,
3. To examine the level of risk culture created that supports the operational risk management of CBE and
4. To describe the challenges of maintaining effective operational risk management framework in CBE.

1.4. Research Questions

Based on the above research objectives, the following research questions are developed.

1. What is the extent of effectiveness of the risk management environment in operational risk management of CBE?
2. What is the level of internal control processes adopted to manage operational risk of CBE?
3. What is the level of risk culture created that supports the operational risk management of CBE and,
4. What are the challenges the bank is facing in having effective operational risk management framework?

1.5. Significance of the Study

Nowadays, the management of operational risk by banks is a phenomenon that is widely accepted by most banking industries worldwide (Young, 2012). A comprehensive research of operational risk management will contribute to more coherent and effective bank operation, which in the future will help to avoid problems when major risks threaten banks. This study is believed to help the bank identify its gap in operational risk management. It shows the bank's board, senior management and other stakeholders where the bank stands with regard to operational risk management and highlights areas which need more attention.

Assessment of current practices could help the regulatory body in identifying gaps which could lead to the issuance of supportive guidelines to help banks comply with the requirements as there is a need to improve the level of operational risk management to the international standards and best practices.

Finally this study contributes to enhance understanding of operational risk management by providing empirical evidence based on a case study on the CBE.

1.6. Scope and Limitation of the Study

Scope of the Study

This study analyzes the operational risk management practices of CBE and the challenges the bank is facing in the process. Due to time and financial constraints it is out of the reach of the researcher to incorporate other Ethiopian commercial banks in this study.

CBE is the largest bank in Ethiopia and to major extents reflects the national economy of Ethiopia. The motivation of selection of CBE for this study is considering its market share in terms of loans and advances, capital, number of branches, deposit position and foreign currency inflow.

Limitation of the Study

The study was limited to CBE which is the largest commercial bank in Ethiopia with relatively well established risk management department. The study was limited to the information collected through questionnaire and interviews to employees and management of CBE. Other Ethiopian commercial banks are not included in the study due to time and financial constraint.

1.7. Organization of the Study

The study is organized in five chapters. Background of the study, statement of the problem, objectives, scope and limitations of the study were discussed in Chapter One. Chapter Two presents literature and empirical review of studies about operational risk, operational risk governance, the operational risk management process and regulatory frameworks. Chapter Three introduces the research design; the sample, population and participants; data collection and analysis; reliability and validity. Chapter Four presents the results and discussions of the study which includes a review of the operational risk management practices of CBE, validity and reliability analysis and discussions of the study findings. And finally, Chapter Five presents summary and recommendations based on the study findings.

CHAPTER TWO

REVIEW OF LITERATURE

2.1. Introduction

This chapter focuses on a review of literature on operational risk with emphasis on the components of operational risk management. Empirical reviews of studies conducted under different contexts and through different research methodologies are presented at the end of the chapter.

2.2. Overview of Operational Risk Management

The banking business, compared to other types of business, is substantially exposed to risks, especially in this ever-changing competitive environment. Banks no longer simply receive deposits and make loans. Instead, they are operating in a rapidly innovative industry with a lot of profit pressure that urges them to create more and more value-added services to offer to and better satisfy the customers. Risks are much more complex now since one single activity can involve several risks (Dam, 2010).

Banks form a crucial part of the financial market and any moves by banks can have immediate impacts on the country's or even the global financial healthiness. The world has been observing a lot of crises stemmed from banking institutions then spread to the whole financial sector, typically of which is the 2008 economic downturn. The issue of a safe and sound banking sector and the importance of a feasible risk management framework in banks are now more alarming than ever (Dam, 2010).

Businesses in general and banks in particular have been aware for many years of hazards and uncertainties arising from information technology (IT) infrastructure, human motivation and fraud, business disruption, legal liability and many similar issues. Developments in modern banking environment, such as increased reliance on sophisticated technology, expanding retail operations, growing e-commerce, outsourcing of functions and activities, and greater use of

structured finance (derivative) techniques that claim to reduce credit and market risk have contributed to higher levels of operational risk in banks (Greuning and Bratanovic, 2003).

The renewed visibility of these risks under the label of 'operational risk' re-positions their location and status for management decision making purposes. Furthermore, Basel II makes connections between the management of operational risk and good corporate governance in such a way as to position these 'old' risks in a new space of regulatory, political and social expectations (Michael, 2003). Data and measurement of operational risk are key challenges to its management. A survey conducted on twenty two Indian banks indicates insufficient internal data, difficulties in collection of external loss data and modelling complexities as significant impediments in the implementation of operational risk management framework in banks in India (Usha, 2009).

According to Nazanin and Kateryna (2015), one of the main causes of major failures at banks until now was the lack of attention to risk management in general and to operational risk management in particular. The relevance of this issue has grown in addition to operational risk management challenges concerning risk culture, internal control and risk governance (Schwarts and Garliste, 2013).

In addition to credit, liquidity and market, operational risk is the other significant risk in banks. These risks are all interconnected to each other, but for the purpose of this research the focus is only on operational risks and how they should be managed. Although the recent financial crisis has been generally characterized as a liquidity crisis, operational risk and its factors have played a significant role in crisis length and severity (Jongh and Vuuren, 2013). Therefore, the need to explore the concept of operational risk has increased significantly.

The Basel Accord I required supervisors to ensure that banks have risk management policies and processes to identify, assess, monitor, and control or mitigate operational risk. The Basel committee further provided guidance to banks for managing operational risk under Accord II and required capital allocation for operational risk.

Despite the guidelines, operational risk management has paused practical challenges due to the difficulty in establishing universally applicable causes or risk factors that can be used to develop standard tools and systems of its management since the events are largely internal to individual banks. Furthermore, the magnitude of potential losses from specific risk factors is often not easy to project. It is also difficult to design an effective mechanism for systematic reporting of trends in a Bank's operational risks because very large operational losses are rare or isolated.

Different definitions have been given to operational risk taking into account the nature, causes and other factors of operational risk. The National Bank of Ethiopia (NBE, 2010) included IT, legal, regulatory, strategic, reputational, and systematic risks as part of operational risk. The NBE in its guideline defined operational risk as follows:

> *"Operational risk includes the exposure to loss resulting from the failure of manual or automated system to process, produce or analyze transactions in an accurate, timely, and secure manner."*

The Securities and Exchange Commission (2003) pointed out that the cause of operational risk is lack of controls and can arise in different areas of operations. The Commission defined operational risk as follows:

> *"Potential losses due to lack of controls within the organization in the following areas: unidentified limit breaches, unauthorized trading, fraud in trading or back office operations, inexperienced personnel and unstable or unprotected and accessible information systems."*

The Basel Committee (Basel, 2004) focused on the causes of (potential) loss events in order to differentiate operational losses from events falling in other risk categories. The Committee defined operational risk as follows:

> *"Operational risk is defined 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."*

A loss event will be considered an operational risk event if it arose as a result of inadequate or failed internal processes, people and systems or from external events. This definition is based on the underlying causes of operational risk. It seeks to identify why a loss happened and at the

broadest level includes the breakdown by four causes: people, processes, systems and external factors. Nazanin and Kateryna (2015) further defined the four causes (risks) as follows.

People risk

People risk includes the risk of loss associated with errors and illegal actions of Bank's employees, their lack of qualifications, improper organization of work in the bank, etc. People risk can also involve human error, insufficient training and management of personnel, lack of segregation of duties, lack of honesty and integrity.

Process risk

Process risk is the risk of loss associated with errors during operations and calculations, accounting, reporting, pricing, etc. The risk includes the implementation of transactions on all stages and other aspects of managing a business such as products and services risk, imperfect control system and lack of security or tough security.

System and technology risk

Implementation of IT into business environment brings challenges to workflow, procedures and policies, which in turn can lead to risks. Thus, risks associated with IT cannot be considered independently, but only in connection with people, process and other related risks. IT system problems caused by viruses, cyber-attacks and other failures lead to significant problems which influence the whole organization. Therefore, system and technology risk can be classified as the risks of losses due to imperfect technology used in the banks, e.g. the lack of systems capacity, their inadequacy in relation to the ongoing operations, inappropriate data processing methods, poor quality or the inadequacy of data used. Using effective IT analysis and management together with providing IT security will lead to successful functioning of the entire risk management system.

External risk

External risk is the risk of loss associated with changes in the environment in which the bank operates. Changes in legislation, politics, economics, and the risk of external physical interference in organization's activities are other major external risks.

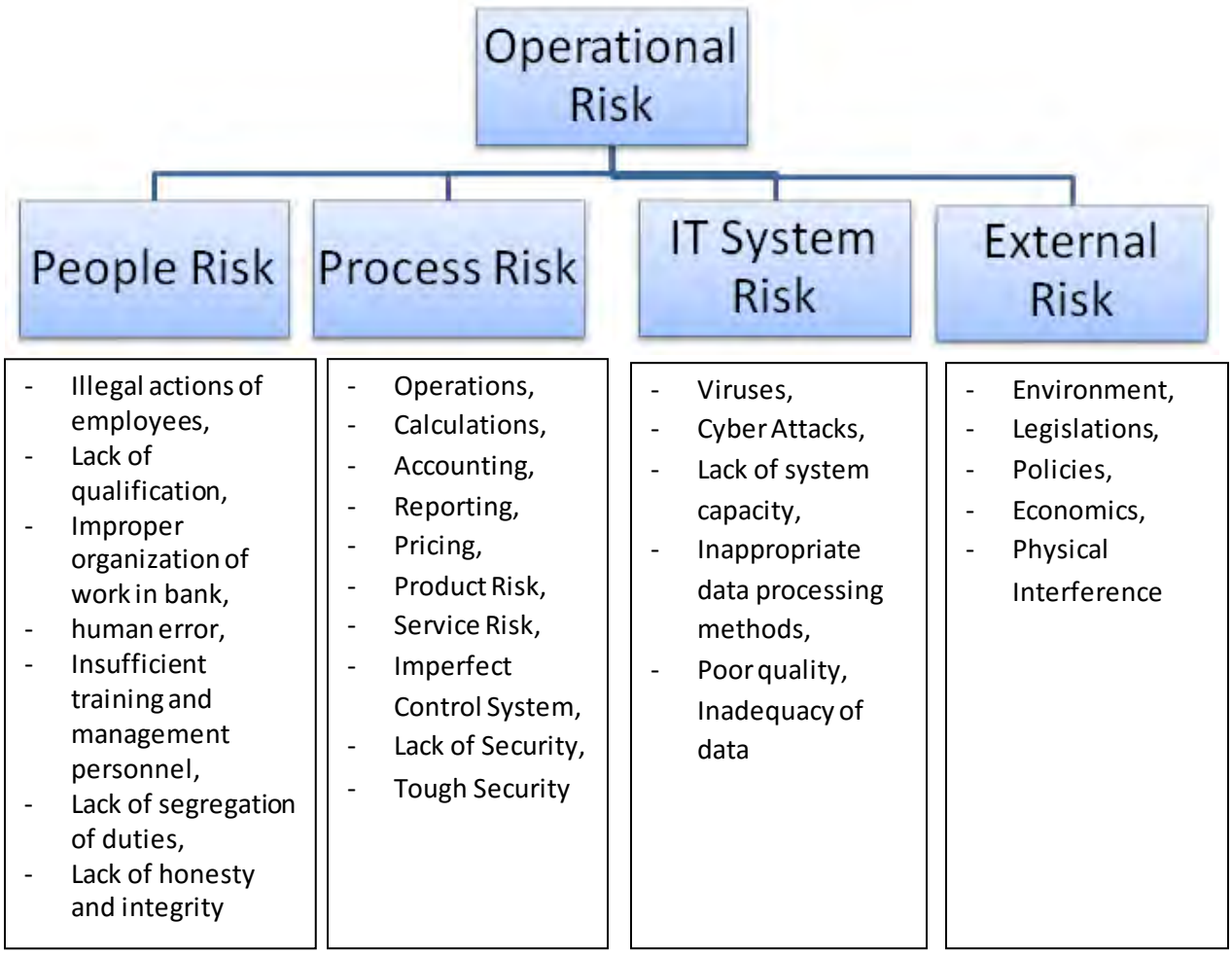

Figure 1: Operational Risk based on underlying causes (Source: Nazanin and Kateryna, 2015)

2.3. Operational Risk Management Framework

Banks should develop, implement and maintain a framework that is fully integrated into their overall risk management processes. The framework includes all the key building blocks for risk management which typically include the risk management environment, internal control and risk reporting. The Framework also covers risk appetite and tolerance and should articulate the key processes a bank needs to have in place.

2.3.1. The Risk Management Environment

The operating environment should comprise the integrity and competence of colleagues, management's philosophy and operating style and the way management communicates and delegates responsibility, and develops its people. The components of the risk management environment are the risk governance, risk culture, risk oversight, risk appetite and tolerance and the three lines of defense.

a) Risk Governance

A bank should have a strategy that involves determination of business objectives, the risk appetite, the organizational approach to risk management, and the approach to operational risk management. The strategy also involves setting up an operational risk policy statement describing the overall approach and can be made specific to each business line as applicable (Reserve Bank of India).

Risk governance is an integral aspect of corporate governance which focuses on the structures, processes and approach to the management of the significant risks to the business objectives. The overall risk management system should be comprehensive embodying all departments/sections of the institution so as to create a risk management culture (Habib, 2011). There should be clearly defined accountabilities and expectations for all relevant parties, including the roles and responsibilities of the Board, management, and employees; clearly defined policy for the management of all significant risks; the rules and process for risk based decision making; a sound system for internal control, and an appropriate assurance process.

b) Risk oversight

Board should oversee senior management to ensure that policies, process, systems are implemented effectively at all decision levels. The board of directors is responsible for outlining the overall risk appetite, objectives, and strategies of risk management for any financial institution. The overall risk objectives should be communicated throughout the institution. Other than approving the overall policies of the bank regarding risk, the board of directors should ensure that the management takes the necessary actions to identify, measure, monitor, and control these risks. The board should periodically be informed and review the status of the different risks the bank is facing through reports.

