DECLARATION

I, the undersigned, declare that this study entitled **"Commercial Bank operational risk management: Exploratory study on selected Ethiopian Commercial Banks"** is my original work and has not been presented for a degree in any other university, and that all sources of materials used for the study have been duly acknowledged.

Declared by:

Name Fasika Firew Mosissa

Signature _____

Date_____

CERTIFICATE

This is to certify that this study, **"Commercial Bank operational risk management: Exploratory study on selected Ethiopian Commercial Banks"**, undertaken by Fasika Firew for the partial fulfillment of Master"s of Business Administration [MBA] at Addis Ababa University, is an original work and not submitted earlier for any degree either at this University or any other University.

Research Advisor: Dr. Yitbarek Takele

Signature _____

Date_____

SCHOOL OF GRADUATE STUDIES

Commercial Bank operational risk management: Exploratory study on selected Ethiopian Commercial Banks

By: Fasika Firew

Approved by Board of Examiners:

_____	_____	_____
Advisor	Signature	Date
_____	_____	_____
Internal Examiner	Signature	Date
_____	_____	_____
External Examiner	Signature	Date

Acknowledgments

First, I would like to express my deepest and heartfelt gratitude to my research advisor Dr. Yitbarek Takele, who tirelessly provided me all the necessary advice, guidance and comments throughout this study.

Next, I‟m deeply gratitude to all the commercial banks which I have contacted and allowed me to do this study in their Institutions. Likewise, I‟m greatly indebted to all my respondents‟ for their willingness in filling and returning the questionnaires on due date. I‟m also deeply thankful to all practitioners who have cooperated and helped me a lot in this study, especially Ato Shimelis Bekele, Ato Getiye and Ato Melkamu Yimer whom I owe them deepest gratitude.

Last but not least, my deepest gratitude goes to my families‟: mom, dad, brothers and sisters for their moral and psychological support throughout my study. My especial thanks go to my elder brother Bizuayehu Firew and sisters, Metasebia Mekonnen and Sinkenesh Takele for their follow-up and invaluable moral support throughout this study. I‟m also grateful to all my friends, especially Diriba Tesfaye, Fiseha Birhanu and Henock Semaw for their sincere friendship and moral support.

Thank you all!!!!!

Table of contents

Contents **Page**

Acknowledgments i
Table of contents ii
List of Tables v
List of Figures vi
Acronyms vii
Abstract viii
Chapter One: Introduction 1
1.1 Background of the study 1
1.2 Banking history in Ethiopia 4
1.3 Statement of the problem 7
1.4 Objectives of the study 8
1.4.1 General objective 8
1.4.2 Specific Objectives 9
1.5 Research questions 9
1.6 Research hypothesis 9
1.7 Significance of the study 10
1.8 Delimitation of the study 10
1.9 Limitation of the study 10
1.10 Ethical consideration 11
1.11 Organization of the study 11
Chapter Two: Review of related literature 12
2.1 Introduction 12
2.2 Theory and nature of risk 12
2.2.1 Risk management 13
2.2.2 Main banking risks 16

2.3 Banking operational risk 17
2.3.1 Conceptualization 17
2.3.2 Operational definition 18
2.4 Basel accord for operational risk 19
2.5 Operational risk management 23
2.6 Quantification approach to operational risk measurement 25
2.6.1 The basic indicator approach (BIA) 26
2.6.2. The standardized approach (TSA) 27
2.6.3. Advanced measurement approaches (AMA) 29
2.7 Basel committee‟s operational risk loss events and business lines 29
2.8 Empirical review 31
2.9 Conceptual framework of the study 35
Chapter 3: Research approach and methodology 37
3.1 Introduction 37
3.2 Research approach 37
3.3 Research Method 38
3.4 Research design 39
3.5 Data type 39
3.6 Unit of analysis 39
3.7 Sampling design 40
3.8 Research Instrument 41
3.9 Variables of the study 42
3.10 Methods of data analysis 42
3.11 Reliability and validity of the study variables 43
3.11.1 Reliability 43
3.11.2 Validity 44

Chapter Four: Results and Discussions 46
4.1 Introduction 46
4.2 Validity and Reliability analysis 46
4.3 Discussion of the study findings 48
4.3.1 Analysis of the correlation significance between the operational risk effect and Loss events 48
4.3.2 The factor analysis of operational risk contributory factors 57
4.3.3. Analysis of banks board approval of operational risk management policies and procedures 63
Chapter 5: Summary, Conclusions and Recommendations 66
5.1 Summary of the findings 66
5.2 Conclusions 67
5.3 Recommendations 69
Future research ideas 71
Bibliography 72
Appendices ix

