ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

OPERATIONAL RISK MANAGEMENT PRACTICES AT DASHEN BANK

BY

BEZAYE TSEHAY MOKONNEN

JUNE 2020

ADDIS ABABA, ETHIOPIA

OPERATIONAL RISK MANAGEMENT PRACTICE AT DASHEN BANK

BY

BEZAYE TSEHAY

A THESIS SUBMITTED TO ST. MARY'S UNIVERSITY SCHOOL OF GRADUATE STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MBA IN GENERAL MANAGEMENT.

JUNE, 2020

ADDISABABA, ETHIOPIA

ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

FACULTY OF BUSINESS

OPERATIONAL RISK MANAGEMENT PRACTICE AT DASHEN BANK

BY

BEZAYE TSEHAY

APPROVED BY BOARD OF EXAMINERS

----------	----------
Dean, Graduate Studies	**Signature**
----------	----------
Advisor	**Signature**
----------	----------
External Examiner	**Signature**
----------	----------
Internal Examiner	**Signature**

Declaration

I, Bezaye Tsehay, declare that this thesis entitled "Operational Risk Management Practices at Dashen Bank" is my original work, prepared under the guidance of Tilaye Kassahun (Dr.), and has not been submitted to St. Mary's University or any other institution of higher learning as a thesis and all sources of information have been dully acknowledged.

Researcher's Name	Date	Signature
_____	_____	_____

ENDORSEMENT

This thesis has been submitted to St. Mary's University, School of Graduate Studies for examination with my approval as a university advisor.

---------- ----------

Advisor **Signature**

St. Mary's University, Addis Ababa Jun, 2020

Table of Contents

Acknowledgments

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.Tilaye Kassahun, who tirelessly provided me with all the necessary advice, guidance and comments throughout this study.

I am thankful to all family, especially my father Tsehay Mokonnen, for their ideas, advices, unlimited support and encouragement.

Lastly, I am grateful to the Dashen Bank Management and staff members for providing me with the relevant information for this study.

List of Tables

List of Figures

ACRONYMS

AMA - Advanced Measurement Approach

BCBS - Basel Committee on Banking Supervision

BIS - Basic Indicator Approach

CORMF – Corporate Risk Management Function

COSO - The Committee of Sponsoring Organizations of the Tread way 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

DB – Dashen Bank

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 Dashen Bank (DB) 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 DB. 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 standardized questionnaires. 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 frequency, percentage, means and standard deviations was employed to interpret the study findings. 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, Operational Risk, Internal Control, risk management framework.*

CHAPTER ONE

1. INTRODUCTION

1.1 Background of the study

All investments involve some degree of risk. The risk arises from the occurrence of some expected or unexpected events in the economy or the financial markets. In finance, risk refers to the degree of uncertainty and/or potential financial loss inherent in an investment decision. In general, as investment risks rise, investors seek higher returns to compensate themselves for taking such risks.

Banks have to take risks all the time. Any bank has to take on risk to make money and they are facing many types of risks such as credit risk, market risk, and operational risk, liquidity risk, foreign exchange risk and business risk.

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. 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 (Osborne, 2012).

Risk management is all about making right decisions that contribute overall achievements of banks objectives by applying them both to functional areas and individual activity. Therefore, ensures mission, vision, and goals are met due diligence, accountability, Innovation and responsible risk-taking. (Andersen 2012)

Operational risk is defined as: 'The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.'

Operational risks range from the very small, for example, the risk of loss due to minor human mistakes, to the very large, such as the risk of bankruptcy due to serious fraud. Operational risk can occur at every level in an organization.

In Ethiopia banks are playing an important role as financial intermediaries in the economic growth process, channeling funds from savers to borrowers for investments. As financial intermediaries, banks play an important role in the operation of an economy.

Operational risk management, it is important to align it with the organization's risk appetite. The risk appetite will be influenced by the size and type of organization, its capacity for risk and its ability to exploit opportunities and withstand setbacks. This study is about operational risk management practice of banks in Ethiopia by taking Dashen bank.

1.2 Background of the organization

Dashen bank was found by eleven visionary shareholders and bankers with initial capital of birr 14.9 million in September 1995. Upon securing license from the national bank of Ethiopia, dashen opened its doors for service on the 1st of January 1996 with eleven fully-fledged branches.

Dashen bank coined its name from the highest peak in Ethiopia, mountain Dashen, and aspires to be unparalleled in banking services.

Headquartered in Addis Ababa, the bank is among the biggest private banks in Ethiopia. It operates through a network of more than 400+Branches, ten dedicated forex Bureaus, 350+ATM and 850 plus point-of-sale (pos) terminals spread across the length and breadth of the nation. It has established correspondent banking relationship with 462 banks covering 70 countries and 170 cities across the world.

1.3 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 Dashen bank.

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 DB against sound operational risk management principles. The operating inefficiency in banks leads to loss and failure. This inefficiency occurred as a result of poor risk assessment and handling mechanism. Without

effective risk assessment, proper risk handling mechanism and efficient operation, the life of the institution is not long.

Apart from this, it is observed that the banks set on the operational risk as a procedure but the controlling mechanism of a day to day operational activity is not to the accepted level., the implementation way of operational risk procedure is not satisfactory and also the management the operational risk process also is not the accepted level.

Due consideration the above literatures and observed gaps, this is therefore, the study is to examine operational risk management practices of DB against sound operational risk management principles in place. In addition, the motivation of this study is to filling the gap in the literature by providing evidence on risk management practices of Ethiopian Banks based on case study of DB.

Finally 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.

1.4 Research Question

The following basic research questions were considered in relation with statement of the problem.

1. How effective is the operational risk management practice of the bank?
2. To what extent internal control processes is adopted to manage operational risk of the Bank?
3. What is the level of risk culture created that supports the operational risk management of the bank?

1.5 Objectives of the Study

1.5.1 General Objective

The objective of this thesis is to assess the degree to which Dashen Bank 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.

1.5.2 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 practice of DB,

2 .To inspect the adequacy of internal control processes in operational risk management of DB and

3. To examine the level of risk culture created that supports the operational risk management of DB

1.6 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 DB.

1.7 Scope of the Study

The scope of the research focused on risk management, credit management, finance, internal audit and corporate banking staffs with a working experience of one or more years in the head office which is located around biherawi. However, other departments of the bank that are not mentioned in the above, junior staff, those newly employed staffs who are on apprentice program and employees of other branch offices will not include in the study because of for the sake of

quality and specialization and to cope with the available time and resource constraints, this study focuses only the operational risk management practice of Dashen Bank.

1.8 Limitations of the Study

It was very difficult to conduct this study specifically some of the employees, as they were very busy. Some of the staff were also not cooperative as far as completing the questionnaire was concerned, so that an extra effort needed to be made to persuade those staff to either cooperate or find replacements for themselves.

Since the respondents of this study came from Dasen Bank, the results obtained may have differed for other organizations. This could limit the generalizability of the results.

1.9 Organization of the Study

The study paper has 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 studies about operational risk, operational risk governance, the operational risk management process and regulatory frameworks. Chapter Three deals with the research design; the sample, population and participants; data collection and analysis; reliability and validity. Chapter four discusses validity and reliability analysis, cross tabulation descriptive analysis of the respondents, operational risk management practices of the bank, the operational risk management practices, the internal control and Chapter five introduces summary, conclusion and recommendation.

CHAPTER TWO

2 REVIEW OF LITERATURE

Introduction

In this chapter, the operational risk management practices in the case of DB were given analysis. Different literature were reviewed and the sources of literature were books, texts, journals, magazines, periodicals newspapers, reports of the regulatory body, internet and other media sources, previous research works and observations related to the subject under consideration

These helped to clarify and strengthen the research work and present the findings in an organized manner.

2.1 Theoretical Framework

2.1.1 Overview of Operational Risk Management

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).

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).

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).

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)

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.

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.