Role of Different Stakeholders in the Risk Management System

Body/Unit	Function	Duties and Role
Board	Setting overall strategy and policies	Define overall objectives and ensure its implementation by management.
Management	Set up an institution-wide risk management system.	Identify the risks and implement the objectives and policies of the board
Risk Management Dept./Unit	Identify and measure risks	Set up standards, limits, and rules, guidelines, and procedures related to risks. Publish various risk reports periodically (for both current situations and expected future scenarios).
All operational units/employees	Identify and control the risks	Follow the standards, limits and rules, guidelines, and procedures related to risk.
Internal Audit	Monitor risk management process	Ensure that risk related guidelines and policies are followed and implemented at different levels of operations.

Source: (Habib, 2011)

c) Risk appetite and tolerance

Within the framework of risk culture, appropriate risk appetite is recognized and the governance makes sure that no risks are taken beyond what the culture and appetite can handle (Nazanin and Kateryna, 2015). Therefore, there should be a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume (BCBS, 2011).

d) The three lines of defense

One common governance model is the "three lines of defense (3LoD)" model. According to Doughty (2011) strategic implementation of the 3LoD is the first principle of risk governance framework for providing effective operational risk management. The 3LoD consist of three levels as following:

The first line includes business frontline personnel. Their main task is to understand their roles and responsibilities and to perform these correctly and fully on a day-to-day basis (Doughty, 2011). In addition, in the first line, employees need to apply internal controls to treat the risk associated with their tasks. Besides the frontline employees, the risk management committee monitors and builds the department's day-to-day risk environment (Doughty, 2011).

The second line consists of supervision functions which includes compliance and risk control. The responsibilities of these line employees include participating in the business unit risk committees, reviewing risk reports and validating compliance to the risk management control requirements (Doughty, 2011).

Lastly, the third line consists of internal auditors who independently and objectively take the role of consultants and add value to the organization. They help the organization to achieve its goals by bringing in a systematic approach that provides effective risk management and control procedures to the business (KPMG, 2009). There is higher level of independency in this line comparing to the second line.

2.3.2. The Risk Culture

The Board and senior management should create an enabling organizational culture placing high priority on effective operational risk management and adherence to sound operating procedures. Successful implementation of risk management process has to emanate from the top management with the demonstration of strong commitment to integrate the same into the basic operations and strategic decision making processes (Reserve Bank of India).

2.3.3. The Operational Risk Management Process and Internal Control

According to a study done by Moody (2010) to increase the effectiveness of risk management in the organization, the risk management process should be part of organizational processes and decision making while it should be dynamic and responsive to changes. According to Andersen, Maberg, Hägerwzx and Tungland (2012) the main causes of the financial crisis were severe violations regarding operational risk management, mostly due to the lack of attention to its processes. In addition, appearance of new and more advanced IT systems with higher security increased attention to ORM ((Jongh and Vuuren, 2013). Apatachioae (2014) stressed that the imperfection of bank's IT and data architecture to support the risk management on the appropriate level, was one of the greatest lessons learned from the global financial crisis for managing operational risks. The management of operational risks can be described as a cycle comprised of the following steps: risk identification, risk assessment, risk treatment and risk monitoring (OeNB and FMA, 2006).

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 (BCBS, 2011).

Internal control failures take a common place in the banks resulting in huge financial losses. Internal control is an important part of operational risk management and provides a reasonable assurance to achieve the objectives of the organization. Together with an effective risk governance, reliability of financial reporting, compliance with applicable laws and regulations, implementation of internal control system can be achieved (COSO, 2004). In addition,

Chernobai, Jorion and Yu (2011) stressed that most of the operational risks come from consequences of weak internal control.

a) Risk Identification and Assessment

During risk identification and assessment, banks should consider several factors in order to establish the risk profile of a company and its activities, for example: types of customers, activities, products; design, implementation and effectiveness of processes and systems; risk culture and risk tolerance of the bank; personnel policy and development; and environment of the bank. The following tools (techniques) have proven especially useful for this work: self-assessment (risk inventory), loss database, business process analysis, scenario analysis, and risk indicators.

As per the Guidelines on Operational Risk Management (OeNB and FMA, 2006), the following processes are included as operational risk identification techniques.

b) Self-Assessment (Risk Inventory)

Self-assessments aim at raising awareness of operational risks and at creating a systematic inventory as a starting point for further risk management processes as well as process improvements towards better performance. They take the form of structured questionnaires and/or (moderated) workshops and complementary interviews.

Their main purpose essentially is to identify significant operational risks and then evaluate them. Using scorecards, qualitative evaluations obtained in a self-assessment can be translated into quantitative parameters for assessing loss frequency and severity in order to be able to rank the risks and, hence, identify the key risks.

Special attention should be paid to the identification of those risks, which could endanger the survival of the institution. In graphic or tabular form, the risk portfolio can be presented as a risk map or risk matrix, respectively. A SWOT analysis serves to identify and present one's own strengths and weaknesses as well as opportunities and threats.

c) Loss Database

The loss data base contains both internal and external loss data. Databases are used to record and classify loss events. The systematic collection of loss data within a credit institution forms the basis for an analysis of the risk situation and, subsequently, for risk control.

d) Business Process Analysis

Within the framework of operational risk management, business process analyses are used, in particular, to link processes, risks and controls in a risk analysis. They may also have the purpose of ensuring risk-oriented process optimization.

The identification of business processes across all organizational units is a prerequisite for allocating loss data to processes and determining the risk for a business process. Moreover, there is a close connection between business process analyses and self-assessments. On the basis of self-assessment, it should be possible to allocate the significant risks and controls identified to the business processes. As a result, at least a rough business process analysis should already be carried out before self-assessment.

e) Scenario Analysis

Scenario analyses are used to identify possible high-impact events that have not occurred to date. In contrast to the collection of loss data that focuses exclusively on the past, scenario analyses emphasize future-oriented aspects of operational risk.

There is a close link between scenario analyses and stress tests because the empirical or analytical identification of extreme scenarios is a prerequisite for performing stress tests. These tests are used to simulate and weight the impact of different scenarios.

f) Key Risk Indicators (KRIs)

Key risk indicators provide information on the risk of potential future losses. They should make it possible to identify areas with elevated risks early on and to take appropriate measures. Thresholds (“triggers”) may be defined for KRIs. They permit statements to be made on trends

and can serve as indicators in an early-warning systems, e.g. in combination with a traffic-light system (red, yellow, green).

Examples of KRIs are: staff fluctuation rate, days of sickness leave, hours of overtime, number and duration of system failures, internal audit findings, frequency of complaints and wrong account entries.

Rao and Dev (2006) in their study outlined four characteristics of KRIs of operational risk that are not only desirable but also critical: a KRI has to be measurable quantitatively; a KRI has to be statistically robust predictor of the probability of the occurrence, if not the severity, of an operational risk event; KRIs for each major operational event category have to be limited in number, say twenty because of pragmatic and statistical reasons; and it has to be possible for the operational risk manager to affect the value of a KRI over time.

g) Risk Reporting, Communication and Information

The Guidelines on Operational Risk Management (OeNB and FMA, 2006) identified one of the objectives of modern risk management is internal and external risk transparency. Open, target-oriented communication, rapid and reliable information and reporting contribute to achieving this objective. The guideline further explained these activities below.

Communication and Information

Various organizational units of a bank need different types of information on risk management. Therefore, an element of effective risk management is regular reporting on the risk situation (in appropriately aggregated form) to the level responsible as a basis of decision-making as well as to monitoring levels (supervisory board, internal audit) and ad-hoc reporting in the case of significant events or changes in the risk situation.

Reporting

On the one hand, internal reports are continuously prepared as a function of materiality thresholds applying at different hierarchy levels. On the other hand, ad-hoc reports should

ensure that decision-makers can take timely measures when loss events or – within the framework of an early-warning system – risk indicators exceed certain thresholds.

As external reporting on the banks' risk management is becoming more and more important, this also applies to external reporting on operational risk management. Many banks include a risk report in their annual reports, be it as part of the directors' report or, in the case of IFRS reports, as a part of the notes on the annual report. Many banks also report on important plans and projects.

In the framework of reporting to banking supervisors, reports will also have to be submitted on operational risks. Ideally, supervisory reporting is an element of an active, open and continuous dialogue between banks and supervisors.

2.3.4. Quantification of Operational Risk

Models for quantifying operational risk are currently still in a relatively early stage of development. Basel II has provided a decisive impetus to the development of appropriate models. "High-frequency, low-severity" and "low-frequency, high-severity" losses involve very different modelling requirements.

This means that, as a rule, there will not be only one way of quantifying operational risk. Rather, it is necessary to find a mix of methods corresponding as well as possible to the bank's risk profile.

The value at risk (VaR) of an asset position or portfolio, as it is used in the control of market or credit risks is the monetary expression of the loss in value not exceeded with a certain probability "a" (confidence level) in a defined period of time (holding duration).

As per the guideline of the Reserve Bank of India, a good assessment model must cover certain standard features. An example is the "matrix" approach in which losses are categorized according to the type of event and the business line in which the event occurred. Banks may quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk.

2.3.5. Operational Risk Treatment

As per the Guidelines on Operational Risk Management (OeNB and FMA, 2006), the key outcome of the risk identification and assessment process is a detailed list of all key risks including those that require treatment as determined by the overall level of the risk against the Bank's risk tolerance levels. The guideline further listed out the basic management elements for coping with identified and valuated operational risks as risk avoidance, risk mitigation, risk sharing and transfer and risk acceptance.

a) Risk Avoidance

In a cost-benefit analysis, a bank should opt for risk avoidance if the expected margin of activities is lower than the expected risk cost taking account of all the risks. Such activities should be abandoned or not be launched in the first place.

Such a decision has to consider several aspects, such as time horizon, available specialized expertise, strategic objectives and reputational risks.

b) Risk Mitigation

The objective may be a cause-oriented reduction of loss frequency or an effect-oriented reduction of loss severity. Both objectives can be supported by internal control activities. Additionally, risk sharing or complete risk transfers are suitable options for reducing loss severity.

The tools of risk mitigation mainly include a multitude of organizational safeguards and control measures within the framework of an internal control system: guidelines and procedures, separation of functions and “four-eyes principle”, need-to-know principle (access control), physical access control, coordination and plausibility checks, limit management, inventories, and disaster recovery and business continuity planning.

c) Risk Sharing and Transfer

Risk sharing or transfer is mainly of interest if a risk cannot or only inadequately be reduced by internal controls or if the cost of controls is higher than the expected loss. Another condition is that, in comparison with the bank’s risk appetite, the risk is so high that it cannot simply be

accepted. Important instruments of risk sharing and/or risk transfer are insurance and outsourcing of activities and functions.

d) Risk Acceptance

As a rule, risk acceptance depends on a cost-benefit analysis or weighting of expected income versus risk. A rational reason for accepting risks would be that the expected loss is lower than the cost of management activities to mitigate the risks. Criteria, such as thresholds, and decision-making processes, including escalation procedures, should exist for accepting risks.

e) Risk Control

The monitoring and reviewing activities of operational risk refers to the mechanisms for tracking whether the operational risks of the bank are being managed in line with the predefined framework, i.e. strategy, policies, procedures, systems, standards, and practices, governing the bank. The results of these monitoring activities should be included in regular management and Board reports, as should compliance reviews performed by the internal audit and/or risk management functions.

On the one hand, there should be ongoing controls embedded in business processes that should be performed by all employees within the framework of their tasks. On the other hand, there should be separate inspections by several internal and external entities.

Among others, tools that are employed towards monitoring operational risk include the development and implementation of key risk indicators (KRIs) and maintenance of internal and external loss data.

To summarize, the basic components of a risk management system are identifying the risks the entity is exposed to, assessing their magnitude, monitoring them, controlling or mitigating them using a variety of procedures, and setting aside capital for potential losses.

2.3.6. Capital Allocation for Operational Risk

The Basel Committee has put forward a framework consisting of three options for calculating operational risk capital charges. These are (i) the Basic Indicator Approach (ii) the Standardized Approach and (iii) Advanced Measurement Approaches.

The Basic Indicator Approach (BIA) allows the banks to hold capital for operational risk equal to the average over the previous three years of a fixed percentage (alpha) of positive annual gross income. Negative and zero gross income are excluded from both the numerator and denominator when calculating the capital. Gross income in its simplest form is defined as net interest income plus net non-interest income (Basel Committee on Banking Supervision, 2006). Most of the supervisors in different countries have decided to go for this approach because of its simplicity in calculation and ease in adapting to Basel II rule.

In the standardized approach, the capital charge for each business line is calculated by multiplying gross income by a factor (beta) assigned to that business line. The total capital charge is calculated as the three year average of the sum of the capital charges across each of the business lines in each year. In the business lines the highest beta factor (18%) is with corporate finance, trading & sales and payment & settlement, while the lowest (12%) are with retail banking, retail brokerage and asset management. Therefore, banks with different exposures on different business lines shall have different capital charge that seems quite sensible based on the industry experience of losses because of operational risk from various business lines (Mestchian, 2003).

The AMA is the most scientific method of the measurement of operational risk in terms of continuum sophistication and risk sensitivity wherein the regulatory capital charge will equal the risk measure generated by the banks' internal risk measurement system using the quantitative and qualitative criteria for the AMA (Operational Risk and Compliance, 2006). The loss model approach is the most used by the internationally active banks in developed economies. The Actuarial loss model approach has become accepted by the industry as the generic AMA for the determination of operational risk regulatory capital for the new Basel II accord. The Basel Committee on Banking Supervision (2006) clearly outlines the standards to

qualify for use of the AMA. The standards are three types: General standards, Qualitative standards and the Quantitative standards. The General standards require a bank to have an actively involved board of directors and senior management in the oversight of operational risk management framework, an operational risk management system and the sufficient resources in the use of the approach. In the Actuarial approach to loss measurement, KRIs play a very significant role. KRIs can be extremely useful in the measurement and management of operational risk.