List of Tables

Table 1: Beta values for TSA……..28

Table 2: Reliability coefficient of the study variables…….47

Table 3: Spearman correlation coefficient values…….....49

Table 4: Correlations between ORE and IF…….49

Table 5: Correlations between ORE and EF…….....51

Table 6: Correlations between ORE and EPWS……..52

Table 7: Correlations between ORE and BDSF……..53

Table 8: Correlations between ORE and DPA……54

Table 9: Correlations between ORE and EDPM…….....55

Table 10: Correlations between ORE and CPBP…….....56

Table 11: KMO and Bartlett‟s test of sphericity…….57

Table 12: KMO interpretations……...57

Table 13: Total variance explained by components of OR contributory factors……58

Table 14: Respondents‟ response towards banks board approval of policies and procedures of ORM…….....63

List of Figures

Figures 1: Risk management Process……15

Figure 2: ORM framework……22

Figure 3: Respondents‟ response to banks board approval of ORM policies and procedures……...64

Acronyms

AMA= Advanced Measurement Approach

BCBS= Basel Committee on Banking Supervision

BDSF= Business Disruption and System Failure

BIA= Basic Indicator Approach

BOD= Board of Directors

CPBP= Clients, Products, and Business practice

DPA= Damage to Physical Asset

EF= External Fraud

EPWS= Employment Practice and Workplace Safety

IF= Internal Fraud

IT= Information Technology

KMO= Kaiser-Meyer-Olkin

KRI= Key Risk Indicator

NBE= National Bank of Ethiopia

OR= Operational Risk

ORE= Operational Risk Effect

ORM= Operational Risk Management

PCA= Principal Component Analysis

RCSA= Risk Control Self Assessment

TSA= The Standardized Approach

Abstract

The purpose of this study is to analyze operational risk management (ORM) of selected Ethiopian commercial banks. As operational risk differs from the other banking risks in terms of its quantification and prediction ability, banks need to measure and manage it carefully as it will have detrimental effect on its entire performance and profitability eventually. The types of data used were both primary and secondary as the research design employed was mixed-mode (Qualitative and quantitative) design. The variables were affirmed reliable fulfilling the minimum 70% requirement of Cronbach"s alpha value. As the study was conducted at institutional level the non probability purposive sampling technique was used to select the banks. Hence, 12 commercial banks have been selected and contacted, where the sample respondents", staffs of risk management section (Risk experts and officers) and internal auditors were used as "key informant" or "Proxy" for the study unit of analysis (Banks). And 96 respondents" for the unit analysis were considered for this study.

As the study was constituted a data having an ordinal scale of measurement, the Spearman correlation (Rho) coefficient and principal component analysis (PCA) were used as methods of data analysis. Besides, the descriptive analysis has been used for an interpretation of close ended questions. Analysis of Spearman Correlation (Rho) coefficient findings has resulted into existence of significant positive correlation coefficient between the variables tough the degree of strength differs. Principal component analysis as factor analysis method has resulted into an extraction of 6 factors as useful factors out of the initial 20 factors considered based on an Eigen value, $\lambda>1.0$ which all together accounts for about 64% of variance. The descriptive analysis of the board approval of policies and procedures of banks operational risk has shown the presence of board approval on the different issues of banks operational risk, based on majority of the responses though it wouldn"t guarantee the presence of effective ORM. It is highly recommended to have committed management and strong internal control mechanisms for an effective ORM.

Key Words: *Operational risk, Operational Risk Management, Operational risk factors (Loss events), Operational risk effect, Operational risk contributory factors, Basel II Framework (Capital Accord)*

Chapter One: Introduction

1.1 Background of the study

Risk is unavoidable. Like the proverbial death and taxes, it‟s one of the few things in life that‟s inevitable. All businesses, whatever their size and shape, whatever markets they operate in and whatever products and services they provide, are constantly faced with a multitude of risks, large and small. In deed businesses can only prosper by successful risk taking as of Osborne (2012).

Operational risk was for the first time treated as a self-contained regulatory issue in the „Operational Risk Management‟ document published by the Basel Committee on Banking Supervision in 1998[1]. `The New Basel Capital Accord' was first formulated in a proposal in 1999, released in 2001 and has became effective in 2007; within the framework, operational risk was integrated in the so called Pillar 1 which implies its inclusion in the calculation of a banks' overall capital charge.

As currently, banking industry is expanding in Ethiopia; besides this expansion it calls for a sound risk management practices and techniques for their survival, as well as, to be competitive enough in this turbulent business environment in service delivery, as it‟s a key driver behind profitability. To do so, it‟s a must to identify, select and apply the appropriate risk measurement and management mechanisms, which are simple but effective risk management tools or techniques.

Specifically, in its banks risk management guidelines (2010), the national bank of Ethiopia has defined operational risk as, risk that inadequate information systems or operational controls e.g., accounting, funds transfer and financial controls shall lead to breaches, fraud or unforeseen catastrophe that shall negatively affect the bank.

Osborne (2012:7) has stated that, in our own businesses we need to strike the correct balance between risk and potential reward; to maximize our upside risk and minimize our downside risk. To succeed we need to manage risk appropriately, not to try eliminating or avoiding it, as, in any case, that simply isn‟t possible. It‟s therefore essential that we understand the major risks to our business operations to enable us to manage them to our advantage.