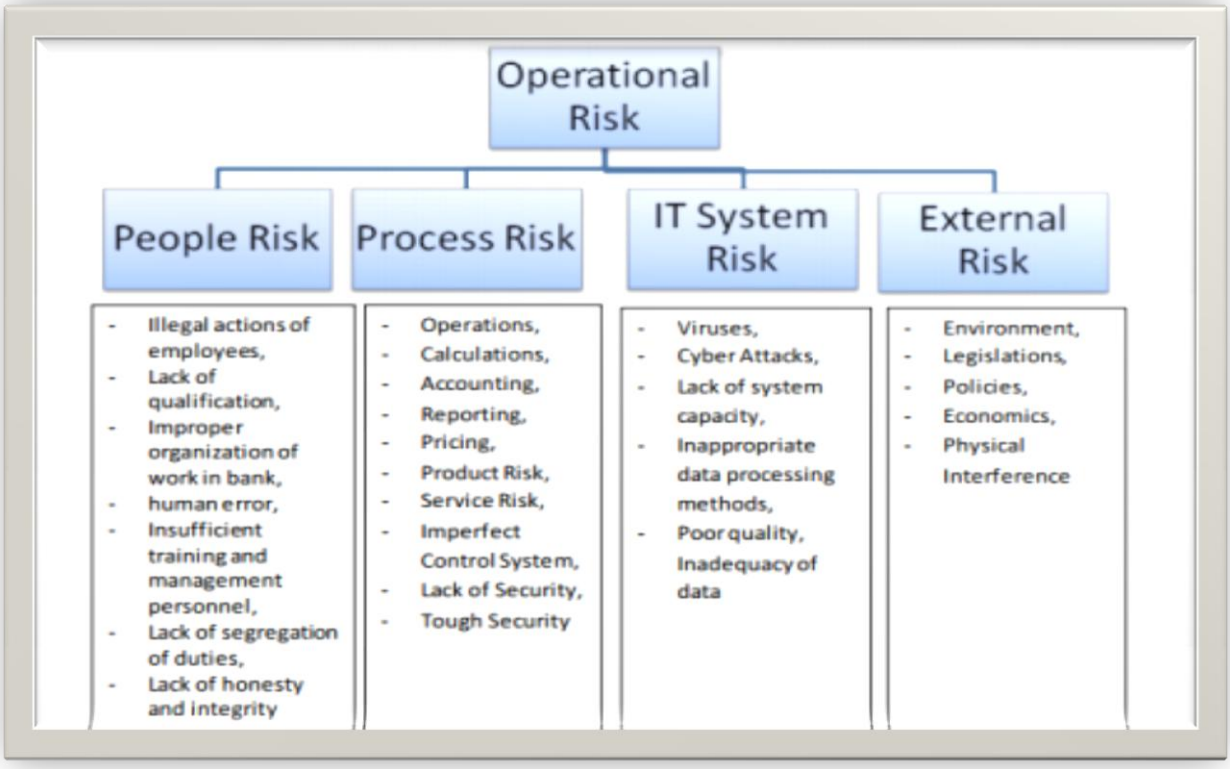

Figure 1: Operational Risk based on underlying causes (Source: Nazanin and Kateryna, 2015)

2.1.2 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.

2.1.3 The Risk Management Practice

The operating environment should comprise the integrity and competence of colleagues, management's philosophy and operating style and the way management communicates and delegate's 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.

Table 1: 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 control the risks	set up standards, limits, and rules guidelines, and procedures related to risks
All operational units/employees	Identify and control the risks	Publish various risk reports periodically 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.

2.1.4 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.

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.

2.1.5 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.

2.1.6 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-eye principle", need-to-know principle (access control), physical access control, coo0rdination 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.

2.1.7 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 bank 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.

2.1.8 International and National Risk Regulation 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).

In2010, 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 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.

2.2 Empirical Review

Studies on risk management practice of commercial banks in different geographical locations and economic development levels were conducted by different researchers using different research methodologies. A review of a few of them is resented below.

The 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.

2.3 Conceptual Framework

Other researcher's mentioned that there are many types of operational risk banks are facing for example computer hacking, internal and external fraud and he failure to adhere to internal polices and some study shows dashen bank also face some of this risk so, banks should use strong internal control system. Effective internal control may prevent or detect mistakes, potential fraud or non-compliance with banks policies. Banks should also maintain an effective internal or external audit program to help detect any deficiencies in the banks internal controls.

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 2: Risk Management Framework

CHAPTER THREE

3 RESEARCH DESIGN AND METHODOLOGY

3.1 Research design and approach

Research design is a strategic frame work for action that services as a bridge between research question and the execution, or implementation of the research strategy (Durrheim 2004). Research design is a master plan that specifies the methods and procedures for collecting and analyzing the needed information.

The main research design were used is descriptive. This research design is used to describe in nature because descriptive study is one in which information is collected without changing the environment and easily to interaction with group of people and it is describing the characteristics of a particular individual and well equipped to protect bias and to maximize the reliability of the research. Quantitative research approaches were used for data collection process. Quantitative survey method was use to meet the purpose of this study. The researcher focuses on quantitative research because it is useful to quantify opinions, attitudes and behavior and find out how the whole population feels about a certain issues.

The questionnaire was composed of structured questions where the respondents were asked to choose an answer from a given set of choices. 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 DB with respect to 62 statements by using a rating from 1 to 5 where 5= Strongly Agree; 4= Agree (SC); 3 = Neutral; 2= Disagree; 1= Strongly Disagree

3.2 Target Population, Sampling size and Sampling Techniques

The target populations of the study were the employees' of risk management, credit management, internal audit, finance and corporate banking department in DB at headquarter in Addis Ababa which is located around biherawi.. There are 153 employees who are working in

the above mentioned department. Therefore, considering the size of the population is small, the target population in general was address fully through census.

3.3 Sources and Tools of Data Collection

To fulfill the purpose of the study, the researcher was used both primary and secondary data. Primary data was collected from the sample selected, i.e. the employees, by the use of questionnaire as a method for data collection. Secondary data was collect from the company records on the previous works, books, journals, articles, organizational reports, company's magazine and National Bank of Ethiopia.

3.4 Procedures of data collection

The researcher were use questionnaire for the selected department, the question enable the respondents to express their idea , close ended questions is prepared to get necessary reliable information particularly from the employees. These methods of data collection play a greater role for motive findings and ideas of respondents. The questions were framed using scale of measurement ranging from Fully Complied with 5 points to Not Complied with 1 point.

3.5 Data Analysis

After gathering the necessary information from all respondents the researcher were analyze those data by using quantitative data analysis technique and the researcher were use the software called statistical package for the social science (SPSS) version 20.0 and descriptive statistics analysis techniques were employed to analyze the data and the results was described by using frequencies, percentage, mean and standard deviation. The findings will presented by using simple table

3.6 Validity

Validity determines whether the researcher truly measures what was intended to measure or how truthful the research result are (Joppe, 2000). Validity is the extent to which differences found with a measuring instrument reflect true differences among those being tested, (Kothari, 2004). In other words, Validity is the most critical criterion and indicates the degree to which an instrument measures what it is supposed to measure. In order to ensure the quality of the research design content and construct validity of the research were checked. According to (Kothari, 2004)

Content validity is the extent to which a measuring instrument provides adequate coverage of the topic under study.

3.7 Reliability

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 62 statements representing each of the two 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 compute

Table 2: Cronbach's Alpha

Variables	**Cronbach's Alpha Based on Standardized Items**	**No.of Items**
Individual variables:		
1.1. Risk Governance	0.897	5
1.2. Oversight	0.841	5
1.3. Risk Management Approach	0.820	5
1.4. Corporate ORM Function	0.878	8
2.1. Risk Identification and Assessment	0.843	5
2.2Key Operational Risk and Performance Indicators	0.866	4
2.3 Operational Risk Control and Mitigation	0.898	6
2.4. Business Resiliency and Continuity	0.907	5
2.5 Operational Risk Reporting and Disclosure	0.885	10

The three dimensions:		
Risk management practice	0.948	23
Internal Control	0.919	30
Risk Culture	0.893	8
The entire questionnaire		
All Variables	0.977	53

Source: SPSS data analysis output, 2020

Hence, the Cronbach's Alpha values for individual factors as well as for the entire 62 tems of the questionnaire results are greater than the 0.7 minimum acceptable values. We can therefore conclude that the items of the questionnaire are internally consistent and reliable.

3.8 Ethical Considerations

The primary responsibility of the researcher will be confirming strictly its confidentiality and guarantying their privacy during treating the information given by respondents. The purpose of the research will be explained to respondents before conducting survey by presenting them with covering letters. It also will be more concerned not to violate the self-esteem and self-respect of the subjects as well. Data and study results are confidential, secured, not disclosed to any one; it is solely used for academic purpose.