In October 2014, the Basel Committee proposed revisions to the standardized approaches for calculating operational risk capital. This committee updated consultative document in March 2016 and proposes further revisions to the framework, which emerged from the Committee's broad review of the capital framework.

The Committee's review of banks' operational risk modelling practices and capital outcomes revealed that the Advanced Measurement Approach's (AMA) inherent complexity and the lack of comparability arising from a wide range of internal modelling practices, have exacerbated variability in risk-weighted asset calculations, and eroded confidence in risk-weighted capital ratios. The Committee is therefore proposing to remove the AMA from the regulatory framework.

The revised operational risk capital framework will be based on a single non-model-based method for the estimation of operational risk capital, which is termed the Standardized Measurement Approach (SMA). The SMA builds on the simplicity and comparability of a standardized approach, and embodies the risk sensitivity of an advanced approach. The combination, in a standardized way, of financial statement information and banks' internal loss experience promotes consistency and comparability in operational risk capital measurement.

2.3.7. International and National Risk Regulations and Frameworks

To manage risks better and for having a proper control mechanism throughout the organization, some international and national frameworks should be implemented. These frameworks are presented below:

The Second Basel Accord (Basel II) is a well-established standard that was initially issued by the BCBS in 2004. Generally, Basel II is intended to facilitate standards for measuring operational risks in banks. It also necessitates the consideration of standards by the board of directors and financial institutions in order to establish a strong risk [management] culture (BCBS, 2003).

In 2010, as a response to the crisis, BCBS issued The Third Basel Accord (Basel III), a new regulatory standard on bank market liquidity risk, capital adequacy and stress testing (BCBS, 2011). The main aim of Basel III is to intensify the existing regulatory capital requirements in order to improve strength and flexibility of international banking system by enhancing the regulation and risk management of the banks (Keefe and Pfleiderer, 2012).

In the Principles for the Sound Management Operational Risk, published in June 2011, the Basel Committee on Banking Supervision (Committee) articulated a framework of principles for the industry and supervisors with emphasis on governance, risk management environment and the role of disclosure.

The Committee of Sponsoring Organizations (COSO) Internal Control – Integrated framework - was introduced in 2004. The framework defines internal control as "process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance" (COSO, 2013). Effectiveness of internal control according to this model is based on five integrative components namely control environment, risk assessment, control activities, information and communication, and monitoring activities (COSO, 2013).

In addition to Basel II, Basel III and COSO as international frameworks, Ethiopian banks have to comply with the rules and regulations which are introduced by the NBE. NBE's main role is to ensure systematic stability in the financial system and to supervise, authorize and monitor all financial institutions with businesses in Ethiopia. Specifically on Operational Risk Management (ORM), NBE published a new set of regulations in 2010. The new regulation contains rules on all aspects of ORM such as risk appetite, control, risk governance, reporting, risk indicators and measurements.

2.4. Empirical Review

Studies on risk management practices of commercial banks in different geographic locations and economic development levels were conducted by different researcher using different research methodologies. A review of a few of them is presented below.

A Study of UAE banks, Hussein and Faris (2007), was conducted through a survey method to examine the degree to which the UAE banks use risk management practices and techniques in dealing with different types of risk. The study found out that the three most important types of risk facing the UAE commercial banks were foreign exchange risk, followed by credit risk, then operating risk. The authors concluded that UAE banks were somewhat efficient in managing risk, and risk identification and risk assessment and analysis were the most influencing variables in risk management practices. The four most important methods of risk identification were inspection by the bank risk manager, audits or physical inspection, financial statement analysis and risk survey.

In a similar research conducted on Ethiopian commercial banks, Tsion (2015), it was found that risk managers perceive risk management as critical to their banks' performance; the types of risks causing the greatest exposures were credit risk, operational risk, liquidity risk, interest rate risk and foreign exchange risk; there was a reasonable level of success with current risk management practices, and banks were utilizing some of the approaches/techniques traditionally used to manage risks. The research concluded that the banks operating in Ethiopia are indeed risk-focused.

A study of Ugandan bank, Nabweteme (2011), was different on its approach whereby correlation research was designed to establish the relationships between operational risk management, organizational environment and organizational performance. The study undertook cross-sectional and descriptive survey design. Data was collected using self-administered questionnaires. The study revealed a significant positive relationship between operational risk management and organizational environment. In the study a significant and positive relationship between organizational environment and organizational performance was also observed. This was confirmed by the findings on the selected dimensions of ORM -

systems, internal processes and people; dimensions of environment - structures, disclosure and cultures, and dimensions of performance – growth, market share and profitability.

Another study revealed that there existed significant correlation between operational risk effect and operational risk factors or loss events (Fasika, 2012). This research was about operational risk management of commercial banks in Ethiopia and was conducted through the use of questionnaire and interviews. Descriptive analysis, Spearman correlation coefficient and principal component analysis were used as methods of data analysis. The risk effect was found to have significant relationship with risk factors (loss events) such as internal fraud; external fraud; employment practices and workplace safety; clients, products and business practices; damage to physical assets; business disruption and system failures, and execution, delivery and process management.

The level of risk awareness in centralized risk management structures of the majority of North Cyprus banks was found to be low and tend to ignore the importance of internal auditing in risk management as revealed by Kesjana and Hatice (2010). Their study was conducted with the aim of investigating the practice of risk management and how the concept was perceived within commercial banks in North Cyprus. The study used a survey method and data was collected through face to face interviews with the general managers of commercial banks. The survey results indicated that most of the banks had good approaches in coping with credit and market risks, but had major weaknesses in terms of managing their operational risks. Besides, the majority of banks did not make provisions for their operational risk.

Thirupathi and Manoj (2013) attempted to identify the risks faced by the banking industry and the process of risk management in India. To achieve the objectives of the study, the researchers collected data from secondary sources i.e., from Books, journals and online publications. The authors concluded that functions of risk management should actually be bank specific dictated by the size and quality of balance sheet, complexity of functions, technical/ professional manpower and the status of the Management Information System in place in that bank. Regarding use of risk management techniques, they found out that internal rating system and risk adjusted rate of return on capital were important. Finally they determined that the

effectiveness of risk measurement in banks depends on efficient Management Information System, computerization and networking of the branch activities.

The use of key risk indicators as an operational risk management tool by South African banks was assessed and found that these banks, in general, are not suitably prepared to implement a key risk indicator management process. According to Young (2012) Key risk indicators (KRIs) can be used as an operational risk management tool, however, it is important to note that an indicator becomes key when it tracks a risk exposure, which could have a major influence on the organization. Young (2012) stated that KRIs are mostly quantitative measures intended to provide insight into operational risk exposures and control measures. Young (2012) argued that KRIs can be used in managing operational risk in a number of ways, for example as early warning, in supporting risk assessments, in determining a realistic risk appetite and in capital allocation. For KRIs to be used as a risk management tool data must be available; data must be quantifiable; a tolerance threshold must be determined; and they must be monitored on a regular basis. The study concluded that banks seem to understand the use of KRIs, but appear not to be fully aware of the value and benefits that the successful implementation of a KRI management process could ensure. Besides, they are still in the initial implementation phase.

A study conducted in a different context and methodology was by Nazanin and Kateryna (2015). It was a case study on operational risk management of one of Sweden's largest retail banks through adopting a qualitative research method. The primary data was collected through the interviews with eligible employees of the bank and secondary data was collected from periodic reports and website of the bank.

The aim of the research of Nazanin and Kateryna (2015) was to answer how risk management, internal control and risk governance have been organized to handle operational risks and how operational risk management has improved since the global financial crisis. It was concluded that although improvements have taken place in how operational risks are being managed, there is still room for improvements. The study revealed that loss of reputation as a result of problems within IT system risks together with external card fraud were among the most common risks that banks should take into consideration when managing operational risks. It

was concluded that internal control frameworks still needed to be modified by regulators to be more efficient while there should be reasonable amount of regulations applicable to banks.

According to Nazanin and Kateryna (2015) banks need to comply with national and international regulations, take an attempt to build positions within the 3LoD and apply stress-testing annually to have control on how operational risks are managed. Operational risks should be reported periodically to senior management and the board of directors who set the risk appetite and risk culture of the organization for better internal control and management of operational risks together with other types of risk.

The National Bank of Ethiopia (NBE 2009) conducted banks' risk management survey through the use of questionnaire to be completed by 15 banks in the industry. The survey aimed to identify status of risk management practices of banks and to put forward recommendations to address weaknesses. It was found that though the banking sector has shown improvements, the risk management practice is yet to be strong. Among the weakness identified in the survey were the Board of Directors lack adequate training on risk management; adequate resources are not allocated for the risk management function; policies do not define limits and communication of risk appetite is low; internal/external auditors do not independently review the effectiveness of risk management function; and the risk identification and preparedness processes are weak.

To summarize, previous studies have revealed that risk management is central in operations of financial institutions, both from business and regulatory perspectives. Habib (2011) explained that risk management is not only about identifying and mitigating risks, but involves a strong risk management system that includes establishing appropriate risk management environment, maintaining an appropriate risk management process, and instituting adequate internal controls. Risk management is a recent phenomenon in the banking industry, but is recognized as important aspect of running the banking business. However, the management of operational risk has not been given enough attention though related potential losses are magnificent.

2.5. Conceptual Framework

The following conceptual framework is produced to show clearly key elements of sound Operational Risk Management Framework.

Source: own design based on Sound Practices for the Management and Supervision of Operational Risk (BCBS, 2011)

Figure 3: Risk Management Framework

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Introduction

This chapter outlines the rationale of the research methodology used in this study. It includes research design, sampling techniques, data collection and analysis, reliability and validity.

3.2. Research Design

This study is descriptive in nature as the researcher tries to describe the topic of operational risk management and its components. The researcher used survey research method involving the use of both standardized questionnaire and personal interviews to collect data in a systematic manner. Data necessary to answer the research questions were collected and have both qualitative and quantitative nature.

The questionnaire was composed of structured questions where the respondents were asked to choose an answer from a given set of choices. At the end of each dimension of the questionnaire questions, respondents were asked to provide a response in their own words to one open ended question. The questionnaire was prepared based on the Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk (BCBS 195) with slight modification to adjust to the prevailing conditions of the banking industry in Ethiopia. Respondents were asked to express the level of compliance of operational risk management practices of CBE with respect to 69 statements by using a rating from 1 to 5 where 5= Fully Complied (FC); 4= Substantially Complied (SC); 3 = Moderately Complied (MC); 2= Partially (to a lower extent) Complied (PC); 1=Not Complied (NC). Open ended questions at the end of each dimension were also part of the questionnaire.

Interview data which was non-numeric and qualitative was gathered to complement the questionnaire and to obtain deeper understanding of the subject matter. Numeric assessment with numeric scores in the form of questionnaire is gathered to get quantitative and objective information about the research (Bhattacherjee, 2012). Hence, primary data was collected by

distributing a structured questionnaire to respondents and conducting interviews with selected employees of the bank.

3.3. Sample, Population and Participants

From the entire population of the employees of the bank, the researcher purposely drew a sample of staff that were suited for the questions. To ensure appropriate responses were collected, departments with responsibilities of risk management or assurance functions were considered, and as much as possible the participants within these departments were chosen taking into account their years of experience. Hence primary data is collected from respondents in Risk Management, Credit Management, Finance, Internal audit and process owners who are believed to have a good understanding of the operational risk management process.

Therefore, the sampling frame, also known as a working population, opted was a non-probability sampling method, contained units or people who were suited for the questions. Expert sampling as Bhattacherjee (2012) defined is a technique where respondents are chosen in a non-random manner based on their expertise on the phenomenon being studied. The basis of selection is therefore the desired knowledge and expertise of the respondents.

3.4. Data Collection and Analysis

The data collection method employed in this study involves gathering both numeric information on the questionnaire as well as text information on the interviews so that the final database represents both quantitative and qualitative information (Creswell, 2010).

The collection and analysis of both quantitative and qualitative data was done concurrently so that the data gathered in the two methods complement each other.

Data collection techniques can be classified as either quantitative or qualitative method. Non-numeric data such as observational or interview data represents the qualitative measures, whereas, numeric assessment such as numeric scores and metric like questionnaire is used as quantitative measures (Bhattacherjee, 2012). Mixed approach whereby the researcher tends to base knowledge claims on pragmatic grounds (e.g., consequence-oriented, problem-centered, and pluralistic) is employed in this study (Creswell, 2010).

The researcher analyzed the data gathered through close ended questionnaires with the aid of SPSS (Statistical Package for Social Science) version twenty (20). A descriptive analysis of data is provided in terms of percentages, means, and standard deviations. Moreover, evaluation of results, possible reasons and their implications are analyzed.

3.5. Reliability

Reliability is about how consistent a researcher's measurements are (Cook and Campbell, 1979). It measures the degree to which a construct is consistent and similar outcomes can be obtained in similar studies under similar underlying phenomenon.

The reliability and internal consistency of the questionnaires were checked by computing Cronbach's alpha values.

3.6. Validity

Validity of data is determined by the strength of conclusions, inferences or propositions (Cook and Campbell, 1979). Data is measured in order to have relevance and validity for the issue that is examined. It is about finding out if the data collected or gathered is relevant to the problem being investigated and whether the survey conducted provided an answer to the problem.

To ensure the instruments employed measured what they were supposed to measure, pretest of the questionnaire and interviews was made with staff in the risk management function of the bank.

CHAPTER FOUR

DATA ANAYSIS AND INTERPRETATION

This chapter presents the research results and discussions based on the research objectives. The background of CBE, its risk governance structure and framework, the Risk and compliance Management Function and the bank's operational risk management processes are introduced in brief. Following the introduction, validity and reliability analysis, data collection process and respondents profile and detail research findings are discussed.