[1] Basel Committee on Banking Supervision (BCBS) was formed in 1974 that constitutes of central bank governors of ten countries and having its head quarter in Basel, Switzerland namely, Banks for International Settlements (BIS).

Wikipedia (accessed on June 18, 2013) has indicated that, all financial institutions regardless of their size, complexity of tasks and whatever the products and services they provide are exposed to some level of financial risk, small or large in their day-to-day operations. Conditions like system failure, working place condition and employment practices, human errors, counter party default, terrorism attacks, etc can lead the institutions to significant losses. And, all necessary measures will be undertaken so that the exposure to such risk will be minimized.

A **commercial bank** (or **business bank**)[2] is a type of financial institution and intermediary. It is a bank that lends money and provides transactional, savings, and money market accounts and that accepts time deposit. While performing these activities there could be different inherent risks that the banks are to bear. Thus, to serve its purpose and to achieve its objectives of being profitable, safe and having liquidity to the interest of its shareholders in particular and to the public in general, it need to undertake and have a health risk profile and sound risk management system.

The risks differ in their natures and occurrences pertaining to different business activities. That‟s to say that certain risks are particular in their natures that specifically affect the operations of a particular firm or industry, for instance banking industry. Likewise, risks associated with banking service differ by type of service rendered. Banks face a number of risks in order to conduct their business, and how well these risks are managed and understood is a key driver behind profitability, and how much capital a bank is required to hold. Some of the main risks faced by banks include:

I. Credit risk as the chance that a debtor or issuer of a financial instrument whether an individual, a company, or a country will not repay principal and other investment-related cash flows according to the terms specified in a credit agreement.

II. Market risk is generally considered as the risk that the value of a portfolio, either an investment portfolio or a trading portfolio, will decrease due to the change in value of the market risk factors. There are three common market risk factors to banks and these are liquidity, interest rates and foreign exchange rates.

[2] Ibid.

III. An operational risk is, as the name suggests, a risk arising from execution of a company's business functions. It is a very broad concept which focuses on the risks arising from the people, systems and processes through which a company operates. It also includes other categories such as fraud risks, legal risks, physical or environmental risks. A widely used definition of operational risk is the one contained in the Basel II regulations. This definition states that operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

According to Osborne (2012), risk management has a part to play in one‟s decision making, whether it‟s with regard to business start-up, strategy, exploiting opportunities, managing one‟s various projects or in one‟s day-to-day business operations. Risk management can help to justify- to the management team, employees, business partners, investors, creditors and customers. And it should mean that you go in to things with your eyes open; that you make informed decisions rather than just acting on gut feel or a hunch.

National bank of Ethiopia (NBE) as a sole regulator and supervisor of all financial institution activities in the country, it has a mandate to issue and provide guidance to all financial institutions as to the risk management system. To this end, it has revised the 2003 bank‟s risk management guidelines in 2010 so as to incorporate latest developments in the area. The guideline presents the risk management system of the banking risks. The first two can be easily dealt with as both could be modeled and predicted by quantifying those risks. But, as far as operational risk concerns, it‟s difficult to quantify all of its risks by using the ordinary banking risk modeling, thus the risk has its own impact on the measurement and management of banks risk management process.

Given the above discussions of banking industry‟s operational risk concept, this study was undertaken in order to analyze the operational risk management of selected Ethiopian commercial banks. As the risk management practice of Ethiopian banks are at its infancy stage, where NBE directives dictating the establishment of the risk department is a recent phenomenon (predominantly, after the financial crisis engulfed the western world at closing months of 2008).

1.2 Banking history in Ethiopia[3]

Banking business in Ethiopia has its origin dates back to 1905 the time when was the modern banking started. The agreement that was reached in 1905 between Emperor Minilik II and Mr.Ma Gillivray, representative of the British owned National Bank of Egypt marked the introduction of modern banking in Ethiopia. Following the agreement, the first bank called Bank of Abysinia was inaugurated in Feb.16, 1906 by the Emperor.

The Bank was totally managed by the Egyptian National Bank and the following rights and concessions were agreed upon the establishment of Bank of Abyssinia:-

- The capital of the Bank was agreed to be Pound Sterling 500,000 and one-fifth was subscribed and the rest was to be obtained by selling shares in some important cities such as London, Paris and New York.
- The Bank was given full rights to issue bank notes and monitor coins which were to be legal tender and all the profits there from a ruling to the bank and freely exchangeable against gold and silver on cover by the Bank as well as to establish silver coins and abolish the Maria Theresa.
- Land was given to the Bank free of charges & permitted to build offices and warehouses. Government and public funds were to be deposited with the bank and all payments to be made by checks.
- The government promised not to allow any bank to be established in the country within the 50-year concession period.