CHAPTER FOUR

4.DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

This chapter presents the findings of the research in accordance to the research objectives.

The analysis and interpretation of the data collected from the respondents is presented. It began with a description of the demographic and general characteristics of the participating respondents. Then, the results of Descriptive Statistics were presented.

3.9 Profile of Respondents

Questionnaires were distributed to151 employees of risk management, credit managment, internal audit, finance and corporate banking department in DB at headquarter. Among these 144 (90%) were filled questionnaires properly and returned on time. The rest 7 (10 %) were failed to complete and return the questionnaires. All the returned questionnaires were completed and considered for the analysis.

Table 3: Response Rate

Questionnaires	**Number**	**Percentage**
Returned	**144**	**95.36**%
Unreturned	**7**	**4.64**%
Total	**151**	100%

Source; survey result 2019

Table 4: Gender of Respondents

Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Male	90	62.5	62.5	62.5
Female	54	37.5	37.5	100.0
Total	144	100.0	100.0	

Source; survey result 2019

As indicated in Table 2, 90 (62.5%) of respondents are male and the remaining 54 (37.5%) are Female respondents.

Table 5: Age of Respondents

Age	Frequency	Percent	Valid Percent	Cumulative Percent
18-25 years	**31**	**21.5**	**21.5**	**21.5**
26-35years	**39**	**27.1**	**27.1**	**48.6**
36-45 years	**49**	**34.0**	**34.0**	**82.6**
46-55 years	**25**	**17.4**	**17.4**	**100.0**
>56 years	**0**	**0**	**0**	
Total	**144**	**100.0**	**100.0**	

Source; survey result 2019

From the above table we can observe that the age of majority of the respondents were between 36 to 45 years old that accounts 49(34%).Employees who were between 26 to 35 years are 39(27.1%), 31 (21.5%) were 18 to 25 years of age and finally 25(17.4%) of respondent were 46 to 55. From this result we can observe that the majority of respondents were adult and senior individuals as compared to the rest.

Table 6: Educational Level of Respondents

Educational Level	Frequency	Percent	Valid Percent	Cumulative Percent
Diploma	**22**	**15.3**	**15.3**	**15.3**
Degree	**83**	**57.6**	**57.6**	**72.9**
Masters	**39**	**27.1**	**27.1**	**100.0**
PhD.	**0**	**0**	**0**	

Total	**144**	**100.0**	**100.0**	

Source; survey result 2019

As indicated in Table 4.4, out of 144 respondents, 83(57.3 %) of them have first degree. Whereas 39 (27.1%) have master's degree and the rest 22 (15.3%) respondent have diploma level of education.

Table 7: Years of service

Work Experience	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1-5 years	25	17.4	17.4	17.4
6-10 years	72	50.0	50.0	67.4
11-15 years	38	26.4	26.4	93.8
16-20 years	9	6.3	6.3	100.0
Above 20	0	0	0	
Total	144	100.0	100.0	

Source; survey result 2019

As can be seen in Table 4.5, Majority of the respondent's service in the company is from 6-10 years which accounts 50% following by 26.4% is 11-15 years of service and 17.4% had 1- 5 years of experience in the company, the rest 6.3 % of the respondent have experience of l6-20 of year. Long years of experience shows that there is a relatively lower employee turnover as a result reduce cost of hiring new employees and saves time. As a result, the company can achieve its objectives and can maximize its profit.

3.10 Descriptive Analysis of the Study Variables

This part of the analysis is made based on survey questionnaires gathered from 144 employee of risk management, credit management, internal audit, finance and corporate banking department of DB employee of sales and marketing department of the company using 5-point Likert scale

(see Appendix I). The study has five independent variables: Accordingly, the paper applies mean and Standard deviation as the best measures for analysis based on the mean range developed by Al- Sayaad et al. (2006).

Table 8*:* Five – scaled likert criterion

NO	MEAN RANGE	RESPONSE OPTIONS
1	1.00 -1.80	STRONGLYDISAGREE
2	1.81-2.60	DISAGREE
3	2.61-3.40	NEUTRAL
4	3.41-4.20	AGREE
5	4.21-5.00	STRONGLY AGREE

Source, Al sayaad et al 2006, cited in bassam, 2013, Ambaye kefyalew, 2018

3.11 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 9: Risk Governance

Risk Governance		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**

1. The Board and Senior Management approved and update Operational Risk Management (ORM) framework.	F	53	25	35	21	10	144	3.63	1.300
	%	36.8	17.4	24.3	14.6	6.9	100		
2. The bank has an ORM system that is theoretically sound and is applied with integrity.	F	29	60	38	17	0	144	3.70	0.924
	%	20.1	41.7	26.4	11.8	0	100		
3. The Board and Senior Management have clearly articulated governance structure, responsibilities and accountability.	F	48	47	31	18	0	144	3.87	1.019
	%	33.3	32.6	21.5	12.5	0	100		
4. The Board and Senior Management confirm all employees are aware of the bank's approach to risk management.	F	12	36	60	30	6	144	3.12	0.974
	%	8.3	25	42	21	4.2	100		
5. There is appropriate and adequate organizational structure and process to implement strong risk culture.	F	24	59	37	24	0	144	3.58	0.958
	%	16.7	41	25.7	16.7	0	100		

Table 4.7 shows that in Item 1, most of the respondents 53(36.8%) tend to strongly agree with the statement. 35(24.3%) are neutral while 25(17.4%) agree with the statement. Also 21(14.6%) of the respondents disagree. The remaining 10(6.9%) strongly disagree with the statement. The implication of the mean at 3.63 According to Fifth-Scaled Likert Criterions of Al-Sayaad et al. (2006) the average mean falls under the range 'agree'.

In item2, a great number of the respondents precisely 60(41.7%) agree with the statement. 38(26.4%) are neutral also 29(20.1%) strongly agree with the statement. The remaining respondents 17(11.8%) disagree with the statement. The implication of the mean at 3.70 indicates that most of the respondents are leaning towards agree.

In item3, 48(33.3%) of the respondents strongly agree with the statement and also 47(32.6%) of the respondents agree with the statement while 31(21.5%) of the respondents neutral. The

remaining respondents 18(12.5%) disagree with the statement. The implication of the mean at 3.87 indicates that most of the respondents are leaning towards agree.

In item4, the highest number of respondents precisely 60(41.7%) of the respondents are neutral while 36(25%) are agree with the statement. Also it shows that 30(20.8%) of the respondents disagree while 12(8.3%) strongly agree with the statement. Only 6(14.2%) of the respondents strongly disagree with the statement. The implications of the mean at 3.12 indicate that most of the respondents are leaning towards neutral.

In item5, majority of the respondents specifically 59(41%) of the respondents agree and 37(25.7%) neutral with the statement. While 24(16.7%) were strongly agree and Also 24(16.7%) of the respondents are disagree with the statement. The implication of the mean at 3.58 indicates that most of the respondents are leaning towards agree.

Table 10: Oversight

Oversight		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
1. The Board oversees Senior Management to ensure that policies, process, systems are implemented effectively at all decision levels.	F	40	61	30	6	7	144	3.84	1.035
	%	27.8	42.4	21	4.2	4.9	100		
2. The Board ensures that the bank's (ORM) Framework is subject to effective independent review by audit or other appropriately skilled parties.	F	28	42	49	19	6	144	3.47	1.077
	%	19.4	29.2	34	13.2	4.2	100		
3. The Board has approved risk appetite and tolerance limits for aggregate and specific operational risks.	F	25	46	42	14	17	144	3.33	1.218
	%	17.4	31.9	29.2	9.7	11.8	100		
4. The Board has established clear lines of management responsibility and	F	31	59	35	19	0	144	3.71	0.953

accountability for implementing a strong control environment.	%	21.5	41	24.3	13.2	0	100		
5. Senior Management has implemented a clear, effective and robust governance structure which is conducive to transparent and consistent lines of responsibilities	F	18	51	50	19	6	144	3.39	1.004
	%	12.5	35.4	34.7	13.2	4.2	100		
6. The bank utilizes a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports.	F	19	50	46	23	6	144	3.37	1.036
	%	13.2	34.7	31.9	16	4.2	100		

In Item 1, majority of the respondents specifically 61(42.4%) of the workforce agree with the statement. While 40(27.8%) strongly agree with the statement, 30(21%) are neutral. Also 7(4.9%) of the respondents as well as 6(4.2%) tends to disagree and strongly disagree with the statement respectively. The implication of the mean at 3.84 indicates that most of the respondents are leaning towards agree.