4.1. Background of CBE

The history of the CBE dates back to the establishment of the State Bank of Ethiopia in 1942. CBE was legally established as a share company in 1963. In 1974, CBE merged with the privately owned Addis Ababa Bank. Since Then, it has been playing significant roles in the development of the country.

The CBE was established to perform major banking functions, including:

- Accepting saving, demand and time deposits,
- Providing short, medium and long term loans;
- Buying and selling foreign exchanges;
- Buying and selling negotiable instruments and securities issued by the government, private organizations or any other person; and
- Engaging in other banking activities customarily carried out by commercial banks.

Governance structure of the CBE

Monetary and banking proclamation No. 83/1994, Licensing and Supervision of Banking Business Proclamation No. 84/1994, Banking Business Proclamation No. 592/2008, and the various directives of the NBE are the basis for the bank's business operation. CBE is supervised by Board of Directors and the day today functions of the bank are managed by the President.

The bank has a process –oriented corporate structure where each process headed by a process owner. CBE performs its operations through its core and support processes.

Core and Support Processes

The bank's core processes are Customer Accounts and Transaction Services (CATS), Trade Services (TS) and Credit Services. The Support Processes are Corporate Human Resources (HR) process, Information Systems (IS), Facilities Management, Finance, Business Development, Risk and Compliance Management, Internal Audit, and Legal and Loan Recovery.

CBE's Market Share

'Position at Year Endings'

Parameters	2010	2011	2012	2013	2014
Loan and Advances	42.3%	46%	53.3%	52%	53%
Capital	43%	39%	42%	39%	34.2%
Number of Branches	32%	39%	42%	40%	38.8%
Deposit Position	57%	62%	65%	65%	67%
FCY Inflow	31%	41%	45%	52%	

Table 1: CBE's Market share (Source: Profile of the CBE, 2014/15)

Operational Performance

'In Millions of Birr at Year Endings'

Particulars	2010	2011	2012	2013	2014	2015
Total Deposit	56,081	86,499	122,195	154,529	193,320	241,732
Outstanding Loan and Bond	50,577	76,219	125,751	153,487	203,680	265,365
Total Assets	74,187	114,265.1	158,853	195,443	242,726	303,635
Total Liabilities	68,632	108,003.6	151,154	186,244	232,680	290,739
Total Capital and Reserves	5.532.7	6.261.5	7.699.9	9,199	10,703	12,896
Total Income	4,494.2	6,994.2	11,573.8	13,566	17,335.6	22,790
Total Expenses	1,675.6	2,756.1	3,624.2	5,166	7,509	10,127
Gross Profit	3,197	4,172	7,891	8,424	9,686	12,664
Capital Adequacy Ratio (CAR) %	17.4	11.5	9.68	13.3	12.9	13.2
Return on Asset (ROA) %	4.2	4.4	5.9	4.8	4.4	4.6
Return of Equity (ROE)%	53.5	70.7	114.1	101.2	98.0	102.8

Table 2: CBE's Operational Performance (Source: Profile of the CBE, 2014/15)

Branch Network

The bank carries on its business through 965 branches (as of June 2015) spread throughout Ethiopia and a subsidiary office in South Sudan. The branches execute their functions under the supervision of 15 district offices.

4.1.1. Risk Governance Structure and Framework

Over the past few years, CBE has witnessed a significant growth, which is manifested by a major balance sheet growth, aggressive branch expansion, technological advancements and an introduction of e-payment. This massive growth, accompanied by momentous asset and liability growth, necessitates comparable and strong operational risk governance to manage the adverse impacts of the observed developments.

CBE has developed a risk governance framework that provides guidance for the management of banking risks. Its internal control framework provides the system by which the bank proactively prevent materialization of potential operational risks and minimization of impacts through implementation of enabling control environment that incorporates, among others, instituting enabling organizational structure, implementation of policy and procedures, code of conduct, segregation of duties, conduct regular risk assessments and audit. Its operational risk management guideline enhances the risk oversight function and facilitates risk based auditing. However, with its current domestic expansion and opening of overseas subsidiaries, it is vital to have a risk governance framework that reflects the bank's growth and the international banking business environment more than ever.

CBE has adopted the three lines of defense model as its Operational Risk Management framework. The model assigns different but mutually complementary duties and responsibilities to the Board of Directors, to all Business Units of the Bank, to Risk and Compliance Management Function and to the Internal Audit Function. Following are the duties and responsibilities of the Board of Directors and the role players in the three lines of defense structure.

Board of Directors: the board of directors has two sub committees; the Loan and Risk Review Committee, and the Audit Committee. Its main role is oversight of the risk management effectiveness through setting the 'tone at the top', establishing risk appetite and risk strategy, approving risk management framework, methods, overall policies, roles and responsibilities, leveraging risk information into decision making process, and accept, transfer or mitigate identified risks.

First Line of Defense: are all business units or departments that are providing business services of the Bank. They are owners of the risk management process in their domain. Accordingly, all departments identify, manage, mitigate and report on different risks in their domain.

Second Line of Defense: is the Risk and Compliance Management Function that provides interpretation of regulations/leading practices and disseminates to business units; designs and deploys the overall risk management framework; monitors adherence to framework and strategy; develops risk management methodologies, policies and procedures; monitors compliance and performs aggregated risk reporting and provides independent testing and verification of efficacy of corporate standard and business line compliance.

Third line of defense: is the Internal Audit Function which validates the overall risk framework, provides assurance that the risk management process is functioning as designed and identifies improvement opportunities.

In line with its responsibility, the Board of directors approved Operational Risk Management Guideline which has been implemented since year 2012. The Loan and Risk Review Committee of the Board oversees significant risks of the bank including operational risk. However, a dedicated Operational Risk Committee at Board level is not yet established.

4.1.2. Organization of the Risk and Compliance Management Function

The bank established the department of Corporate Risk and Compliance Management following a Business Process Re-engineering (BPR) study in 2008 aiming to spearhead risk management system across the bank and intensify the awareness of risk based performance. As shown in the following structure, the department has three divisions namely Corporate Risk Management,

Corporate Compliance Management and the newly incorporated Information Security Management Division. The department is staffed with risk experts, compliance officers, cyber-attack analysts, and information security officers.

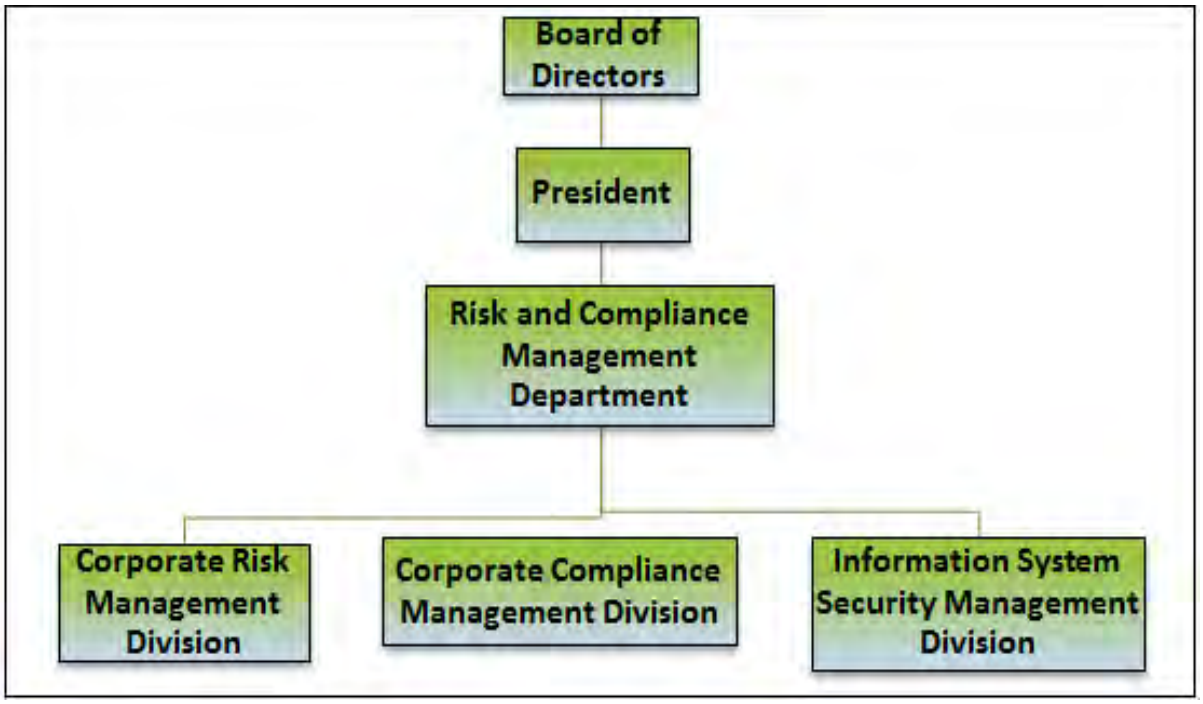

Figure 2: Organizational Structure of the Risk and Compliance Management Function (Source: CBE's Corporate Risk and Compliance Management department)

4.1.3. Operational Risk Identification, Assessment and Recording

In CBE operational risk is unique from other type of risks in that it is inherent to business (inseparably linked with almost all business activities). All measures to control and mitigate it strongly depend on the specific profile of the bank as there is no one size fits all for managing operational risk. The diversity of operational risk makes it difficult to limit the number of dimensions required to describe it. Operational risk encompasses the types of risk emanating from all areas of the bank; front office, back office or support areas. Hence, identifying operational risk is more difficult and complex in its causes, sources, and manifestations.

Any event that may negatively or positively impact the achievement of each department's objective and the bank's objective as a whole is encouraged to be identified as a risk and assessed at least once in a year. Emerging events, if any, are identified at any time. Internally

developed self-assessment questionnaire, process and risk mapping, facilitated workshops/brainstorming and scenario analysis are the most common methods CBE uses to identify operational risks. Key risk indicators are also used where the information is available such as historical occurrences of events but not significantly and systematically deployed.

The major categories of operational risks are execution, delivery and process management, fraud, and business disruption and system failures. Such risks are mainly caused due to skill gap, internal process design, integrity problem of human resource, and dependence on sole service providers like network, power, and software.

In consideration of the internal control effectiveness in preventing the potential operational risks, the bank determines the likelihood and impact of a given potential risk and measures the exposure using quantitative scores. Qualitatively, the probability of a given potential risk can be almost certain, likely, possible, rare or unlikely and its impact can be rated as disastrous, major, moderate, minor or insignificant.

So far the bank doesn't allocate capital charge for its operational risk exposure but has experience of allocating operational expense budget for some common and recurrent operational losses even though operational risk management is not yet integrated with key performance indicators.

4.2. The data collection process and respondents profile

Questionnaires and interview data were collected from selected departments of the bank. Descriptive analysis of the data in the form of percentages, means and standard deviations is presented. The average mean of each factor is also calculated and interpreted based on Best and Khan (1995) who gave ratings of 'lowest' for 1 – 1.80, 'lower' for 1.81 – 2.61, 'average' for 2.62 – 3.41, 'good/high' for 3.42 – 4.21 and 'very good/very high' for 4.22 – 5.00 mean values.

The questionnaires were distributed to a total of 93 staff members of the Risk Management, Internal Audit, Credit Management, Credit Appraisal, Credit Portfolio Management, Finance and other functions of the bank. 86 questionnaires were returned which is a 92% response rate. Three of the returned questionnaires missed some information and are excluded from analysis.

The questionnaire consisted of questions about the profile of the respondents and basic research questions. The questions about the profile of the respondents included educational background, work experience and their respective departments within the bank to ensure the right employees are participated in the completion of the questionnaire.

4.2.1. Cross Tabulation Descriptive Analysis of the Respondents

As case processing summary below indicates out of the 86 responses 83 are valid whereas the 3 case are shown as missing for the reasons the respondents failed to mention their working department, level of education, years of experience or any other information.

Table 4.2.1: Case processing summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Department respondents were working in	83	96.50%	3	3.50%	86	100.00%
Level of education of respondents	83	96.50%	3	3.50%	86	100.00%
Years of service of respondents	83	96.50%	3	3.50%	86	100.00%

Source: SPSS data analysis output, 2016

Table 4.2.2 Department respondents were working in vs. Level of Education Cross Tabulation

Department respondents were working in vs. Level of Education Cross Tabulation					
		Level of Education			Total
		Diploma	Degree	Masters Degree	
Department respondents were working in	Credit Appraisal and Portfolio Management	0	6	13	19
	Credit Management	0	6	12	18
	Finance	1	5	3	9
	Internal Audit	0	9	5	14
	President Office	0	0	2	2
	Program Management Office	0	1	0	1
	Risk & Compliance Management	0	13	7	20
Total	Count	1	40	42	83
	% of Total	1%	48%	51%	100%

Source: SPSS data analysis output, 2016

Table 4.2.2 shows that above half of the respondents have masters degree and 48% of the respondents have first degree. Moreover, as shown in Table 4.1.3 below, the working experience of the respondents in the bank is 16 years and above for about 45% of the respondents. 32% of the respondents serve the bank for 5-10 years. Overall, about 77% of the respondents have 5 years and above working experience in the bank.

Analysis of educational background and years of service indicates the respondents are equipped with both the necessary qualification and experience to understand the operational risk of the bank. Hence, it can be concluded that their response to the questionnaire are valid taking into account their exposure to the management of operational risk which is inherent in their day to day activities.