Within the first fifteen years of its operation, Bank of Abyssinia opened branches in different areas of the country. In 1906 a branch in Harar (Eastern Ethiopia) was opened at the same time of the inauguration of Bank of Abyssinia in Addis Ababa. Another at Dire Dawa was opened two years later and at Gore in 1912 and at Dessie and Djibouti in 1920. Mac Gillivray, the then representative and negotiator of Bank of Egypt, was appointed to be the governor of the new bank and he was succeeded by H Goldie, Miles Backhouse, and CS Collier were in change from 1919 until the Bank‟s liquidation in 1931.

[3] Some part of this discussion is taken from the National Bank of Ethiopia Website: http://www.nbe.gov.et/aboutus/index.html

The society at that time being new for the banking service, Bank of Abyssinia had faced difficulty of familiarizing the public with it. It had also need to meet considerable cost of installation and the costly journeys by its administrative personnel. As a result, despite its monopolistic position, the Bank earned no profit until 1914. Profits were recorded in 1919, 1920 and from 1924 onwards. Generally, in its short period of existence, Bank of Abyssinia had been carrying out limited business such as keeping government accounts, some export financing and undertaking various tasks for the government.

Moreover, the Bank faced enormous pressure for being inefficient and purely profit motivated and reached an agreement to abandon its operation and be liquidated in order to disengage banking from foreign control and to make the institution responsible to Ethiopia‟s credit needs. Thus by 1931 Bank of Abyssinia was legally replaced by Bank of Ethiopia shortly after Emperor Haile Selassie came to power .

The new Bank, Bank of Ethiopia, was a purely Ethiopian institution and was the first indigenous bank in Africa and established by an official decree on August 29, 1931 with capital of £750,000. Bank of Egypt was willing to abandon its cessionary rights in return for a payment of Pound Sterling 40,000 and the transfer of ownership took place very smoothly and the offices and personnel of the Bank Of Abyssinia including its manager, Mr. Collier, being retained by the new Bank. Ethiopian government owned 60 percent of the total shares of the Bank and all transactions were subject to scrutiny by its Minister of Finance.

Following the demise of the Dergue regime in 1991 that ruled the country for 17 years under the rule of command economy, the EPRDF declared a liberal economy system. In line with this, Monetary and Banking proclamation of 1994 established the national bank of Ethiopia as a judicial entity, separated from the government and outlined its main function.

Monetary and Banking proclamation No.83/1994 and the Licensing and Supervision of Banking Business No.84/1994 laid down the legal basis for investment in the banking sector. Moreover, Mauiri (2008) discussed that, the liberalization of financial sector in 1994 when the government announces the monetary and banking proclamation No. 83/1994 laid a cornerstones to the introduction of private banks into the financial system that stimulate competition with public banks which is vital in the development of current banking businesses.

As of National Bank of Ethiopia‟s official website, after the proclamation the first private bank, Awash International Bank was established in 1994 by 486 shareholders and by 1998 the authorized capital of the Bank reached Birr 50.0 million. Dashen Bank was established on September 20, 1995 as a share company with an authorized and subscribed capital of Birr 50.0 million. 131 shareholders with subscribed and authorized capital of 25.0 million and 50 million founded bank of Abysinia. Wegagen Bank with an authorized capital of Birr 60.0 million started operation in 1997. The fifth private bank, United Bank was established on 10th September 1998 by 335 shareholders. Nib International Bank was started operation on May 26, 1999 with an authorized capital of Birr 150.0 million. Cooperative Bank of Oromia was established on October 29, 2004 with an authorized capital of Birr 22.0 million. Lion International Bank with an authorized capital of Birr 108 million started operation in October 02, 2006. Zemen Bank has started operation on June 17, 2008 with an authorized capital of Birr 87.0 million. The last bank to be established to date is Oromia International Bank that started operation on September 18, 2008 with an authorized capital of Birr 91 million. Currently, there are 18 private and 3 government-owned banks, 14 private and 1 government owned insurance companies, and 31 MFIs (as of May,2012).

Furthermore, Ethiopian government has also enacted proclamation No. 592/2008 that states how to provide banking business in the country, where it indicate that banks play an important role in economic development through mobilization of funds from within and outside the country and channeling such funds to various sectors of economy.

1.3 Statement of the problem

The study has investigated the operational risk management practices of selected Ethiopian Commercial banks.

According to BCBS capital accord (2007) operational risk is an important risk facing banks and that banks need to hold capital to protect against losses from it.

In banks risk management system, why it‟s very crucial to give emphasis for the measurement and management of operational risk, the National Bank of Ethiopia in its banks risk management guideline (2010) has indicated that, managing operational risk is an important feature of sound risk management practice in any bank.

In this turbulent business environment, most recently where the financial institutions, particularly banks, in the world were in a financial crisis elsewhere, it calls for careful assessment and treatment of banks risk inherent to their operations in order to survive and eventually be competitive enough in the financial industry.

Power (2003) has described that, until the „Basel II‟[4] reforms to banking supervision, operational risk was largely a residual category for risks and uncertainties which were difficult to quantify, insure and manage in traditional ways.