In Item 2, 49(34%) of the respondents neutral with the statement. 42(29.2%) of the respondents agree with the statement while 28(19.4%) of the respondents strongly agree. From the remaining 25 respondents 19(13.2%) disagree and only 6(4.2%) are strongly disagree. The implication of the mean at 3.47 indicates that most of the respondents are leaning strongly towards agree.

A great number of the respondents in **Item 3**, that is 46(31.9%) agree with the statement, 42(29.2%) were neutral while 25(17.4%) strongly agree with the statement, 17(11.8%) strongly disagree and the remaining 14(9.7%) disagree. The implication of the mean at 3.33 indicates that most of the respondents are leaning towards neutral.

Item 4 also shows in that the highest number of respondents precisely 59(41%) of the respondents agree and 35(24.3%) were neutral while 31(21.5%) strongly agree with the

statement and the remaining 19(13.2%) are disagree. The implication of the mean at 3.71 indicates that most of the respondents are leaning towards agree.

In Item 5, most respondents 51(35.4%) agree with the statement and 50(34.7%) neutral, 19(13.2%) were disagree and also 18(12.5%) were strongly agree about the statement. The implication of the mean at 3.39 indicates that most of the respondents are leaning towards neutral.

In Item 6, 50(34.7%) of the respondents agree and also 46(31.9%) of the respondents neutral with the statement while 23(16%) of the respondents disagree while 19(13.2%) respondents strongly agree. The remaining 6(4.2%) strongly disagree. The implication of the mean at 3.37 indicates that most of the respondents are leaning strongly towards neutral.

Table11RiskManagementApproach

Risk Management Approach		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
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.	F	35	40	42	16	11	144	3.50	1.194
	%	24.3	27.8	29.2	11.1	7.6	100		
2. Business Units identify and manage the risks inherent to the products, activities, processes and systems.	F	26	61	48	9	0	144	3.72	0.832
	%	18.1	42.4	33.3	6.3	0	100		
3. The ORM Function performs independently and is responsible for the design and implementation of the bank's ORM framework.	F	11	65	50	18	0	144	3.48	0.810
	%	7.6	45.1	34.7	12.5	0	100		

4. Internal audit coverage includes opinions on the overall appropriateness and adequacy of the implemented ORM Framework and associated governance processes of the bank.	F	13	52	51	21	7	144	3.30	0.990
	%	9	36.1	35.4	14.6	4.9	100		
5. Internal audit evaluates whether the ORM Framework meets organizational needs and supervisory expectations.	F	15	47	41	24	17	144	3.13	1.172
	%	10.4	32.6	28.5	16.7	11.8	100		

In Item 1, 42(29.2%) of the respondents neutral and also 40(27.8%) of the respondents agree with the statement while 35(24.3%) of the respondents strongly agree, 16(11.1%) respondents disagree and the remaining 11(7.6%) strongly disagree. The implication of the mean at 3.50 indicates that most of the respondents are leaning towards agree.

In Item 2, Majority of the respondents, precisely 61(42.4%) of the workforce tend to agree with the statement while 48(33.3%) were neutral. 26(218.1%) tends to strongly agree with the statement. Only 9(6.3%) of the workforce tend to disagree with the statement. The implication of the mean at 3.72 indicates that most of the respondents are leaning towards agree.

In Item 3, a greater number of the respondents 65(45.1%) elected to agree with the statement. Although 50 (34.7%) were neutral, 18(12.5%) of the respondents disagree while 11(7.6%) of the respondents strongly agree with the statement. The implication of the mean at 3.48 indicates that most of the respondents are leaning towards agree.

In Item 4, 52(36.1%) of the respondents agree and also 51(35.4%) of the respondents neutral with the statement while 21(14.6%) of the respondents disagree, 13(9%) respondents strongly agree and the remaining 7(4.9%) strongly disagree. The implication of the mean at 3.30 indicates that most of the respondents are leaning towards neutral.

In Item 5, a greater number of the respondents 47(32.6%) elected to agree with the statement. Although 41 (28.5%) were neutral, 24(16.7%) of the respondents disagree while 17(12%) of the respondents strongly disagree the remaining 15(10.4%) of the workforce strongly agree with the statement. The implication of the mean at 3.13 indicates that most of the respondents are leaning towards neutral.

Table 12: Corporate ORM Function (CORMF)

Corporate ORM Function (CORMF)		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
1. Policy/Procedures are in place over the roles, responsibilities and its mandate.	F	42	72	24	6	0	144	4.04	0.792
	%	29.2	50.0	16.7	4.2	0	100		
2. CORMF provides an adequate and independent challenge to management and business lines inputs, outputs, risk management, measurement and reporting systems.	F	18	54	54	18	0	144	3.50	0.869
	%	12.5	37.5	37.5	12.5	0	100		
3. CORMF is independent and responsible for the design and implementation of the bank's ORM framework.	F	12	72	42	18	0	144	3.54	0.818
	%	8.3	50.0	29.2	12.5	0	100		
4. CORMF has operational risk officers/experts with clearly defined roles and responsibilities.	F	36	60	36	12	0	144	3.83	0.901
	%	25.0	41.7	25.0	8.3	0	100		
5. CORMF has reporting relationship with operational risk officers/experts within the business units with clearly delineated roles and responsibilities.	F	24	60	36	18	6	144	3.54	1.044
	%	16.7	41.7	25	12.5	4.2	100		
6. CORMF provides regular updates on the adherence to risk appetite and tolerance to	F	12	60	42	24	6	144	3.33	0989

Board and Senior Management.	%	8.3	41.7	29.2	16.7	4.2	100		
7. CORMF is appropriately equipped with skilled and experienced staff and with required material and information processing resources to fulfill its responsibilities.	F	6	54	48	36	0	144	3.21	0.868
	%	4.2	37.5	33.3	25	0	100		
8. CORMF provides enterprise wide training for the first line of defense on the ORM framework.	F	18	60	30	30	6	144	3.37	1.077
	%	12.5	41.7	20.8	20.8	4.2	100		

Table 4.10 indicates **in Item 1**, a high number of respondents that is 72(50%) tend to agree with the statement. While 24(29.2%) strongly agree with the statement. 24(16.7%) of the workforce are neutral. Also 6(4.2%) of the respondents disagree with the statement. The implication of the mean at 4.04 indicates that most of the respondents are leaning towards agree.

In Item 2, 54(37.5%) of the respondents neutral and also 54(37.5%) of the respondents agree with the statement while 18(12.5%) of the respondents strongly agree and the same as 18(12.5%) respondents disagree with the statement. The implication of the mean at 3.50 indicates that most of the respondents are leaning towards agree.

In Item 3, Majority of the respondents 72(50%) agrees with the statement, 42(29.2%) neutral While 18 (12.5%) of the respondents disagree and 12(8.3%) respondents strongly agree with the statement. The implication of the mean at 3.54 indicates that most of the respondents are leaning towards agree.

In Item 4, 60(41.7%) of the respondents agree with the statement. 36(25%) of the respondents strongly agree with the statement and also 36(25%) of the respondents neutral. The remaining 12(8.3%) respondents disagree with the statement. The implication of the mean at 3.83 indicates that most of the respondents are leaning towards agree.

Item 5 in Table 4.10 also shows in that the highest number of respondents precisely 60(41.7%) of the respondents agree and 36(25%) are neutral with the statement while 24(16.7%) are

strongly agree. From the remaining 24 respondents 18(12.5%) disagree and 6(4.2%) strongly disagree with the statement. The implication of the mean at 4.21 indicates that most of the respondents are strong leaning towards agree.

In Item 6, most respondents 60(41.7%) agree with the statement and 42(29.2%) neutral, 24(16.7%) were disagree about the statement. While 12(8.3%) strongly agree with the statement. Only the remaining 6(4.2%) of the respondents strongly disagree with the statement. The implication of the mean at 3.33 indicates that most of the respondents are leaning towards neutral.