Table 4.2.3: Department respondents were working in vs. Years of service Cross Tabulation

Department respondents were working in vs. Years of service Cross Tabulation							
			Years of service				Total
			<5	5-15	16-25	26-40	
Department respondents were working in	Credit Appraisal and Portfolio Management	Count	7	6	7	0	20
		% of Total	8.4%	7.3%	8.4%	0.0%	24.1%
	Credit Management	Count	3	7	7	0	17
		% of Total	3.7%	8.4%	8.4%	0.0%	20.5%
	Finance	Count	1	2	4	2	9
		% of Total	1.2%	2.4%	4.8%	2.4%	10.8%
	Internal Audit	Count	1	4	7	2	14
		% of Total	1.2%	4.8%	8.4%	2.4%	16.9%
	President Office	Count	0	0	2	0	2
		% of Total	0.0%	0.0%	2.4%	0.0%	2.4%
	Program Management Office	Count	0	0	1	0	1
		% of Total	0.0%	0.0%	1.2%	0.0%	1.2%
	Risk & Compliance Management	Count	7	8	5	0	20
		% of Total	8.4%	9.6%	6.0%	0.0%	24.1%
		Count	**19**	**27**	**33**	**4**	**83**
		% of Total	**23%**	**32%**	**40%**	**5%**	**100%**

Source: SPSS data analysis output, 2016

Table 4.2.3 shows the departments the respondents were working in. The respondents from Risk and Compliance management and Internal Audit together are 41% of the total respondents. 45% of the respondents are from Credit Management, Credit Appraisal and Credit Portfolio management. The remaining small portion of the respondents was from Finance, President Office, and Program Management Office.

4.2.2. Validity and Reliability Analysis

The items of the questionnaire were developed based on thorough review of both theoretical and empirical literatures to ensure its validity. Likewise, repeated discussions were made with the risk personnel of the bank to have deep insight of the subject matter and to contextualize the study variables. Moreover the questionnaire was pre-tested by Risk Management staff and their feedback was incorporated in the final questionnaire.

The reliability of the scales used within the questionnaire is evaluated using Cronbach's alpha. It allows measuring the reliability of different variables. The questionnaire adopted for this study contains 69 statements representing each of the three aspects of risk management. Cronbach's alpha is used to estimate how much variation in scores of different variables is attributable to chance or random errors. Cronbach's alpha values were computed for multi item scales for individual factors, between the dimensions and for the whole questionnaire. The Cronbach's alpha was used as measure of reliability. In this model the alpha coefficient ranges from 0 to 1. The higher the score, the more reliable scale is, Cooper and Schindler (2003) noted that a score of 0.7 is acceptable reliability coefficient. The following table shows the reliability statistics of the Cronbach's alpha values computed.

Table 4.2.4 Cronbach's Alpha

Variables	Cronbach's Alpha Based on Standardized Items	No. of Items
Individual variables:		
1.1. Risk Governance	0.897	6
1.2. Oversight	0.841	6
1.3. Risk Management Approach	0.820	5
1.4. Corporate ORM Function	0.878	8
2.1. Risk Identification and Assessment	0.843	6
2.2. Key Operational Risk and Performance Indicators	0.866	4
2.3 Operational Risk Control and Mitigation	0.898	11
2.4. Business Resiliency and Continuity	0.907	5
2.5 Operational Risk Reporting and Disclosure	0.885	10
3. Risk Culture	0.895	8
The three dimensions:		
The Risk Environment	0.948	25
Internal Control	0.919	36
Risk Culture	0.893	8
The entire questionnaire		
All Variables	0.977	69

Source: SPSS data analysis output, 2016

Hence, the Cronbach's Alpha values for individual factors as well as for the entire 69 items of the questionnaire results are greater than the 0.7 minimum acceptable value. We can therefore conclude that the items of the questionnaire are internally consistent and reliable.

4.3. Operational Risk Management Practices of Commercial Bank of Ethiopia

The responses to the basic research questions are categorized under the three major factors of the Operational Risk Management framework: The Operational Risk Management Environment, The Internal Control and The Risk Culture. Detail analysis and discussions of each factor are presented in the following sections.

4.3.1. The Operational Risk Management Environment

In the Operational Risk Management Environment we will see the efforts and commitment of the board and senior management to establish sound operational risk management framework. The Risk Management Environment is the foundation of the other risk management

components by providing discipline and structure. It has a pervasive influence on the way business activities are structured, objectives established and risks managed.

In the following sections, the risk governance, the risk oversight, the risk management approach and the established risk management structure, which are the components of the operational risk management environment, will be presented in detail.

Table 4.3.1: Risk Governance

Risk Governance	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
The Board and Senior Management approved and update Operational Risk Management (ORM) framework.	83	1.2	3.6	21.4	35.7	38.1	4.06	0.92
The bank has an ORM system that is conceptually sound and is implemented with integrity.	83	-	14.1	24.7	42.4	18.8	3.66	0.95
The Board and Senior Management have clearly articulated governance structure, responsibilities and accountabilities.	83	-	13.1	22.6	33.3	31.0	3.82	1.02
The Board and Senior Management ensure all employees are aware of the bank's approach to risk management.	83	2.4	21.2	40.0	24.7	11.8	3.22	0.99
There is an established escalation line and issues escalated dealt with swiftly and decisively.	83	1.2	18.3	31.7	39.0	9.8	3.38	0.94
There is appropriate and adequate organizational structure and process to implement strong risk culture.	83	-	15.7	26.5	39.8	18.1	3.60	0.96
Average Mean							**3.62**	

Source: SPSS data analysis output, 2016

The effectiveness of the board and senior management in risk management can be measured by the established risk governance framework. CBE in this regard has good performance as reflected by average mean of the risk governance factors which is 3.62. As per Best and Khan, (1995) the average mean falls under the range 'good'. Majority of the respondents agree on the statement 'The Board and Senior Management approved and update Operational Risk Management (ORM) framework'. Moreover, above 57% of the respondents agree that the bank is in full or substantial compliance with items 1, 2, 3 and 6. The mean values indicate that all of the factors are significant as their values are average and above in all cases.

The responses for item 4 and 5, on the other hand, fall under the 'average' range indicating the board and senior management need to work more in creating awareness among employees and strengthening escalation line of issues affecting the bank's operations. Risk awareness and an appropriate level of risk training should be provided to all employees, compatible with their functions and levels of responsibility for effective management of operational risk.

The view from the senior management, however, is that risk governance is an area of development and the implementation of the above six statements is at medium or partial compliance level.

Table 4.3.2: Risk Oversight

Risk Oversight	**No.**	**NC %**	**PC %**	**MC %**	**SC %**	**FC %**	**Mean**	**Std. Dev**
The Board oversees Senior Management to ensure that policies, processes, systems are implemented effectively at all decision levels.	83	2.4	6.0	23.8	40.5	27.4	3.85	0.98
The Board ensures that the bank's (ORM) Framework is subject to effective independent review by audit or other appropriately skilled parties.	83	4.8	13.3	34.9	28.9	18.1	3.42	1.08
The Board has approved risk appetite and tolerance limits for aggregate and specific operational risks.	83	10.8	7.2	28.9	34.9	18.1	3.42	1.19
The Board has established clear lines of management responsibility and accountability for implementing a strong control environment.	83		11.9	26.2	42.9	19.1	3.69	0.92
Senior Management has implemented a clear, effective and robust governance structure which is conducive to transparent and consistent lines of responsibilities.	83	3.5	11.8	35.3	38.8	10.6	3.41	0.96
The bank utilizes a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports.	83	3.7	14.6	32.9	28.1	20.7	3.48	1.09
Average Mean							**3.55**	

Source: SPSS data analysis output, 2016

The average mean value of the risk oversight factors is rated as good and individual mean of the factors range between 3 and 4. Individual factors mean values are closer to each other

indicating these factors have similar level of significance. Less than 50% of the respondents agree that the bank is in substantial or full compliance with factors 2, 5 and 6. Moreover, a relatively high proportion of the respondents (10.8%) have replied that the board is not in compliance with regards to approving risk appetite and tolerance limits for aggregate and specific operational risks (which is item No. 2).

The feedback from senior management is consistent with the above findings. The bank is yet to have a clear risk appetite and tolerance statement. The survey of the National Bank of Ethiopia (NBE, 2009) also identified that the banks' policies do not define limits and communication of risk appetite is low. CBE, therefore, should have a robust process to set these limits and should be able to adjust in response to changing circumstances. Sound business practice is the board of directors approves and reviews a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

The bank needs to determine its appetite for different types of risks taking into consideration its capacity to manage such risks. Business objectives need to be developed in line with that risk appetite. Moreover, the bank doesn't have a dedicated operational risk committee to oversee risks and reports from the risk management function and enforce action plans.

Table 4.3.3: Risk Management Approach

Risk Management Approach	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
Framework has clearly articulated the roles and responsibilities of the three lines of defense (1) the business lines (2) the Corporate Operational Risk Management Function, (3) independent review or Internal Audit.	83	2.4	8.2	28.2	30.6	30.6	3.79	1.05
Business Units identify and manage the risks inherent to the products, activities, processes and systems.	83	1.2	3.6	36.1	39.8	19.3	3.72	0.86
The ORM Function performs independently and is responsible for the design and implementation of the bank's ORM framework.	83	2.4	11.8	31.8	44.7	9.4	3.47	0.91
Internal audit coverage includes opinions on the overall appropriateness and adequacy of the implemented ORM Framework and associated governance processes of the bank.	83	6.0	11.9	39.3	36.9	6.0	3.25	0.96
Internal audit evaluates whether the ORM Framework meets organizational needs and supervisory expectations.	83	10.8	18.1	30.1	32.5	8.4	3.1	1.13
Average Mean							**3.47**	

Source: SPSS data analysis output, 2016

The average mean value of the factors in the table above is rated as good, however, individual mean values of item 4 and 5 (related to internal audit) fall under average rating. The feedback from senior management is consistent with the above findings.

About 61% of the respondents agree at full or substantial level on the establishment of framework for the adoption of the three lines of defense model and this statement has the highest mean value of 3.79. This is a demonstration of the bank's adoption of the three lines of defense model as a Risk Management Approach and its above average operation.

Majority of the respondents also agreed business units were responsible for the management of operational risks inherent to their units' functions. Although the risk management function plays a central role in setting policy and overseeing the program, business units remain in the front line where risks are taken, and it is important that they understand and take responsibility for managing risk.

As mentioned above less than 50% of the respondents agree that the bank is in substantial or full compliance with these factors with regards to the performance of internal audit. It should be the duty of internal audit to evaluate whether the ORM Framework meets organizational needs and supervisory expectations as well as to provide opinion on the overall appropriateness and adequacy of the implemented ORM Framework and associated governance processes of the bank. Besides, internal audit's coverage should be adequate to independently validate and verify that the Framework and ORM has been implemented as intended and is functioning effectively. However, the coverage is very low as the internal audit staff size is very small compared to the size of the bank.

The findings on internal audit support Kesjana and Hatice (2010) who identified that the majority of banks in North Cyprus tend to ignore the importance of internal auditing in risk management.

In the study of Nazanin and Kateryna (2015), it was reported that following the adoption of the 3LoD, the bank under study had very clear separation of roles and responsibilities between first and second line. The second line more and more fulfilled the tasks historically performed by third line as first line assumes ownership for risk management. This necessitated collaboration between risk management, risk control, compliance and audit to avoid duplication of efforts and hence the implementation of a risk based planning process.

Table 4.3.4: Corporate ORM Function (CORMF)

Corporate ORM Function (CORMF)	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
Policy/Procedures are in place over the roles, responsibilities and its mandate.	83	1.2	4.7	21.2	47.1	25.9	3.92	0.88
CORMF Provides an adequate and independent challenge to management and business lines inputs, outputs, risk management, measurement and reporting systems.	83	1.2	12.0	43.4	31.3	12.0	3.41	0.90
CORMF is independent and responsible for the design and implementation of the bank's ORM framework.	83	1.2	10.6	32.9	44.7	10.6	3.53	0.87
CORMF has operational risk officers/experts with clearly defined roles and responsibilities.	83	-	7.2	28.9	36.1	27.7	3.84	0.92
CORMF has reporting relationship with operational risk officers/experts within the business units with clearly delineated roles and responsibilities.	83	2.4	11.8	30.6	36.5	18.8	3.58	1.00
CORMF provides regular updates on the adherence to risk appetite and tolerance to Board and Senior Management	83	3.7	15.9	32.9	39.0	8.5	3.33	0.97
CORMF is appropriately equipped with skilled and experienced staff, and with required material and information processing resources to fulfill its responsibilities.	83	-	19.5	39.0	35.4	6.1	3.28	0.85
CORMF provides enterprise wide training for the first line of defense on the ORM framework.	83	2.5	18.5	30.9	35.8	12.3	3.37	1.01
Average Mean							**3.53**	

Source: SPSS data analysis output, 2016

The average mean value of CORMF factors is 3.53 and is rated as good. However, more than 50% of the respondents do not agree that the CORMF is in substantial or full compliance with four or half of the factors. The feedback from senior management is consistent with the above findings, besides it was confirmed the CORMF failed to provide regular updates on the adherence to risk appetite and tolerance to Board and Senior Management. The rest of the factors are explained below.

The first factor is the main duty of the CORMF which is to provide an adequate and independent challenge to management and business lines inputs, outputs, risk management, measurement and reporting systems.

The second factor is on the competence of staff and resources of the CORMF. The bank needs to have risk management professionals who have adequate business experience, are highly competent communicators, and are proficient in all aspects of risk theory, including economics, financial theory, mathematics and statistics, information science, and information technology. The bank should develop a thorough understanding of the knowledge, skills and expertise required of those involved in risk management to perform their roles successfully.

The last factor is on training for the first line of defense on the ORM framework. An appropriate level of operational risk training should be available at all levels throughout the bank. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended. The bank should organize training initiatives and should encourage and financially support employees' individual efforts to keep abreast of developments in their areas of expertise through courses, conferences, journals, memberships, and other channels.

4.3.2. The Internal Control

Internal control is considered to be an instrument in handling risks that could prevent an organization from attaining its objectives. Internal control ensures effective operations, high quality internal and external reporting, organization's compliance with laws, regulations and internal guidelines, including the organization's value and codes of ethics (BCBS 195, 2011). The internal control process in the bank is further divided into five risk management processes which are described as follows.