Furthermore, as there are different banking risks that exist such as market risk, credit risk and operations risk (Gunther and Christian, 2005; Indian Reserve bank, 2005) argued, until recent years the operational risk didn‟t receive much attention as that of the other banking risks mentioned due to many reasons. One of the reasons is that, any other risks rather than credit and market risk was usually considered as an operational risks which is thought to be residual that couldn‟t be affect banks operations significantly, but in fact, the reality is that the materialization of such risk had huge impact on the performance and survival of financial industries as observed in the last two decades due to fundamental changes in financial markets, deregulation and globalization.

[4] Basel II is the decisions passed by Basel Committee on Banking Supervision (BCBS) with regard to Capital Accord including capital charge for the assessment and treatment of operational risks.

A survey conducted by national bank of Ethiopia (NBE) in the year 2009 on the bank‟s risk management status has revealed that, 53% of the respondents (15 banks) being considered says operational risk had most affected their banks in the last two years. However, the survey did not indicate what were the operational risk factors (Loss events) affected them and their interrelationship with operational risk effect, the contributory operational risk factors and how they were dealt with it in their risk management system to tackle its potential effects.

Furthermore, as operational risk emanates from executing the business functions, which are in fact at the heart of an existence and survival of any business organizations, it require much attention in order to manage its catastrophic financial consequences and treat it accordingly. However, there is insufficient (few) literature that has been so far undertaken in the country with regard to banks operational risk management.

Thus, to deal with the identified gap of the study, the researcher has analyzed the management of operational risk of selected Ethiopian Commercial Banks taking in to account the operational risk factors (Loss events) and their effect on entire banks performance. Likewise, the study has explored the most contributory factors of banking operational risk management.

1.4 Objectives of the study

1.4.1 General objective

The general objective of this study is to analyze the operational risk management practice of selected Ethiopian Commercial banks.

1.4.2 Specific Objectives

The specific objectives of the study include the following:

- To analyze the correlation significance between an operational risk effect and operational risk factors (loss events).
- To explore key factors that would be crucial and most useful in the banks operational risk management.
- To identify banks board approval of policies and procedures of operational risk management in which it could be impetus for its implementation.

1.5 Research questions

The study has sought answers for the following questions persistent to the raised problem and objectives of the study.

- Does the operational risk effect significantly correlate to the operational risk factors (Loss events)?
- What are the key contributing factors for the effectiveness of the banks operational risk management?
- Does the board approve policies and procedures related to banks ORM for effectiveness of its routine banking operations?

1.6 Research hypothesis

Based on the research objective and thorough analysis of theoretical and empirical literatures, the researcher has developed and tested the following hypothesis:

H_1: The operational risk effect significantly correlates to all operational risk factors (Loss events).

1.7 Significance of the study

It is the believe of the researcher that, the findings and recommendations that has been made based on data analysis will be an important ingredient to the banks under investigation and regulatory body in particular and to the society in general. Additionally, the study will have the following significances:

- It will also provide possible information for regulatory body on the status of the bank‟s operational risk management and findings could also be used in policy formulation.
- It will also be used by other banks in evaluating their operations in identifying and taking corrective actions about possible risk exposure areas.
- It will be also serve as a reference material for anyone who will undertake a further study on the same or related topic.

1.8 Delimitation of the study

This study is confined itself to analyze operational risk management of selected Ethiopian commercial banks by excluding other risks such as credit, market and liquidity risk.

1.9 Limitation of the study

Here are some of the limitations that were faced by the researcher that could be affected the study findings to a certain extent.

- The researcher has made a strong attempt for the inclusion of two other commercial banks to have more samples, but due to management‟s unwillingness and taking too long time to respond, he has forced to exclude both of them from this study consequently.
- It would have been interesting to distribute questionnaire to the heads of functional units to have in-depth understanding of operational risk management, but this was not done due to risk that they will not complete the questionnaire accurately given their knowledge about the subject in interpretation of the questions.

- As the research used survey method, this is often open to response bias as the respondents‟ are asked their perception about their bank‟s operational risk management practices. However, indirect questions were used in addition to asking respondents‟ to provide their genuine and natural responses freely.

1.10 Ethical consideration

As of Bhattacherjee (2012), ethics is the moral distinction between right and wrong, and what is unethical may not necessarily be illegal. Moreover, with regard to the importance of research ethics (Ibid.) has stated that, because, science has often been manipulated in unethical ways by people and organizations to advance their private agenda and engaging in activities that are contrary to the norms of scientific conduct.

Hence, the researcher would like to acknowledge all participants of this study and assures that the promised confidentiality has maintained. The researcher also confirms that the findings of this study certainly represent the response of the study participants. Furthermore, for this study the data collection, analysis and interpretation was done in an ethical manner of scientific procedures and the findings represents the real situation of the study unit of analysis.