In Item 7, a great number of the respondents precisely 54(37.5%) agree with the statement. 48(33.3%) neutral with the statement while 36(25%) disagree the remaining 6(4.2%) are strongly agree with the statement. The implication of the mean at 3.21 indicates that most of the respondents are leaning towards neutral

In Item 8, a great number of the respondents precisely 60(41.7%) agree with the statement. 30(20.8%) neutral and another 30(20.8%) disagree with the statement. Of the remaining 24 respondents 18(12.5%) strongly agree with the statement and 6(4.2%) are strongly disagree. The implication of the mean at 3.37 indicates that most of the respondents are leaning towards agree.

3.12 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 13: Risk Identification and Assessment

Risk Identification and Assessment		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**

1. The bank has identified and communicated its financial, operational and compliance objectives.	F	29	70	32	8	5	144	3.76	0.953
	%	20.1	48.6	22.2	5.6	3.5	100.0		
2. Risk identification and assessments are clearly linked to inherent risks on the financial, operational and compliance objectives of the bank.	F	30	51	49	8	6	144	3.63	1.009
	%	20.8	35.4	34	5.6	4.2	100.0		
3. An independent challenge is in place to ensure accuracy, completeness, timeliness and reliability of the internal operational risk events.	F	18	43	58	20	5	144	3.34	0.984
	%	12.5	29.2	40.3	13.9	3.5	100.0		
4. Business units regularly conduct risk assessments and perform root cause analysis and corrective actions on significant internal loss events.	F	17	43	60	18	6	144	3.33	0.981
	%	11.8	29.2	41.7	12.5	4.5	100.0		
5. The bank has a systematic tracking of relevant operational risk data including material losses by business units.	F	6	42	66	22	8	144	3.11	0.909
	%	4.2	29.2	45.8	15.3	5.6	100.0		
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.	F	12	43	54	26	9	144	3.16	1.022
	%	8.3	29.2	37.5	18.1	6.3	100		

Table 4.11 **Item 1** shows that, most of the respondents 70(48.6%) tend to agree with the statement. 32(22.2%) are neutral and also another 29(20.1%) are strongly agree while 8(5.6%) disagree and 5(3.5%) also strongly disagree with the statement. The implication of the mean at 3.76 indicates that most of the respondents are leaning towards agree.

In Item 2, a great number of the respondents precisely 51(35.4%) agree with the statement, 49(34%) were neutral. While 30(20.8%) of the respondents strongly agree. Of the remaining 14 respondents 8(5.6%) disagree and 6(4.2%) strongly disagree with the statement. The implication of the mean at 3.63 indicates that most of the respondents are leaning towards agree.

In Item 3, majority of the respondents specifically 58(40.3%) are neutral, 43(29.2%) agree, 20(13.9%) are disagree and also 18(12.5%) are strongly agree. The remaining 5(3.5%) are strongly disagree with the statement. The implication of the mean at 3.34 indicates that most of the respondents are leaning towards neutral.

Item 4 in **Error! Not a valid bookmark self-reference.** 4.11 also shows in that the highest number of respondents precisely 60(41.7%) are neutral, 43(29.2%) agree, 18(12.5%) are disagree and also 17(11.8%) are strongly agree. The remaining 6(4.2%) are strongly disagree with the statement. The implication of the mean at 3.33 indicates that most of the respondents are leaning towards neutral.

In Item 5, most respondents 66(45.8%) neutral with the statement and 42(29.2%) agree. 22(15.3%) were disagree about the statement. While 8(5.6%) strongly disagree with the statement. Only the remaining 6(4.2%) of the respondents strongly agree with the statement. The implication of the mean at 3.11 indicates that most of the respondents are leaning towards neutral.

Item 6, majority of the respondents specifically 54(37.5%) of the workforce neutral and 43(29.2%) agree with the statement. While 26(18.1%) were disagree. Also 12(8.3%) of the respondents as well as 9(6.3%) tends to strongly agree and strongly disagree with the statement respectively. The implication of the mean at 3.16 indicates that most of the respondents are leaning towards neutral.

Table 14: Key Operational Risk and Performance Indicators

Key Operational Risk and Performance Indicators		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
1. Business units identify both qualitative	F	9	59	59	14	3	144	3.40	0.830

and quantitative KRIs and KPIs which are aligned with the units inherent operational risks	%	6.3	41	41	9.7	2.1	100		
2. KRIs and KPIs are paired with escalation triggers to warn when risk levels exceed acceptable ranges and prompt mitigation plans.	F	7	48	51	29	9	144	3.10	0.987
	%	4.9	33.3	35.4	20.1	6.3	100		
3. The bank uses statistics and/or metrics to provide insight into operational risk position.	F	22	39	65	15	3	144	3.43	0.944
	%	15.3	27.1	45.1	10.4	2.1	100		
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	F	10	47	62	21	4	144	3.26	0.893
	%	6.9	32.6	43.1	14.6	2.8	100		

Table 4.12 shows that in **Item 1**, most of the respondents 59(41%) tend to agree and also 59(41%) are neutral with the statement. 14(9.7%) are disagree while 9(6.3%) strongly agree with the statement. Also 3(2.1%) of the respondents strongly disagree. The implication of the mean at 3.40 indicates that most of the respondents are leaning towards neutral.

In Item 2, a great number of the respondents precisely 51(35.4%) neutral, 48(33.3%) agree with the statement while 29 (20.1%) are disagree. Of the remaining 16 respondents 9(6.3%) strongly disagree with the statement and 7(4.9%) are strongly agree with the statement. The implication of the mean at 3.10 indicates that most of the respondents are leaning towards neutral.

Majority of the respondents in **Item 3**, 65(45.1%) neutral with the statement, 39(27.1%) are agree while 22(15.3%) strongly agree with the statement. The remaining 18 respondents that is 15(10.4%) are disagree and 3(2.1%) strongly disagree about the statement. The implication of the mean at 3.43 indicates that most of the respondents are leaning towards agree.

A great number of the respondents in **Item 4**, that is 62(43.1%) neutral with the statement, 47(32.6%) were agree while 21(14.6%) disagree with the statement, 10(6.9%) strongly agree and the remaining 4(2.8%) strongly disagree. The implication of the mean at 3.26 indicates that most of the respondents are leaning towards neutral.

Table 4.15 Operational Risk Control and Mitigation

Operational Risk Control and Mitigation		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
1. The Bank conducts regular evaluation of compliance to policy/procedure and regulations to ensure required authorized approvals and accountability are maintained	F	24	66	36	12	6	144	3.63	0.996
	%	16.7	45.8	25.0	8.3	4.2	100		
2. The Internal controls for operational risk include close monitoring of adherence to assigned risk limits	F	18	48	60	12	6	144	3.42	0.957
	%	12.5	33.3	41.7	8.3	4.2	100		
3. Areas of potential conflicts of interest are proactively identified, minimized, and are subject to careful independent monitoring and reviews.	F	6	36	72	24	6	144	3.08	0.865
	%	4.2	25.0	50.0	16.7	4.2	100		
4. The bank has implemented adequate segregation of duties and check and balance, and dual control on required areas.	F	30	66	30	18	0	144	3.75	0.927
	%	20.8	45.8	20.8	12.5	0	100		
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	F	48	50	32	8	6	144	3.88	1.07

	%	33.3	34.7	22.2	5.6	4.2	100		
b) Appropriate staffing level and training to maintain expertise at all levels	F	24	66	36	12	6	144	3.63	0.996
	%	16.7	45.8	25	8.3	4.2	100		
c) Regular verification and reconciliation of financial transactions and accounts.	F	30	72	36	6	0	144	3.88	0.783
	%	20.8	50	25	4.2	0	100		
d) A vacation/leave policy for all employees.	F	30	54	42	18	0	144	3.67	0.946
	%	20.8	37.5	29.2	12.5	0	100		
e) Information Assets identification, user access level control unauthorized access prevention	F	36	72	30	6	0	144	3.96	0.792
	%	25	50	20.8	4.2	0	100		
f) Cyber-attack, database integrity, database activity management, testing of similar attempts	F	18	60	36	24	6	144	3.42	1.041
	%	12.5	41.7	25	16.7	4.2	100		
6. The bank has an integrated approach to identifying, measuring, monitoring all information assets, technological devices and infrastructure risks.	F	18	48	54	18	6	144	3.37	0.996
	%	12.5	33.3	37.5	12.5	4.2	100		

Table 4.13 Item 1 shows that, most of the respondents 66(45.8%) tend to agree with the statement. 36(25%) are neutral while 24(16.7%) strongly agree with the statement, 12(8.3%) of the respondents disagree and only 6(4.2%) who strongly disagree with the statement. The implication of the mean at 3.63 indicates that most of the respondents are leaning towards agree.