Table 4.3.5: Risk Identification and Assessment

Risk Identification and Assessment	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
The bank has identified and communicated its financial, operational and compliance objectives.	83	1.2	6.0	22.6	51.2	19.0	3.81	0.86
Risk identification and assessments are clearly linked to inherent risks on the financial, operational and compliance objectives of the bank.	83	1.2	4.8	36.9	38.1	19.0	3.69	0.88
An independent challenge is in place to ensure accuracy, completeness, timeliness and reliability of the internal operational risk events.	83	2.4	10.8	42.2	30.1	14.5	3.43	0.95
Business units regularly conduct risk assessments and perform root cause analysis and corrective actions on significant internal loss events.	83	4.7	10.6	37.6	35.3	11.8	3.39	0.99
The bank has a systematic tracking of relevant operational risk data including material losses by business units.	83	6.0	11.9	47.6	29.8	4.8	3.15	0.91
The bank quantifies its exposure to operational risk by using the output of its risk assessment tools as inputs into a model that estimates operational risk exposure.	83	9.5	11.9	40.5	28.6	9.5	3.17	1.07
Average Mean							**3.44**	

Source: SPSS data analysis output, 2016

The average mean value of the factors of the risk identification and assessment component is 3.44 which has a rating of good. Majority of the respondents agree that the bank has identified and communicated its financial, operational and compliance objectives, as revealed by the highest mean of 3.81. The second highest mean of 3.69 is for the risk identification process is linked to inherent risks on the financial, operational and compliance objectives of the bank.

The responses for the rest of the factors by more than 50% of the respondents are the bank is not in substantial or full compliance with any of these factors. In addition a noncompliance response by 9.5% of the respondents was given for the last factor indicating the challenges of the bank in measuring its operational risk. Business units have the best knowledge of their risks and processes hence they should play a major role in risk identification if their operational risk management awareness is enhanced. The feedback from senior management is consistent with the above findings.

Table 4.3.6: Key Operational Risk and Performance Indicators (KRIs and KPIs)

Key Operational Risk and Performance Indicators	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
Business units identify both qualitative and quantitative KRIs and KPIs which are aligned with the units inherent operational risks	83	4.8	11.9	39.3	35.7	8.3	3.31	0.96
KRIs and KPIs are paired with escalation triggers to warn when risk levels exceed acceptable ranges and prompt mitigation plans.	83	8.4	15.7	37.3	33.7	4.8	3.11	1.01
The bank uses statistics and/or metrics to provide insight into operational risk position.	83	6.0	7.2	44.6	26.5	15.7	3.39	1.03
An independent challenge is in place to ensure the accuracy, completeness, timeliness and reliability of the KRI identified by the first line of defense/business units	83	4.9	15.9	41.5	32.9	4.9	3.17	0.93
Average Mean							**3.25**	

Source: SPSS data analysis output, 2016

Four measures were considered to assess the use of Key Operational Risk and Performance Indicators as part of the risk management process and more than 50% of the respondents indicated that the bank is in substantial or full compliance with the use of none of these factors. It can also be seen from the table above that there is no big difference among the means of the four questions, which indicates that respondents viewed fairly well each of these questions. The view of senior management is consistent with the above findings and it was acknowledged that the bank is not properly using KRIs as risk management tool and implementation of all of the above statements is at partial compliance level.

The overall mean value of these factors is 3.25 and has a rating of 'average'. The bank should make use of KRIs in providing information on the risk of potential future losses. KRIs should make it possible to identify areas with elevated risks early on and to take appropriate measures. They permit statements to be made on trends and can serve as indicators in an early-warning systems, e.g. in combination with a traffic-light system (red, yellow, green).

Hence, effective indicators are closer to the root cause of event and provide more time to management for proactive action. It is the responsibilities of both Processes and the CORMF to work towards improving the use of KRIs and KPIs.

The findings on the use of KRIs in South African Banks is similar in that they were not suitably prepared to implement a key risk indicator management process (Young, 2012). Those banks appeared not to be fully aware of the value and benefits that the successful implementation of a KRI management process could ensure.

Table 4.3.7: Operational Risk Control and Mitigation

Operational Risk Control and Mitigation	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
The Bank conducts regular evaluation of compliance to policy/procedure and regulations to ensure required authorized approvals and accountability are maintained.	83	1.2	8.3	25.0	47.6	17.9	3.73	0.90
The Internal controls for operational risk include close monitoring of adherence to assigned risk limits.	83	1.2	9.5	41.7	34.5	13.1	3.49	0.89
Areas of potential conflicts of interest are proactively identified, minimized, and are subject to careful independent monitoring and reviews.	83	3.6	15.5	48.8	26.2	6.0	3.15	0.89
The bank has implemented adequate segregation of duties and check and balance, and dual control on required areas.	83	-	9.4	21.2	47.1	22.4	3.82	0.89
The Bank's Internal controls for operational risk incorporated the following:								
a) Safeguards for access to, and use of, the bank's assets and records.	83	1.2	4.7	25.9	36.5	31.8	3.93	0.94
b) Appropriate staffing level and training to maintain expertise at all levels.	83	2.4	7.1	30.6	44.7	15.3	3.64	0.91
c) Regular verification and reconciliation of financial transactions and accounts.	83	-	4.8	23.8	50	21.4	3.88	0.80
d) A vacation/leave policy for all employees.	83	-	12	30.1	36.1	21.7	3.67	0.95
e) Information Assets identification, user access level control unauthorized access prevention	83	-	5.9	22.4	48.2	23.5	3.89	0.83
f) Cyber-attack, database integrity, database activity management, testing of similar attempts	83	2.4	17.1	25.6	42.7	12.2	3.45	0.99
6. The bank has an integrated approach to identifying, measuring, monitoring all information assets, technological devices and infrastructure risks.	83	2.4	10.8	38.6	37.3	10.8	3.43	0.91
Average Mean							**3.64**	

Source: SPSS data analysis output, 2016

As shown in the table above the average mean value of operational risk control and mitigation factors is 3.64 which is good and individual mean values range between 3 and 4. Specific to the control activities listed under item 5, more than 50% of the respondents agree that the bank has substantially or fully complied with except for the last factor which is IT related. These are traditional control activities which have been in existent before establishing risk management as separate function. These control measures facilitate the smooth running of the bank in achieving its objectives and goals. On the other hand factors 2, 3 and 6 have a lower compliance rate as more than 50% of the respondents rate them below substantial or full compliance. The feedback from senior management is consistent with the findings above.

The study indicates lower level of monitoring of adherence to assigned risk limits and this could result in frequent breaches of these limits. Conflicts of interest are not also dealt with proactively as per the majority of the responses. The avoidance of any form of conflict of interest is a requirement of sound risk management. Preventing conflict of interest is achieved through putting in place key checks and balances. Most importantly any risk taking decision should be separated from the risk assessment and controls over it, i.e., those functions should be independent. The risk management function, in addition to reporting to the senior management, needs to have a direct access to the Board to maintain its independence.

The last factor with lower rate of compliance is on the level of integrated approach the bank has to identifying, measuring, monitoring all information assets, technological devices and infrastructure risks. The bank has also challenges in establishing adequate controls on cyber-attack, database integrity, and database activity management as well as testing of similar attempts. Acknowledging these challenges, a dedicated IT unit is recently established under the risk management function.

Nazanin and Kateryna (2015) have also identified that there is the risk of accessibility, competency, security and development that are challenging within the IT system risk for the bank under their study. Cyber-attacks and security breaches are increasing and have a high threat level to the bank.

Table 4.3.8: Business Resiliency and Continuity

Business Resiliency and Continuity	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
The bank has established business continuity plans, taking into account different types of plausible scenarios of vulnerability.	83	3.6	14.3	29.8	41.7	10.7	3.42	0.98
Plausible disruptive scenarios are assessed for their financial, operational and reputational impact.	83	3.7	17.1	32.9	32.9	13.4	3.35	1.04
The bank has contingency strategies, recovery/resumption procedures, and communication plans for informing management, employees, and all stakeholders.	83	7.2	10.8	36.1	34.9	10.8	3.31	1.05
The bank periodically reviews its continuity plans to ensure contingency strategies relevance to prevailing vulnerabilities.	83	8.5	13.4	34.1	30.5	13.4	3.27	1.12
Regular awareness creations are implemented to ensure staff can effectively execute contingency plans.	83	13.4	23.2	29.3	25.6	8.5	2.93	1.17
Average Mean							**3.26**	

Source: SPSS data analysis output, 2016

The overall mean of the factors here is rated average. The bank has performed the least in the Business Resiliency and Continuity. 52.4% of the respondents fully or substantially agree only on the fact that the bank has established business continuity plans, taking into account different types of plausible scenarios of vulnerability. The feedback from senior management is consistent with the above findings confirming that the bank has business continuity plan but subsequent actions are not taken to enable the bank manage a crisis situation.

For the other four factors the majority of the respondents indicated that the bank is not in substantial or full compliance with any of them. Moreover, 13.4% of the respondents replied that regular awareness creations are not implemented to ensure staff can effectively execute contingency plans as indicated in their response for item 5. The mean value for item 5 is 2.93 which is the least from the 5 factors.

Table 4.3.9: Operational Risk Reporting and Disclosure

Operational Risk Reporting and Disclosure	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
The bank has maintained operational risk reporting system to the Board and stakeholders.	83	1.2	9.6	15.7	43.4	30.1	3.92	0.98
Has reporting thresholds for internal operational risk events and monitors to ensure adherence.	83	1.2	10.8	33.7	37.3	16.9	3.58	0.94
Incorporates internal loss data, in a complete and timely manner, into the operational risk reporting for capital impact analysis.	83	2.5	10.0	46.3	30.0	11.3	3.38	0.91
Incorporates breaches of the bank's risk appetite and tolerance statement.	83	4.9	8.5	42.7	32.9	9.8	3.83	4.48
Includes results of relevant assessments of business environment factors, risk and control self-assessments and other internal control factors.	83	9.5	33.3	41.7	14.3	1.2	4.1	4.49
Dashboard is created to summarize key information and highlight major events for efficient communication to Board and Senior Management and other stakeholders.	83	6.0	15.7	28.9	38.6	10.8	3.33	1.06
The results of monitoring activities are included in regular management and board reports,	83	1.2	12.2	24.4	45.1	17.1	3.65	0.95
Findings in operational risk reports are appropriately assigned and associated with action items to address deficiencies.	83	2.4	7.3	26.8	47.6	15.9	3.67	0.92
The bank publicly discloses relevant ORM information	83	14.3	25.0	28.6	25.0	7.1	2.86	1.16
The bank discloses its ORM framework in a manner that allows stakeholders and counterparties to determine whether it identifies, assesses, monitors and mitigates operational risks effectively.	83	3.7	24.4	29.3	30.5	12.2	3.23	1.07
Average Mean							**3.56**	

Source: SPSS data analysis output, 2016

The average mean value of Operational Risk Reporting and Disclosure factors is 3.56 which is rated as good. The highest mean value of 4.1 is obtained for item 5 which is 'the bank includes results of relevant assessments of business environment factors, risk and control self-assessments and other internal control factors'. However, 9.5% of the participants responded the bank is not at all in compliance with this factor.

Only items 1, 2, 7 and 8 got a response of the bank is in substantial or full compliance by more than 50% of the respondents. This indicates that majority of the factors under operational Risk Reporting and Disclosure are not well addressed by the bank. Special attention should be given to publicly disclosing relevant ORM information as it has the lowest mean value of 2.86 whereas the activity is very important in terms of awareness creation as well as control of risk by the staff. The other areas which need attention are completeness and correctness of data, consistent reporting of breaches of control, reporting of the results of risk assessments using different tools and the use of appropriate channels of communication.

The senior management acknowledged the bank needed to work more towards operational risk reporting and disclosure. It was recognized adequate and regular internal risk reporting was not made and information sharing media are not well developed. The banks didn't also disclose relevant ORM information to its stakeholders.

4.3.3. The Risk Culture

Beyond setting the right policies and structure, risk culture plays a major role for the success of an organization in its risk management. The bank must continuously develop a culture of understanding risk, recognizing the importance of risk management, and carrying personal responsibility and accountability for identifying and managing risks. The findings on risk culture factors are presented in the table below.

Table 4.3.10: Risk Culture

Risk Culture	No.	NC %	PC %	MC %	SC %	FC %	Mean	Std. Dev
The Board has established a code of conduct that sets clear expectations for integrity and ethical values of the highest standard, acceptable business practices and prohibited conflicts.	83	1.3	7.5	21.3	37.5	32.5	3.92	0.98
Setting business objectives is accompanied by identification of inherent risks and their mitigations to achieve the objectives.	83	4.9	4.9	22.2	45.7	22.2	3.75	1.02
The bank employees well understand their roles and responsibilities for risk as well as their authority to act.	83	4.9	7.3	40.2	39	8.5	3.39	0.93
There is strong and consistent Board and Senior Management support for risk management and ethical behavior.	83	2.4	11.0	30.5	39	17.1	3.57	0.98
Individuals and business units are measured or incentivized based on their risk performance against the bank's long-term objectives.	83	10.8	24.1	31.3	27.7	6.0	2.94	1.10
Risk management function is well-resourced and staffed with sufficiently skilled human resources.	83	6.0	12.0	38.6	32.5	10.8	3.3	1.02
Breaches are monitored and escalated to Senior Management in a timely manner.	83	3.7	15.9	32.9	40.2	7.3	3.32	0.95
There is an overall strong culture of risk management and ethical business practices	83	1.2	14.5	38.6	38.6	7.2	3.36	0.86
Average Mean							**3.44**	

The average mean of Risk Culture factors is 3.44 and falls under the good rating category. The mean values of these factors range from 2.94 to 3.92. However, only 3 out of the 8 factors have more than 50% of the respondents who agree that the bank is in substantial or full compliance. The feedback from the senior management is consistent with these findings and it was acknowledged that implementation is at partial compliance level for the majority of the factors.

The existence of a code of conduct established by the board was substantially or fully agreed by about 70% of the respondents and has a mean value of 3.92 which is the highest among the risk culture factors.