1.11 Organization of the study

This study is organized under five chapters. The first chapter is concerned with introduction which in turn contains background of the study, statement of the problem, objectives of the study, research questions, research hypothesis and so forth. Chapter two presents and elaborates both theoretical literatures and empirical review which includes theory and nature of risk, banking operational risk, Basel accord for operational risk, operational risk management, quantification approach to operational risk measurement, empirical review and conceptual framework. Whereas, chapter three introduces the research approach and methodology which in turn includes research approach, research method, research design, data type, unit of analysis, sampling design, research instrument, variables of the study, method of data analysis and validity and reliability of the study variables. Chapter four presents the results and discussions of the study which includes introduction, validity and reliability analysis and discussions of the study findings. And finally, chapter five presents the summary, conclusions and recommendations based on the study findings.

Chapter Two: Review of related literature

2.1 Introduction

This chapter briefly discusses theory and nature of risk, banking operational risk, Basel accord for operational risk, operational risk management, quantification approach to operational risk measurement, Basel Committee‟s operational risk loss events and business lines, empirical review and conceptual framework.

2.2 Theory and nature of risk

Risk is all about uncertainty. That is inability to precisely determine what will occur in the future, as future is full of uncertain. With regard to what is a risk Osborne (2012) has claimed that, what we all are talking about is a future problem- or, indeed, opportunity – or the potential future effect of a decision or an action that we take now. And every decision we make or action we take contains some element of risk.

"Whatever can go wrong will go wrong" (Murphy"s Law)

The implication of risk is that, something that we could not expect could happen and it will lead to huge losses. And, of course, risk is a state of nature as every walk of life is surrounded by a certain level of risk. However, it can‟t be generalized that risk only leads to cost (loss) but could also involve an opportunity (reward) if it is dealt with wisely as like in the case of undertaking business activities.

Furthermore, Osborne (2012) has indicated that,

> *Risks can arise as a result of our business"sactivities or as a result of external factors such as legislation, market forces, interest or exchange rate fluctuations, the activities of others or even the weather. They can be a product of business environment, the natural environment, the political or economic climate or of human inadequacies, failing or errors. The bottom line is that risk may impact on our ability to meet our business objectives or even threaten the business itself.*

The types and the degree of effect of risk defers among business organizations, even within industry level as they might differ in their size, complexity of task, types of service or product being offered or organizational structure.

Thus, risks that business organizations face are inherent to their operations or endeavors. As to the classification of risk Jorion and Khoury (1996:2) argument has cited by Khan and Ahmed (2001) discusses that,

> *There are different ways in which risks are classified. One way is to distinguish between business risk and financial risks. Business risk arises from the nature of a firm"s business. It relates to factors affecting the product market. Financial risk arises from possible losses in financial markets due to movements in financial variables.*

2.2.1 Risk management

As of Osborne (2012) risk management is a central part of any organization"s strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organization. It marshals the understanding of the potential upside and downside of all those factors which can affect the organization. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organization"s overall objectives.

Furthermore, he has stated that,

> *Many risks are seen as having purely negative consequences and for this reason it"s not uncommon for those involved in risk management to take a pessimistic view of a risk. But we shouldn"tforget that many risks also have positive consequences. Effective risk management can help us to reduce the negative and increase the positive consequences of risk, thus helping our business to grow and flourish.*

Risk management covers three main aspects; namely risk identification, risk measurement and risk mitigation. It has a huge impact on organization"s objective accomplishment. To be successful, business organizations need to undertake risk management process so as to indentify, measure and manage their inherent risks. Particularly, risk management is said to be a cornerstone of prudent banking practice.

According to de Fontnouvelle et al (2003), risk management becomes more sophisticated; bank supervisors are encouraging banks to develop their risk models, both by directly rating risk management through the supervisory process and by incorporating the models into the regulatory process.

Thus, it"s clear that every organization (private or public, for profit or not for profit) need to identify and assess the inherent risks to their operations. To do so, they must undertake the risk management process in order to accurately measure and manage their risks by risk models accordingly.

However, among banking risks the credit and market risk could be measured and dealt with by using the ordinary banking risk models, but the operational risks can"t be measured by the ordinary banking risk models as it has impeded by insufficiency of internal and external loss data.

Power (2003) has cited the work of Bessis (2001) indicates that,

> *The goal of risk management is to measure risks in order to monitor and control them, and also enable it to serve other important functions in a bank in addition to its direct financial function. These include assisting in the implementation of the bank,,s ultimate strategy by providing it with a better view of the future and therefore defining appropriate business policy and assisting in developing competitive advantages through the calculation of appropriate pricing and the formulation of other differentiation strategies based on customers,, risk profiles.*

According to Raghavan (2003), risk is inherent in any walk of life in general and in financial sectors in particular. Banks are exposed to same competition and hence are compelled to encounter various types of financial and non-financial risks. Risks and uncertainties form an integral part of banking which by nature entails taking risks.

Moreover, the state bank of Pakistan (2003) in its risk management guideline for commercial banks has claimed that, the risk management activities takes place at different hierarchical levels. Hence, it has indicated the following hierarchical levels of risk management activities in every financial institution.