In Item 2, a great number of the respondents precisely 60(41.7%) were neutral with the statement, 48(33.3%) agree with the statement. While 18(12.5%) of the respondents strongly agree. Of the remaining 18 respondents 12(8.3%) disagree and the remaining 6(4.2%) strongly

disagree with the statement. The implication of the mean at 3.42 indicates that most of the respondents are leaning towards agree.

In Item 3, majority of the respondents specifically 72(50%) of the workforce neutral with the statement, 36(25%) agree and 24(16.7%) are disagree. While 6(4.2%) strongly agree with the statement. Also 6(4.2%) of the respondents tends to strongly disagree with the statement. The implication of the mean at 3.08 indicates that most of the respondents are leaning towards neutral.

Item 4 also shows in that the highest number of respondents precisely 66(45.8%) of the respondents agree, 30(20.8%) of the respondents strongly agree and also 30(20.8%) were neutral with the statement. only 18(12.5%) of respondents are disagree. The implication of the mean at 3.75 indicates that most of the respondents are leaning towards agree.

In Item 5a, most respondents 50(34.7%) agree with the statement and 48(33.3%) strongly agree, 32(22.2%) were neutral about the statement. While 8(5.6%) disagree with the statement. Only the remaining 6(4.2%) of the respondents strongly disagree with the statement. The implication of the mean at 3.88 indicates that most of the respondents are leaning towards agree.

In Item 5b, majority of the respondents specifically 66(45.8%) of the workforce agree with the statement, 36(25%) neutral and 24(16.7%) are strongly agree. While 12(8.3%) disagree with the statement. Also 6(4.2%) of the respondents tends to strongly disagree with the statement. The implication of the mean at 3.63 indicates that most of the respondents are leaning towards agree.

Item 5c also shows in that the highest number of respondents precisely 72(50%) of the respondents agree and 36(25%) of the respondents neutral with the statement while 30(20.8%) are strongly agree with the statement. finally 6(4.2%) of the workforce were disagree. The implication of the mean at 3.88 indicates that most of the respondents are strong leaning towards agree.

In Item 5d, most respondents 54(37.5%) agree with the statement and 42(29.2%) neutral, 30(20.8%) were strongly agree about the statement. The remaining 18(12.5%) disagree with the

statement. The implication of the mean at 3.67 indicates that most of the respondents are leaning towards agree.

In Item 5e, 72(50%) of the respondents agree with the statement. 36(25%) of the respondents strongly agree with the statement while 30(20.8%) of the respondents neutral. only 6(4.2%) respondents disagree. The implication of the mean at 3.96 indicates that most of the respondents are leaning towards agree.

In Item 5f shows that the highest number of respondents precisely 60(41.7%) of the respondents agree with the statement while 36(25%) are neutral. Also it shows that 24(16.7%) of the workforce disagree while 18(12.5%) strongly agree with the statement. Only 6(4.2%) respondents strongly disagree with the statement. The implication of the mean at 3.42 indicates that most of the respondents are leaning towards agree.

In Item 6, 54(37.5%) of the respondents neutral with the statement. 48(33.3%) of the respondents agree with the statement while 18(12.5%) of the respondents strongly agree and also 18(12.5%) disagree. The remaining 6(4.2%) strongly disagree. The implication of the mean at 3.37 indicates that most of the respondents are leaning towards neutral.

Table 16: Business Resiliency and Continuity

Business Resiliency and Continuity		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
1. The bank has established business continuity plans, taking into account different types of plausible scenarios of vulnerability	F	24	51	46	13	10	144	3.46	1.090
	%	16.7	35.4	31.9	9	6.9	100		
2. Plausible disruptive scenarios are assessed for their financial, operational and reputational impact.	F	18	45	44	29	8	144	3.25	1.087
	%	12.5	31.3	30.6	20.1	5.6	100		
3. The bank has contingency strategies, recovery/resumption procedures, and	F	16	47	48	20	13	144	3.23	1.108

communication plans for informing management, employees, and all stakeholders.	%	11.1	32.6	33.3	13.9	9	100		
4. The bank periodically reviews its continuity plans to ensure contingency strategies relevance to prevailing vulnerabilities.	F	22	43	51	17	11	144	3.33	1.109
	%	15.3	29.9	35.4	11.8	7.6	100		
5. Regular awareness creations are implemented to ensure staff can effectively execute contingency plans	F	12	40	45	26	21	144	2.97	1.176
	%	8.3	27.8	31.3	18.1	14.6	100		

Item 1 shows that, most of the respondents 51(35.4%) tend to agree with the statement. 46(31.9%) are neutral while 24(16.7%) strongly agree and also 13(9%) are disagree with the statement. Only 10(6.9%) of the respondents strongly disagree. The implication of the mean at 3.46 indicates that most of the respondents are leaning towards agree.

Table 4.13 shows that in **Item 2**, most of the respondents 45(31.3%) tend to agree and also 44(30.6%) are neutral with the statement. 29(20.1%) are disagree while 18(12.5%) strongly agree with the statement. Also 8(5.6%) of the respondents strongly disagree. The implication of the mean at 3.25 indicates that most of the respondents are leaning towards neutral.

Item 3, most of the respondents 48(33.3%) tend to neutral and also 47(32.6%) are agree with the statement. 20(13.9%) are disagree and also 16(11.1%) strongly agree with the statement. Only 13(9%) of the respondents strongly disagree. The implication of the mean at 3.23 indicates that most of the respondents are leaning towards neutral.

Item 4, most of the respondents 51(35.4%) tend to neutral and 43(29.9%) are agree with the statement. 22(15.3%) are strongly agree and also 17(11.8%) disagree with the statement. Only 11(7.6%) of the respondents strongly disagree. The implication of the mean at 3.33 indicates that most of the respondents are leaning towards neutral.

In Item 5, a great number of the respondents precisely 45(31.3%) neutral with the statement, 40(27.8%) were agree. While 26(18.1%) of the respondents disagree. Of the remaining 33 respondents 21(15%) strongly disagree and the remaining 12(8.3%) strongly agree with the statement. The implication of the mean at 2.97 indicates that most of the respondents are leaning towards neutral.

Table 17: Operational Risk Reporting and Disclosure

Operational Risk Reporting and Disclosure		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
1. The bank has maintained operational risk reporting system to the Board and stakeholders.	F	42	60	24	12	6	144	3.83	1.071
	%	29.2	41.7	16.7	8.3	4.2	100		
2. Has reporting thresholds for internal operational risk events and monitors to ensure adherence.	F	18	54	48	18	6	144	3.42	1.000
	%	12.5	37.5	33.3	12.5	4.2	100		
3. Incorporates internal loss data, in a complete and timely manner, into the operational risk reporting for capital impact analysis.	F	18	42	66	12	6	144	3.37	0.953
	%	12.5	29.2	45.8	8.3	4.2	100		
4. Incorporates breaches of the bank's risk appetite and tolerance statement.	F	18	48	60	12	6	144	3.42	0.957
	%	12.5	33.3	41.7	8.3	4.2	100		
5. Includes results of relevant assessments of business environment factors, risk and control self-assessments and other internal control factors.	F	6	18	60	48	12	144	2.71	0.938
	%	4.2	12.5	41.7	33.3	8.3	100		
6. Dashboard is created to summarize key information and highlight major events for efficient communication to Board and Senior Management and	F	18	54	42	24	6	144	3.38	1.037
	%	12.5	37.5	29.2	16.7	4.2	100.0		

other stakeholders.									
7. The results of monitoring activities are included in regular management and board reports,	F	24	66	24	24	6	144	3.54	1.083
	%	16.7	45.8	16.7	16.7	4.2	100		
8. Findings in operational risk reports are appropriately assigned and associated with action items to address deficiencies.	F	24	72	30	12	6	144	3.67	0.989
	%	16.7	50	20.8	8.3	4.2	100		
9. The bank publicly discloses relevant ORM information	F	12	36	42	36	18	144	2.92	1.156
	%	8.3	25	29.2	25	13	100		
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	F	18	42	42	36	6	144	3.21	1.083
	%	12.5	29.2	29.2	25	4.2	100		

In Item 1, Table 4.14 shows that a great number specifically 60 of the respondents constituting 41.7% of the respondents tend to agree with the statement. Another 42(29.2%) of the respondents tend to strongly agree with the statement. Also 24(16.7%) of the workforce are neutral about the statement while 12 respondents (8.3%) of the workforce disagree. Only 6 (4.2%) of the entire workforce strongly disagree with the statement. The implication of the mean at 3.83 indicates that most of the respondents are leaning towards agree.