Only 48% of the respondents substantially or fully agree that the bank employees well understand their roles and responsibilities for risk as well as their authority to act. A good risk-aware culture ensures employees and management at all levels of the bank are aware of their individual responsibility and accountability in identifying and managing risks.

Risk performance based incentive has the least mean value among the risk culture factors. This factor is again not supported by 10.8% of the respondents as they responded the bank is not at all in compliance. A sound business practice is to align compensation policies to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. Compensation policies should also appropriately balance risk and reward.

Incentives and compensations to employees and management should be on the basis of long – term value added to the bank. Some incentive compensation plans and business targets may encourage excessive risk taking. At all levels of the bank, excessive focus on short-term profit without regard to risk and longer-term financial impact is fatal to the survival of the bank. Achievement of profitability and any other targets of business units should be measured against the bank's exposure to risks due to their actions.

The last factor is a general question about Risk Culture, and the mean value of the responses to this question is 3.36, which supports the above statements regarding appropriate risk culture. The fact that there is strong and consistent board and senior management support for risk management and ethical behavior, as supported by the majority of the respondents, indicate that risk culture is growing within the bank.

4.3.4. Challenges of Maintaining Effective Operational Risk Management

Operational risk management in banks is evolving and continuous improvement in the area is expected from banks (Deloitte, 2013). As presented in the discussion above the bank has overall compliance level of average and good in implementation of the operational risk management principles. However, the data analysis indicates that the aggregate substantial and full compliance agreement is less than 50% for the bank's practices on the following individual factors. Discussion of these factors and their implications on operational risk management is presented below. This discussion is also substantiated by the data gathered through interview.

- The bank doesn't have dedicated operational risk committee both at board level and senior management level which should have been enforcing the awareness creation, capacity building and proper reporting of the operational risk management process.
- The bank doesn't have a statement of risk appetite and tolerance limits. The bank should have a robust process to set these limits and should be able to adjust in response to changing circumstances. The bank needs to determine its appetite for different types of risks taking into consideration its capacity to manage such risks. Business objectives need to be developed in line with that risk appetite.
- Awareness of operational risks of the bank among employees is low. It is important that business units understand and take responsibility for managing risk as they remain in the front line where risks are taken.
- Though the bank has implemented the three lines of defense risk governance model, this model is not adequately cascaded down to the lower business units. Either the second or the third line of defense are missing in some business units and staff with control functions lack independence as they report to their respective business unit.
- The reporting line of the risk management function is to the senior management and its independence might be impaired unless it is granted direct access to the board.
- The risk management function's capacity is limited due to inadequate human and other resources. The bank should adequately resource the risk management function with skilled human resource and other materials to enable it effectively carry out its responsibilities in

creating awareness and providing training, risk monitoring and reporting and the overall risk management role.

- Effective risk management relies on a robust technology infrastructure. The bank's risk management system lacks the capability to integrate and quickly analyze data across the bank; as a result risk experts perform these analyses using end-user computing tools, such as Excel spreadsheets. The lack of automation means that less time is available to devote to higher-value activities such as more in-depth risk analysis or discussions with the business units.
- Internal audit coverage is insignificant compared to the size of the bank as the unit has inadequate human resource to carry out its tasks.
- The bank's challenge in risk identification and assessment is mainly due to lack of comprehensive internal loss data which is a fundamental building block needed to develop loss history. Front line business units have limited awareness, human and materials resources including data processing system and incentives to maintain and disclose operational loss data. However, they should be an integral part of risk identification and management as they have the best knowledge of their risks and processes.
- The Bank is often encountered with high frequency low severity risk events but it is often low frequency high severity events that can jeopardize the existence of a bank. There is limited work on the identification and analysis of predictive key risk indicators and use of scenario analysis to simulate the impact of irregular events, due to lack of historical data.
- The bank is not properly making use of KRIs as a risk identification and assessment tool and in providing information on the risk of potential future losses. KRIs help to identify areas with elevated risks early on and to take appropriate measures. Their numbers should be limited and they should be tracked to analyze trends and to serve as indicators in an early-warning systems, e.g. in combination with a traffic-light system (red, yellow, green).
- Operational risk losses are usually less frequency high severity events and when they materialize the consequence is devastating. The business resiliency and continuity plan however does not incorporate contingency strategies, recovery/resumption procedures and communication plans. The plan should be regularly reviewed and awareness created.

- The risk awareness and risk culture to avoid incomplete and erroneous data reporting is low in the bank. However, the bank should consistently recognize operational losses and to the extent possible verify and reconcile number of losses and amount with the General Ledger. Any operational loss including regulatory penalties and fines over a defined threshold should be reported.
- Risk performance is not linked to evaluation of business strategy implementation. Aspiring to achieve the business targets, business units breach risk limits and internal controls the consequences of which might not be visible in the short term.
- Technology is rapidly advancing global and the world is becoming digital. CBE has been investing in automation and networking through implementation of interconnected applications software. Connection to the World Wide Web and local networks presents both opportunity and vulnerability unless comparable security measures are integrated, updated and monitored regularly.

CHAPTER FIVE

SUMMARY AND RECOMMENDATIONS

5.1. Summary

Managing and monitoring of operational risk is an integral part of CBE's risk management. Sound operational risk management is therefore considered as strategic tool used to achieve the bank's objectives. The bank is working towards establishing effective risk management practices compatible with the changing business environment and the requirements of regulatory bodies. The study attempted to examine the operational risk management practices of CBE in terms of the three major operational risk management components: the Risk Management Environment, the Internal Control and the Risk Culture.

The bank has established a risk management environment which is also the foundation of the other operational risk management components. The senior management has the overall responsibility for the management of all risk types wherein operational risk management is one of them. To ensure the effectiveness of operational risk management, the bank has created good Operational Risk management Environment that is reflected through its risk governance, risk oversight and risk management approach and the risk management function. The Board of Directors, Senior Management, the Risk and Compliance Function and individual Business Units have their respective roles in operational risk management.

The implementation of sound operational risk management practices with respect to operational risk management environment is good in most of the cases. The bank, however, has not provided adequate training to employees to raise their awareness and carry out their respective duties regarding operational risk management. Besides, the bank doesn't have a clear risk appetite and tolerance statement for operational risk. The contribution of internal audit in providing assurance on whether the ORM Framework meets organizational needs and supervisory expectations is limited. The risk management function has limitations in skills and resources to manage and monitor risks and provide trainings to other business units and employees of the bank.

Internal control is an important part of the bank's operational risk management and is exercised to handle risks that could prevent the bank from achieving its objectives. The implementation of the internal control system through risk identification and assessment, operational risk control and mitigation, and risk reporting and disclosure was good. However, the use of key operational risk indicators, development and updating of business resiliency and continuity plan, and complete, consistent and timely reporting are areas to improve. The bank has also challenges in risk identification and measurement, in developing methodologies to quantify operational risks and in establishing adequate controls on IT.

The bank has put efforts to create a strong risk culture among its employees as evidenced by the establishment of code of conduct, consistent board and senior management support for risk management and ethical behavior, and through assigning responsibility and accountability for identifying and managing risks. However, risk management is not aligned with performance evaluation and reward mechanisms which may result in poor risk management aspiring to achieve business targets. The risk management function is not well-resourced and staffed with sufficiently skilled human resources.

5.2 Recommendations

Based on the major findings of the study, the researcher recommends the following.

- There should be a dedicated operational risk committee to enable the bank deal with the growing operational risk challenges through providing strong leadership and promoting a risk-aware culture throughout the bank.
- Risk awareness and an appropriate level of risk training should be provided to all employees, compatible with their functions and levels of responsibility for effective management of operational risk. All employees need to understand how their risk taking behavior affects the attainment of the objectives of the bank.
- The management of operational risk should be the responsibility of senior management and all staff in all business lines in addition to the risk management function. The responsibility and accountability for risk management of each staff should be well documented and

communicated. Each employee needs to have a good understanding of the importance of risk management to the bank and his/her roles and responsibilities for risk management.

- The bank should adequately resource the risk management function with human and material resources. The bank needs to have risk management professionals who have adequate business experience and are proficient in all aspects of risk theory and information technology. The bank needs to have a well-developed risk infrastructure including risk applications, hardware and data sourcing.
- The Internal audit function, without jeopardizing its independence, should integrate with the risk management function in order to get an increased understanding of current and evolving key risks. The function should emphasize on risk based audits in addition to ad hoc and investigative audits.
- Operational risks when materializes can jeopardize the achievement of the bank's objectives be it profit, service excellence, service expansion, reputation and satisfaction of stakeholders. The development of business resiliency and continuity plan is hence to reduce the impact of such events. The bank should develop, test, update and ensure employees are aware of business continuity plans which would enable the bank respond to crisis situations.
- The bank needs to set up a system for consistent and comprehensive loss data gathering. The board of directors and senior management need to promote an approach of disclosure and transparency by setting an example, in stated policies, and through demanding regular and timely reporting.
- Effective risk management should be incorporated during objectives setting as well as performance evaluation of individuals and business units.
- Finally, as operational risk management is evolving, the bank needs to continuously improve this risk management function to meet the changes in the environment.

Suggestions for further Research

A comparative analysis research among commercial banks in Ethiopia on their operational risk management practices could indicate the level of the practice in the industry. It would therefore be an absolute delight to see a research done in this direction.

REFERENCES

Andersen, L.B., Maberg, S., Hägerwzx, D., Næss M.B. & Tungland, M. (2012), "The financial crisis in an operational risk management context – A review of causes and influencing factors", Reliability Engineering & System Safety, Vol. 105, pp. 3-12.

Apatachioae, A. (2014), "New challenges of the management of banking risks", Procedia Economics and Finance, Vol.15, pp. 1364-1373.

Atakelt Hailu Asfaw (2015), "Credit Risk Management Practice of Ethiopian Commercial Banks", European Journal of Business and Management, Vol.7, No.7.

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods and Practices, 2nd ed.

Basel Committee on Banking Supervision (2006), "International Convergence of Capital Measurement and Capital Standards", a Revised Framework, Geneva: A BIS Publication.

Basel Committee on Banking Supervision (BCBS), (2003), "Sound Practices for the Management and Supervision of Operational Risk".

Basel Committee on Banking Supervision (BCBS), (2011), "Principles for the Sound Management of Operational Risk".

Best J.W. & Khan J.V. (1995), "Research in Education", 7th ed., Prentice- Hall press, New York.

Birhanu Tsehay (2012), "Determinants of Commercial Banks Profitability: Empirical Evidence from the Commercial Banks of Ethiopia, AAU, Masters Thesis.

Chernobai, A., Jorion, P., & Yu, F. (2011), "The Determinants of Operational Risk in U.S. Financial institutions", Journal of financial and quantitative analysis, vol. 46, no. 6, pp. 1683–1725.

Cook, T. D. and Campbell, D. T. (1979), "Quasi-Experimentation: Design and Analysis for Field Settings", Rand McNally, Chicago, Illinois.

Cooper, D., & Schindler, P., (2006), "Marketing research", 3rd ed, New York: McGraw-Hill, Irwin

Creswell, J. W. (2010). "Research design: Qualitative, Quantitative and Mixed methods approaches", 2nd ed., California: sage publications.

Dam Dan Luy (2010), "Evaluation of Credit Risk Management: Policies and Practices in a Vietnamese Joint-Stock Commercial Bank's Transaction Office", Business Economics & Tourism.

Deloitte (2013), "Global risk management survey: Setting a higher bar", eighth edition.

Doughty, K. (2011), "The Three Lines of Defense Related to Risk Governance", ISACA Journal, Vol.5. pp. 1-3.

Fasika Firew (2012), "Commercial Bank operational risks management: Exploratory study on selected Ethiopian Commercial Banks", AAU, Masters Thesis.

Greuning, H. & Brajovic Bratanovic, S. (2003), "Analyzing and managing banking risk: a framework for assessing corporate governance and risk management", 2nd ed, Washington, DC

Habib Ahmed (2011),"Risk Management Assessment Systems: An Application to Islamic Banks", Islamic Economic Studies, Vol. 19 No. 1, pp. 63-86.

Hussein A. Hassan Al-Tamimi and Faris Mohammed Al-Mazrooei (2007), "Banks' risk management: a comparison study of UAE national and foreign banks", The Journal of Risk Finance Vol. 8 No. 4, pp. 394-409.

Jongh, E. and Vuuren, G. (2013), "A review of operational risk in banks and its role in the financial crisis", SAJEMS, Vol.16, No.4, pp.364-382.

Jacobus Y. and Joseph C. (2013), "Implementing A Risk Management Framework in Developing Markets, International Business & Economics Research Journal – June 2013 Vol. 12, No. 6

Jeet Singh and Preeti Yadav (2013), "Strategies for managing risks in banks", Acta de Gerencia Ciencia, Vol.1, No.2, pp. 6-20.

Kayed, R.N. and K.M. Mohamed (2009), "Unique risks of Islamic modes of finance: systemic, credit and market risks", Journal of Islamic Economics, Banking and 1 Finance, Vol. 5, No.3.

Keefe, B. & Pfleiderer, A. (2012), “Basel III: What It Means for the Global Banking System”, Banking and finance law review, pp. 407-426.

Kesjana Halili and Hatice Jenkins (2010), “Risk Management Practices of Commercial banks in the Absence of Political Settlement in North Cyprus”, Banking and Finance Letters, Vol. 2, No. 3.

KPMG, (2009), “The three lines of defense”, Accessed on 10 April 2016, from https://www.kpmg.com/RU/en/IssuesAndInsights/ArticlesPublications/Audit-Committee-Journal/Documents/The-three-lines-of-defence-en.pdf.

Mestchian Peyman(2003), “Operational Risk Management:The Solution is in the Problem”, 2nd edition.

Michael Power (2003), "The Invention of Operational Risk”, Accessed on 19 March 2016, https://www.researchgate.net/publication/30520467.