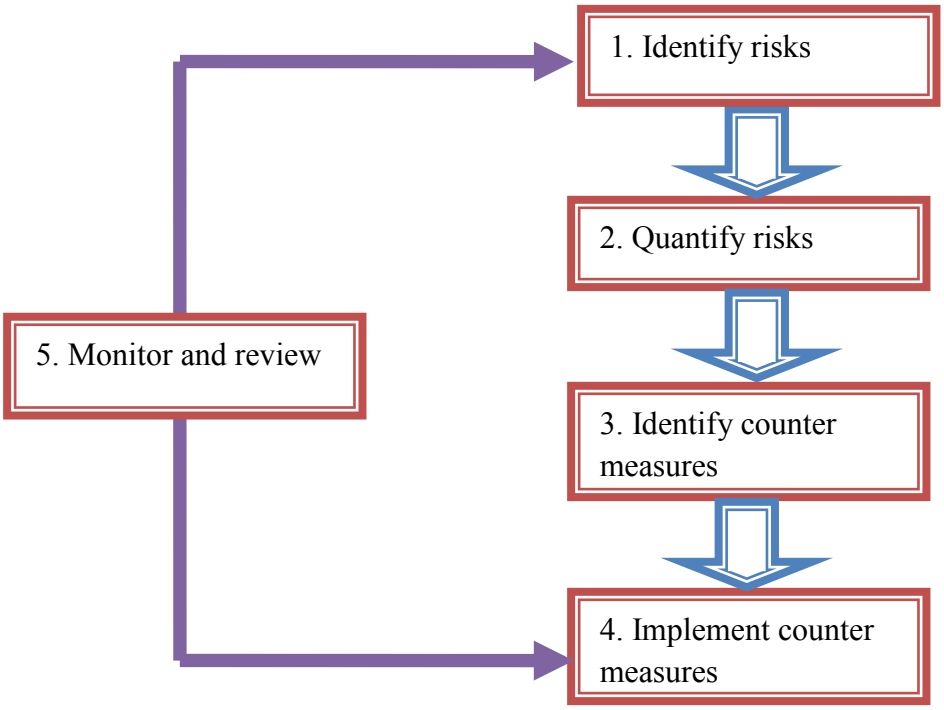
I) **Strategic level:** It encompasses risk management functions performed by senior management and BOD. For instance definition of risks, ascertaining institutions risk appetite, formulating strategy and policies for managing risks and establish adequate systems and controls to ensure that overall risk remain within acceptable level and the reward compensate for the risk taken.

II) **Macro Level**: It encompasses risk management within a business area or across business lines. Generally the risk management activities performed by middle management or units devoted to risk reviews fall into this category.

III) **Micro Level**: It involves „On-the-line" risk management where risks are actually created. This is the risk management activities performed by individuals who take risk on organization"s behalf such as front office and loan origination functions. The risk management in those areas is confined to following operational procedures and guidelines set by management.

The following diagram shows the risk management process adopted from Osborne (2012).

Figure 1: Risk management process



Stage 1: Before we can take any meaningful action to address our risk we need to know what we're up against. So we need to identify the risk we face.

Stage 2: Once we have identified our risks we need to quantify them. Because the risks that we are really interested in are those we consider significant enough to do something about. So we need a way to sort the wheat from the chaff. We do this by assessing the likelihood of the risk occurring and the impact if it does.

Stage 3: Once we know which risks are the most serious we can start to deal with them, by identifying and implementing possible counter measures or mitigation measures- methods of removing, reducing, controlling or recovering from an adverse events.

Stage 4: Having determined which counter measures we feel are sensible and cost effective and decided which one we want to interest in, we can go ahead and implement them.

Stage 5: To complete the process we must monitor the effectiveness, or otherwise, of the controls we put in place.

2.2.2 Main banking risks

The risks differ in their natures and occurrences pertaining to different business activities. That's to say that certain risks are particular in their natures that specifically affect the operations of a particular firm or industry, for instance banking industry. Likewise, risks associated with banking service differ by type of service rendered. Banks face a number of risks in order to conduct their business, and how well these risks are managed and understood is a key driver behind profitability, and how much capital a bank is required to hold[5].

Machiraju (2008) has argued, banks have to manage four significant forms of risk to earn profits for maximizing shareholders wealth. These are credit risk, interest rate risk, liquidity risk, and operational risk. He also argued that, there is systematic risk arising due to various disruptions in the working of major bank which in no time could spread to other banks or the whole financial system.

[5] This part is accessed from http://.en.wikipedia.org/wiki/Bank#Risk_and_capital

2.3 Banking operational risk

2.3.1 Conceptualization

With regard to the definition of operational risk, there is no universally accepted single definition that fit all banks. But, the most commonly used among industry is the one that the Basel committee on banking supervision adopted though there is also a criticism on this definition,

"The risk of direct or indirect loss resulted from inadequate or failed internal processes, people, and systems or from external events."

This definition includes legal risk but excluded both strategic and reputational risks. According to Basel Committee on banking Supervision (2004), legal risk itself includes, however not limited to, exposure to fines, penalties, or disciplinary damages as a result from supervisory actions , as well as private settlements. However, this definition excludes strategic and reputation risk. Strategic risk, for instance strategic misguided of business decision and reputational risk is a loss as a result of decline in firm‟s valued due to damaged firm‟s image.