In Item 2, the table also shows that most of the respondents 54(37.5%) agree with the statement. Furthermore 48(30.9%)of the respondents neutral with the statement. Although 18(12.5%) of the respondents were strongly agree and also 18(12.5%) are disagree, Only 6(4.2%) of the workforce strongly disagree with the statement. The implication of the mean at 3.42 indicates that most of the respondents are leaning towards agree.

In Item 3, Most respondents 66(45.8%) were neutral with the statement. while 42(29.2%) are agree. Also 18(12.5%) of the respondents strongly agree with the statement while 12(8.3%)

disagree. Only 6(4.2%) strongly disagrees with the statement. The implication of the mean at 3.37 indicates that most of the respondents are leaning towards neutral.

In Item 4, from the table shows that 60(41.7%) of the respondent neutral with the statement and 48(33.3%) agree with the statement, also 18(12.5%) were strongly agree. While 12(8.3%) of the respondents disagree with the statement. Only 6(4.2%) of the respondents strongly disagree. The implication of the mean at 3.42 indicates that most of the respondents are leaning towards agree.

In Item5, majority of the respondents that is 60(41.7%) neutral with the statement. While 48(33.3%) tend to disagree with the statement. Also 18(12.5%) agree with the statement. While 12(8.3%) were strongly disagree. The remaining 6(4.2%) of the respondents strongly agree with the statement. The implication of the mean at 2.71 indicates that most of the respondents are leaning towards neutral.

A great number of the respondents in Item 6 that is 54(37.5%) agree with the statement, 42(29.2%) were neutral while 24(16.7%) disagree with the statement. The rest 18(12.5%) and 6(4.2%) strongly agree and stron gly disagree respectively with the statement. The implication of the mean at 3.38 indicates that most of the respondents are leaning towards neutral.

In item 7, which comprises 66(45.8%) agree with the statement, while 24(16.7%) were neutral, strongly agree and disagree respectively about the statement. Only 6(4.2%) of the workforce strongly disagree with the statement. The implication of the mean at 3.54 indicates that most of the respondents are leaning towards agree.

In Item 8, 72(50%) of the respondents agree with the statement. 30(20.8%) of the respondents neutral with the statement while 24(16.7%) of the respondents are strongly agree. Also 12(8.3%) disagree with the statement and the remaining 6(4.2%) strongly disagree. The implication of the mean at 3.67 indicates that most of the respondents are leaning towards agree.

Majority of the respondents in Item 9 comprising 42(29.2%) tends to neutral with the statement. 36(25%) agree and also 36(25%) disagree with the statement. The remaining 18(12.5%) strongly disagree and 12(8.3%) strongly agree with the statement. The implication of the mean at 2.92 indicates that most of the respondents are leaning towards neutral.

Item 10, most of the respondents 42(29.2%) tend to agree and also 42(29.2%) are neutral with the statement. 36(25%) are disagree while 18(12.5%) strongly agree with the statement. Also 6(4.2%) of the respondents strongly disagree. The implication of the mean at 3.21 indicates that most of the respondents are leaning towards neutral.

3.13 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 18: Risk Culture

Risk Culture		**5**	**4**	**3**	**2**	**1**	**Total**	**Mean**	**SD**
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.	F	42	53	41	8	0	144	3.90	0.891
	%	29.2	36.8	28.5	5.6	0	100		
2. Setting business objectives is accompanied by identification of inherent risks and their mitigations to achieve the objectives.	F	44	55	27	14	4	144	3.84	1.056
	%	30.6	38.2	18.8	9.7	2.8	100		
3. The bank employees well understand their roles and responsibilities for risk as well as their authority to act.	F	12	49	64	10	9	144	3.31	0.950
	%	8.3	34.0	44.4	6.9	6.3	100		
4. There is strong and consistent Board and Senior Management support for risk management and ethical behavior..	F	25	50	43	21	5	144	3.48	1.051
	%	17.4	34.7	29.9	14.6	3.5	100		
5. Individuals and business units are	F	6	35	49	36	18	144	2.83	1.067

measured or incentivized based on their risk performance against the bank's long-term objectives.	%	4.2	24.3	34.0	25	12.5	100		
6. Risk management function is well-resourced and staffed with sufficiently skilled human resources. Events for efficient communication to Board and Senior Management and other stakeholders.	F	23	43	59	15	4	144	3.46	0.974
	%	16	29.9	41	10.4	2.8	100		
7. There is an overall strong culture of risk management and ethical business practices	F	6	60	48	24	6	144	3.25	0.927
	%	4.2	41.7	33.3	17	4.2	100		

Item 1, most of the respondents 53(36.8%) tend to agree and also 42(29.2%) are strongly agree with the statement. 41(28.5%) are neutral and the remaining 8(5.6%) disagree with the statement. The implication of the mean at 3.90 indicates that most of the respondents are leaning towards agree.

A great number of the respondents in **Item 2** that is 55(38.2%) agree with the statement, 44(30.6%) were strongly agree while 27(18.8 %) neutral with the statement. The rest 14(9.7%) and 4(2.8%) disagree and strongly disagree respectively with the statement. The implication of the mean at 3.84 indicates that most of the respondents are leaning towards agree.

In **item 3**, which comprises 64(44.4%) neutral with the statement, while 49(34%) were agree about the statement. While 12(8.3%) are strongly agree and 10(6.9%) also disagree with the statement. The remaining 9(6.3%) strongly disagree with the statement. The implication of the mean at 3.31 indicates that most of the respondents are leaning towards neutral.

Majority of the respondents 50(34.7%) agrees with the statement in **item 4**, 43(29.9%) neutral .While 25 (17.4%) of the respondents strongly agree and 21 respondents that is 14.6% of the total workforce disagree with the statement. The remaining 5(3.5%) were strongly disagree.
The implication of the mean at 3.48 indicates that most of the respondents are leaning towards agree.

Item 5, most of the respondents 49(34%) tend to neutral, 36(25%) are disagree and also 35(24.3%) agree with the statement. While 18(12.5%) are strongly disagree and the remaining 6(4.2%) strongly agree with the statement. The implication of the mean at 2.83 indicates that most of the respondents are leaning towards neutral.

A great number of the respondents in **Item 6** that is 59(41%) neutral with the statement, 43(29.9%) were agree while 23(16%) strongly agree and 15(10.4%) disagree with the statement. Only 4(2.8%) strongly disagree with the statement. The implication of the mean at 3.46 indicates that most of the respondents are leaning towards agree.

In item 7, which comprises 60(41.7%) agree with the statement, while 48(33.3%) were neutral about the statement. While 24(16.7%) are disagree while 6(4.2%) strongly agree and also the remaining 6(4.2%) strongly disagree with the statement. The implication of the mean at 3.25 indicates that most of the respondents are leaning towards neutral.

CHAPTER FIVE

4 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

4.1 Introduction

This is the final chapter and it presents summary, conclusion and recommendation of the study. First summary of the findings, which is obtained while answering the research question, is Presented, and then based on the findings it reached on conclusions. Finally, based on the overall conclusions it proposed recommendation.

4.2 SUMMARY OF THE STUDY FINDINGS

The objective of this study was to assess operational risk management practice at dashen bank /head office/.

Based on the analysis of collected data, findings show that 62.5% of respondent were male and 37.5% of respondent were female.

With regard to age 34% of the respondents were in the age category of 36-45, this indicates that the majority the selected department were adult age group.