Nabweteme A. (2011), “Operational Risk Management, Organizational Environment and Organizational Performance at Stanbic Bank Uganda Limited”, Makerere University.

National Bank of Ethiopia (2010), “Commercial banks risk management guidelines”

National Bank of Ethiopia (2009), “Banking Industry Risk Management Survey Report”.

Nazanin Bagherzadeh and Kateryna Jöehrs (2015), “Operational Risk Management Improvements within Internal Control Frameworks”, Master’s Thesis.

Nordic Investment Bank (NIB) (2015), “Operational Risk Management Policy”, Accessed on March 22, 2016, www.nib.int.

OeNB and FMA (2006), “Guidelines on Operational Risk Management”, Otto-Wagner-Platz 3, 1090 Vienna, Austria.

Operational risk & compliance (2006), Vol. 7, pp. 27-29, London: Incisive Media publications.

Osborne, A. (2012), “Risk Management Made Easy”, Ventus Publishing Aps. ISBN 978-87-7681-984-2

Pulane Modiha (2011), “Critical evaluation of operational risk tools used in regulatory capital calculations”, University of Pretoria, Master’s Thesis for MBA.

Rao, Vandana and Dev, Asihish. (2006), “Operational Risk: Some Issues in Basel II AMA Implementation in US Financial Institutions”.

Reserve Bank of India, “Guidance Note on Management of Operational Risk”, Accessed on 19 March 2016, https://www.rbi.org.in/upload/notification/pdfs/66813.pdf.

Schwarts M. and Garliste, A. (2013), “The Operational Risk Management in Banking – Evolution of Concepts and Principles, Basel II Challenges”, Review of International Comparative Management, Vol. 14, No. 1, pp. 165-174.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004), Enterprise Risk Management – Integrated Framework

Thirupathi Kanchu and M. Manoj Kumar (2013), “Risk Management in Banking Sector - An Empirical Study”, International Journal of Marketing, Financial Services & Management Research, ISSN 2277- 3622, Vol.2, No. 2.

Tsion Fekadeselassie (2015), “Risk Management Practice of Ethiopian Commercial Banks”, AAU, Masters Thesis.

U.S. Securities and Exchange Commission, “Annual Report 2003”. Accessed on 19 March 2016, www.sec.gov.

Usha, J. (2008), “Operational Risk Management in Indian Banks in the Context of Basel II: A Survey of the State of Preparedness & Challenges In Developing The Framework Asia Pacific”, Journal of Finance & Banking Research Vol. 2. No. 2.

Young, J. (2012). “The use of key risk indicators by banks as an operational risk management tool: A South African perspective”, international conference, Helsinki.

APPENDIX

Annex I – Questionnaire

Addis Ababa University

College of Business and Economics

Graduate studies (EMBA program)

This questionnaire is prepared by a graduate student of Addis Ababa University with the aim of gathering data on a research topic "Assessment of Operational Risk Management Practice of CBE" as a partial fulfillment of the requirements for the degree of Executive Masters of Business Administration in Management (EMBA) at Addis Ababa University. The researcher would like to thank you in advance for your kind response by allotting your precious time in filling the questionnaire. As your responses have a great impact on the study findings, you are kindly requested to provide your genuine responses freely without mentioning your name. The information provided is to be used only for the sake of this study and will be kept strictly confidential.

Part I. Personal information

Instruction: Please circle the letter in the choices to indicate your response.

1. Sex:

A) Male B) Female

2. Age:

A) 18-29 B) 30-39 C) 40-49 D) 50-59 E) >60 years

3. Years of service:

A) <5 years B) 5-15 C) 16-25 D) 26-40 E) >40 years

4. Level of education:

A) Diploma B) Bachelor Degree C) Masters degree D) PhD

5. Department you are currently working in _____

Part II. Operational risk management evaluation questions

Please indicate the level of compliance of operational risk management practices of CBE with respect to the following statements by using a rating from 1 to 5 where **5= Fully Complied (FC); 4= Substantially Complied (SC); 3 = Moderately Complied (MC); 2= Partially (to a lower extent) Complied (PC); 1=Not Complied (NC).**

Read all the items thoroughly and please put a tick mark (√) in the space provided under the scale of your choice against each statement.

1. THE RISK MANAGEMENT ENVIRONMENT	**FC (5)**	**SC (4)**	**MC (3)**	**PC (2)**	**NC (1)**
1.1. Risk Governance					
1. The Board and Senior Management approved and update Operational Risk Management (ORM) framework.					
2. The bank has an ORM system that is conceptually sound and is implemented with integrity.					
3. The Board and Senior Management have clearly articulated governance structure, responsibilities and accountabilities.					
4. The Board and Senior Management ensure all employees are aware of the bank's approach to risk management.					
5. There is an established escalation line and issues escalated dealt with swiftly and decisively.					
6. There is appropriate and adequate organizational structure and process to implement strong risk culture.					
1.2 Oversight	**5**	**4**	**3**	**2**	**1**
1. The Board oversees Senior Management to ensure that policies, process, systems are implemented effectively at all decision levels.					
2. The Board ensures that the bank's (ORM) Framework is subject to effective independent review by audit or other appropriately skilled parties.					
3. The Board has approved risk appetite and tolerance limits for aggregate and specific operational risks.					
4. The Board has established clear lines of management responsibility and accountability for implementing a strong control environment.					
5. Senior Management has implemented a clear, effective and robust governance structure which is conducive to transparent and consistent lines of responsibilities.					
6. The bank utilizes a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports.					

1.3. Risk Management Approach	5	4	3	2	1
1. Framework has clearly articulated the roles and responsibilities of the three lines of defense (1) the business lines (2) the Corporate Operational Risk Management Function, (3) independent review or Internal Audit.					
2. Business Units identify and manage the risks inherent to the products, activities, processes and systems.					
3. The ORM Function performs independently and is responsible for the design and implementation of the bank's ORM framework.					
4. Internal audit coverage includes opinions on the overall appropriateness and adequacy of the implemented ORM Framework and associated governance processes of the bank.					
5. Internal audit evaluates whether the ORM Framework meets organizational needs and supervisory expectations.					
1.4. Corporate ORM Function (CORMF)	**5**	**4**	**3**	**2**	**1**
1. Policy/Procedures are in place over the roles, responsibilities and its mandate.					
2. CORMF provides an adequate and independent challenge to management and business lines inputs, outputs, risk management, measurement and reporting systems.					
3. CORMF is independent and responsible for the design and implementation of the bank's ORM framework.					
4. CORMF has operational risk officers/experts with clearly defined roles and responsibilities.					
5. CORMF has reporting relationship with operational risk officers/experts within the business units with clearly delineated roles and responsibilities.					
6. CORMF provides regular updates on the adherence to risk appetite and tolerance to Board and Senior Management					
7. CORMF is appropriately equipped with skilled and experienced staff and with required material and information processing resources to fulfill its responsibilities.					
8. CORMF provides enterprise wide training for the first line of defense on the ORM framework.					

Please explain if you have any issues you want to raise with respect to the operational risk management environment of CBE _____

_____

_____

_____

_____

2.INTERNAL CONTROL					
2.1. Risk Identification and Assessment	**5**	**4**	**3**	**2**	**1**
1. The bank has identified and communicated its financial, operational and compliance objectives.					
2. Risk identification and assessments are clearly linked to inherent risks on the financial, operational and compliance objectives of the bank.					
3. An independent challenge is in place to ensure accuracy, completeness, timeliness and reliability of the internal operational risk events.					
4. Business units regularly conduct risk assessments and perform root cause analysis and corrective actions on significant internal loss events.					
5. The bank has a systematic tracking of relevant operational risk data including material losses by business units.					
6. The bank quantifies its exposure to operational risk by using the output of its risk assessment tools as inputs into a model that estimates operational risk exposure.					
2.2. Key Operational Risk and Performance Indicators	**5**	**4**	**3**	**2**	**1**
1. Business units identify both qualitative and quantitative KRIs and KPIs which are aligned with the units inherent operational risks					
2. KRIs and KPIs are paired with escalation triggers to warn when risk levels exceed acceptable ranges and prompt mitigation plans.					
3. The bank uses statistics and/or metrics to provide insight into operational risk position.					
4. An independent challenge is in place to ensure the accuracy, completeness, timeliness and reliability of the KRI identified by the first line of defense/business units					
2.3 Operational Risk Control and Mitigation	**5**	**4**	**3**	**2**	**1**
1. The Bank conducts regular evaluation of compliance to policy/procedure and regulations to ensure required authorized approvals and accountability are maintained.					
2. The Internal controls for operational risk include close monitoring of adherence to assigned risk limits.					
3. Areas of potential conflicts of interest are proactively identified, minimized, and are subject to careful independent monitoring and reviews.					
4. The bank has implemented adequate segregation of duties and check and balance, and dual control on required areas.					
5. The Bank's Internal controls for operational risk incorporated the following: a) Safeguards for access to, and use of, the bank's assets and records.					
b) Appropriate staffing level and training to maintain expertise at all levels.					

c) Regular verification and reconciliation of financial transactions and accounts.					
d) A vacation/leave policy for all employees.					
e) Information Assets identification, user access level control unauthorized access prevention					
f) Cyber-attack, database integrity, database activity management as well as testing of similar attempts.					
6. The bank has an integrated approach to identifying, measuring, monitoring all information assets, technological devices and infrastructure risks.					
2.4. Business Resiliency and Continuity	**5**	**4**	**3**	**2**	**1**
1. The bank has established business continuity plans, taking into account different types of plausible scenarios of vulnerability.					
2. Plausible disruptive scenarios are assessed for their financial, operational and reputational impact.					
3. The bank has contingency strategies, recovery/resumption procedures, and communication plans for informing management, employees, and all stakeholders.					
4. The bank periodically reviews its continuity plans to ensure contingency strategies relevance to prevailing vulnerabilities.					
5. Regular awareness creations are implemented to ensure staff can effectively execute contingency plans.					
2.5 Operational Risk Reporting and Disclosure	**5**	**4**	**3**	**2**	**1**
1. The bank has maintained operational risk reporting system to the Board and stakeholders.					
2. Has reporting thresholds for internal operational risk events and monitors to ensure adherence.					
3. Incorporates internal loss data, in a complete and timely manner, into the operational risk reporting for capital impact analysis.					
4. Incorporates breaches of the bank's risk appetite and tolerance statement.					
5. Includes results of relevant assessments of business environment factors, risk and control self-assessments and other internal control factors.					
6. Dashboard is created to summarize key information and highlight major events for efficient communication to Board and Senior Management and other stakeholders.					
7. The results of monitoring activities are included in regular management and board reports.					
8. Findings in operational risk reports are appropriately assigned and associated with action items to address deficiencies.					
9. The bank publicly discloses relevant ORM information					
10. The bank discloses its ORM framework in a manner that allows stakeholders and counterparties to determine whether it identifies, assesses, monitors and mitigates operational risks effectively.					

Please explain if you have any issue you want to raise with respect to internal control of CBE

_____
_____
_____
_____
_____
_____

	3. RISK CULTURE	5	4	3	2	1
1.	The Board has established a code of conduct that sets clear expectations for integrity and ethical values of the highest standard, acceptable business practices and prohibited conflicts.					
2.	Setting business objectives is accompanied by identification of inherent risks and their mitigations to achieve the objectives.					
3.	The bank employees well understand their roles and responsibilities for risk as well as their authority to act.					
4.	There is strong and consistent Board and Senior Management support for risk management and ethical behavior.					
5.	Individuals and business units are measured or incentivized based on their risk performance against the bank's long-term					
6.	Risk management function is well-resourced and staffed with sufficiently skilled human resources.					
7.	Breaches are monitored and escalated to Senior Management in a timely manner.					
8.	There is an overall strong culture of risk management and ethical business practices					

Please explain if you have any issue you want to raise with respect to the risk culture of CBE

_____
_____
_____
_____
_____
_____

Thank you for your valuable time and participation!!!

Annex 2 - Interview Questions

1. How do you express the **risk governance structure**, the **oversight role of the Board** and the **focus given** to operational risk management in the Bank, in terms of:

    a) Implementation of approved operational risk management framework/Procedure;
    b) Establishment of operational risk board level committee;
    c) Evaluation of performance of the bank by board and senior management in achievement of financial, operational and compliance objectives;
    d) Establishment of sufficiently resourced and independent operational risk management and internal audit functions;
    e) Ensuring that senior management has a full understanding of the operational risk exposure of the bank.
    f) The role of NBE in the operational risk management of the bank;
    g) Compliance of the Bank in meeting the requirements of NBE regarding ORM.

2. How is the **operational risk management function** organized and performs:

    a) Roles responsibilities and accountability of business units, senior management , Internal Audit and corporate risk management function;
    b) Reporting relationship between the corporate units, business units, senior management and Board;

3. How do you evaluate the Bank's operational risks **identification**, **assessment** and **recording**:
    a) Manner and methods of potential risk identifications;
    b) Uniqueness of operational risk from other type of risks;
    c) Types and frequency of potential operational risks identification;
    d) Major causes and categories of potential operational risks;
    e) The Internal control effectiveness of the operational risks;
    f) Measurement methods and tools of the potential risks;
    g) Integration of operational risk management with Key performance indicators
    h) Data collection, validation and maintenance of risk events;

4. Awareness of Operational Risk

    a) The Board, the management and all employee;
    b) Monitoring performance with compliance;
    c) Identification and Assessment Operational risks on individual objectives

5. Monitoring and Control

    a) Controlling mechanism for operational risk in the bank?
    b) Follow-up of risk profile changes along time line?
    c) The role of internal control in preventing and reducing operational risks impact?
    d) The importance of communication in risk management?

6. How do you view the bank's operational risk exposures **relative to advancement of** information technology infrastructure and expansion of electronic services?

7. What can you say in general about your bank's **operational risk measurement and management** practices?
8. What do you think on **prevailing challenges** the bank encountered in measuring and managing operational risks?
9. Could you explain the overall CBE's **risk culture** concerning operational risks?