With regard to educational level, large number of the selected department which is 57.6% of respondent are who holds degree, therefore majority of the selected department were higher level of educational background.

With regard to work experience 50% of the respondents were working 6-10 years, which implies that the company can achieve its objectives and can maximize its profit.

Regarding with risk governance, five different questions were raised, from those question respondent were neutral only on confirmation of the board and Senior Management that all employees are aware of the bank's approach to risk management. In general most of respondents agree with the reaming statements that are listed.

In the case of risk oversight the finding survey show that, the respondent were agree on the board oversees Senior Management to ensure that policies, process, systems are implemented effectively at all decision levels, bank's (ORM) Framework is subject to effective independent review by audit or other appropriately skilled parties and has established clear lines of management responsibility and accountability for implementing a strong control environment. And also the respondents were neutral on the board has approved risk appetite and tolerance limits for aggregate and specific operational risks, has implemented a clear, effective and robust governance structure which is conducive to transparent and consistent lines of responsibilities and bank utilizes a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports.

Regarding with Risk Management Approach, response from respondent indicate that most of respondent were agree on questions and respondent were neutral on the internal audit activities.
In the case of risk corporate ORM function (CORMF) the finding survey show that, most respondent were agree on the Policy/Procedures are in place over the roles, responsibilities and its mandate, CORMF provides an adequate and independent challenge to management, is independent and responsible for the design and implementation of the bank's ORM framework, has operational risk officers/experts and has reporting relationship with operational risk officers/experts within the business units with clearly delineated roles and responsibilities. with clearly defined roles and responsibilities and on the remaining statement respondents are neutral.

Regarding with risk identification and assessment, response from respondent indicate that most of respondent were neutral on An independent challenge ensure accuracy, completeness, timeliness and reliability of the internal operational risk events, Business units regularly conduct risk assessments and perform root cause analysis and corrective actions on significant internal loss events, the bank has a systematic tracking of relevant operational risk data including material losses by business units and quantifies its exposure to operational risk by using the output of its risk assessment tools and on the remaining statement respondents were agree

Regarding with key operational risk and performance indicators, four different questions were raised, from those question respondent were agree only on bank uses statistics and/or metrics to provide insight into operational risk position. In general most of respondents neutral with the reaming statements that are listed.

Regarding with operational risk control and mitigation, six different questions were raised, from those question respondent were neutral only on areas of potential conflicts of interest are proactively identified, minimized, and are subject to careful independent monitoring and reviews and bank has an integrated approach to identifying, measuring, monitoring all information assets, technological devices and infrastructure risks. In general most of respondents neutral with the reaming statements that are listed.

In the case of business resiliency and continuity the finding survey show that, the respondent were agree on the bank has established business continuity plans, taking into account different types of plausible scenarios of vulnerability. In general most of respondents neutral with the reaming statements that are listed.

Regarding with operational risk reporting and disclosure, response from respondent indicate that respondent were agree on questions and also respondent were neutral on the reaming statements that are listed.

Regarding with risk culture, seven different questions were raised, from those question respondent were neutral only on bank employees well understand their roles and responsibilities for risk as well as their authority to act, Individuals and business units are measured or incentivized based on their risk performance against the bank’s long-term objectives and strong

culture of risk management and ethical business practices. In general most of respondents agree with the reaming statements that are listed.

4.3 Conclusions

Managing and monitoring of operational risk is an integral part of DB'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 DB in terms of the three major operational risk management components: the Risk Management practice, the Internal Control and the challenge to maintaining effective operational risk management.

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.

4.4 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-awareness 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.

- 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.

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.
- 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".
- Creswell, J. W. (2010). "Research design: Qualitative, Quantitative and Mixed methods approaches", 2nd ed., California: sage publications.
- Sue Greener (2008), Business Research Methods; 1st Ed., viewed 19 February 2014 and Published in Book Boon Database
- 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.
- FasikaFirew (2012), "Commercial Bank operational risks management: Exploratory study on selected Ethiopian Commercial Banks", AAU, Masters Thesis
- Hana Berhe (2016), " Operational Risk Management Practices: The case of Commercial Bank of Ethioia" AAU, Masters Thesis
- Greuning, H. &BrajovicBratanovic, S. (2003), "Analyzing and managing banking risk: a framework for assessing corporate governance and risk management", 2nd ed, Washington, DC
- Jeet, S. and Preeti, Y. (2013), "Strategies for managing risks in banks", Acta de GerenciaCiencia, Vol.1, No.2, pp. 6-20
- 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
- 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.
- 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.
- Mark S, Philip L, Adrian T. et al. (2007), Research Methods for Business Students; 4th Ed., Prentice Hall, New Jersy (USA).
- Nabweteme A. (2011), "at Stanbic Bank Uganda Operational Risk Management, Organizational Environment and Organizational Performance Limited", Makerere University
- National Bank of Ethiopia (2010), "Commercial banks risk management guidelines"
- National Bank of Ethiopia (2009), "Banking Industry Risk Management Survey Report".
- 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 M. (2011), "Critical evaluation of operational risk tools used in regulatory capital calculations", University of Pretoria, Master's Thesis for MBA
- 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.
- TsionFekadeselassie (2015), "Risk Management Practice of Ethiopian Commercial Banks", AAU, Masters Thesis.
- 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.
- http://en.wikipedia.org/wiki/Bank Risk and capital
- National Bank of Ethiopia website: http://www.nbe.gov.et/aboutus/index.html.
- Official site of Bank of International Settlement, www.bis.org.

Appendices

ST. MARY UNIVERSITY

SCHOOL OF GRADUATE STUDIES

DEPARTMENT OF MBA GENERAL

QUESTIONNAIRE FOR COMPANYS SALES PERSONS

Dear respondents first of all I would like to thank you for your willingness to complete this questionnaire.

This questionnaire is a major material in the preparation of a thesis on *"*operational risk management practice at dashen bank*"* for the fulfillment of the requirement of Masters of Art Degree in general Management at St. Marry University, Addis Ababa.

The information that you will provide will be used only for educational purpose and will be kept confidential. Furthermore writing name is not necessary. The researcher kindly asks your cooperation to attempt all questions objectively and honestly.

Thank you for your cooperation!

Part I. Personal information

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

1. Gender

1) Male 2) Female

2. Age:

A) 18-25 B) 26-35 C) 36-45 D) 46-55 E) >56 years

3. Level of education:

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

4. Years of service:

A) 1-5 years B) 6-10 C) 11-15 D) 16-20 E) above 20 years

Part II. Operational risk management evaluation questions

Please indicate the level of compliance of operational risk management practices of dashen bank (DB) with respect to the following statements by using a rating from 1 to 5 where **5= strongly agree 4 =agree 3 =neutral 2 =disagree 1= strongly disagree**

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

Risk Governance	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std Dev.**
1. The Board and Senior Management accepted and update Operational Risk Management (ORM) framework.							
2. The bank has an ORM system that is theoretically sound and is applied with integrity.							
3. The Board and Senior Management have clearly articulated governance structure, responsibilities and accountabilities.							

4. The Board and Senior Management confirm all employees are aware of the bank's approach to risk management.							
5.There is appropriate and adequate organizational structure and process to implement strong risk culture.							
6. There is appropriate and adequate organizational structure and process to implement strong risk culture.							

Oversight	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std Dev.**
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.							

Risk Management Approach	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**
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.							

Corporate ORM Function (CORMF)	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**
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.							

INTERNAL CONTROL							
Risk Identification and Assessment	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**
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.							

Key Operational Risk and Performance Indicators	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**
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							

Operational Risk Control and Mitigation	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**
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, testing of similar attempts							
6. The bank has an integrated approach to identifying, measuring, monitoring all information assets, technological devices and infrastructure risks.							

Business Resiliency and Continuity	**5**	**4**	**3**	**2**	**1**	**Man**	**Std. Dev**
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							

Operational Risk Reporting and Disclosure	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**
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							

Risk Culture	**5**	**4**	**3**	**2**	**1**	**Mean**	**Std. Dev**

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 objectives.							
6. Risk management function is well-resourced and staffed with sufficiently skilled human resources. Events for efficient communication to Board and Senior Management and other stakeholders.							
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							

Thank you for your valuable time and participation!!!