In Ethiopia‟s context as of NBE‟s Commercial banks risk management guideline (2010), operational risk is defined as,

"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."

Additionally, the operational risk category includes IT, legal, regulatory, strategic, reputational, and systematic risks as per the guideline.[6]

[6] Ibid.

2.3.2 Operational definition

For the sake of this study the common industry wide definition adopted by Basel committee has been used. Hence, in this study, operational risk is 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.

As of Basel Committee on Banking Supervision‟s (Hereinafter BCBS) definition, there are four causes of operational risk viz. process, people, and system or external events. With regard to decomposition of BCBS‟s operational risk causes, Moosa (2008) cited the work of Mestchian (2003) suggests the decomposition of the definition of the BCBS into the following components:

1. Process risks, such as inefficiencies or ineffectiveness in the various business processes within the firm. These include **value-driving processes**, such as sales and marketing, product development and customer support, as well as **value-supporting processes** such as IT, HR, and operations.

2. People risks, such as employee error, employee misdeeds, employee unavailability, inadequate employee development, and recruitment.

3. Technology (or system) risks, such as the system failures caused by breakdown, data quality and integrity issues, inadequate capacity, and poor project management.

4. External risks, such as the risk of loss caused by the actions of external parties (for example, competitor behavior, external fraud, and regulatory changes) as well as macroeconomic and socioeconomic events.

Moreover, according to Moosa (2008), the classification of operational losses (resulting from exposure to operational risk) can be approached from three alternative angles: the **causes** of operational failure, the resulting **loss events**, and the legal and accounting forms of **consequential losses**.

2.4 Basel accord for operational risk

The Basel Committee on Banking Supervision (BCBS) is the world‟s most important financial institution in the area of banking supervision and bank‟s risk management. The Basel Committee on Banking Supervision (BCBS) was formed by the central governors of the group of 10 countries (G-10) countries constituted of Belgium, Canada, France, Germany, Italy, Japan, Netherlands, Sweden, United States, Switzerland and United Kingdom. Aftermath of serious disturbances in international currency and banking markets (notably the failure of Bankhaus Herstatt in West Germany).

The Committee provides a forum for regular cooperation between its member countries on banking supervisory matters. Initially, it discussed modalities for international cooperation in order to close gaps in the supervisory net, but its wider objective has been to improve supervisory understanding and the quality of banking supervision worldwide.

According to BCBS (2009), it seeks to do this in three principal ways: by exchanging information on national supervisory arrangements; by improving the effectiveness of techniques for supervising international banking business; and by setting minimum supervisory standards in areas where they are considered desirable.

Capital Accord (Basel II) initially was published in January 2001, and its final version was released in 2004. The advanced version of Basel II was issued in 2006.

Manic (2008) stated,

> *BCBS tends to find the best common approaches and common standards for every member country in order to promote the advancement of risk management in the banking system, strengthen banking supervisory frameworks and to improve financial reporting standards. To achieve this, BCBS has published many documents in the field of capital adequacy, banking problems, accounting and auditing, core principles for effective banking supervision, credit risk and securitization, market risk, operational risk, money laundering and terrorist financing, transparency and disclosure. For the risk management the most important documents are the Basel Accords,* ***Basel I and Basel II****.*

Furthermore, Manic (2008) has indicated, where Basel committee has establishes risk measurement standards and minimum capital charge the banks should have to hold against its risk exposures.

The Basel committee BCBS (2006) proposes the two capital charges viz. regulatory and economic, to overcome possible consequences those risks.

Regulatory capital[7], also called the capital charge or the minimum capital requirement, is the capital defined by the regulators that bank should set aside as a buffer against its potential losses. The regulatory capital is meant to assure bank's ability to cover major potential losses (or to cover significant but not catastrophic losses) without causing a banking crisis. Consequently, regulatory capital management should ensure the soundness and the stability of the banking sector and protect depositors.

Economic capital is, on the other hand, every kind of capital (such as book capital, reserves, charges etc.) that can absorb economic losses without interrupting any banking activity. It is calculated according to the banks experts" opinions and it is not a subject of supervisory review.

Further, the economic capital management helps in identifying the measure of risks, base strategic decisions on accurate information, strengthen an institution's long-term profitability and competitiveness. Indeed, the regulatory and economic capitals are highly connected.

The universe of the risks which banks can face is composed of three basic types - credit, market and operational risk. In Basel I the main focus was on market and credit risk, leaving operational risk with no operational capital requirements.

[7] Ibid.

Basel II, as a big improvement of Basel I, has introduced the operational risk equally important as market and credit risks are. The risks are defined as following.

Credit risk is the risk that a counterpart will not be able to meet their contractual obligations for full value.

Market risk is the risk of losses in on- and off- balance sheet positions arising from movements in the level or volatility of market prices.

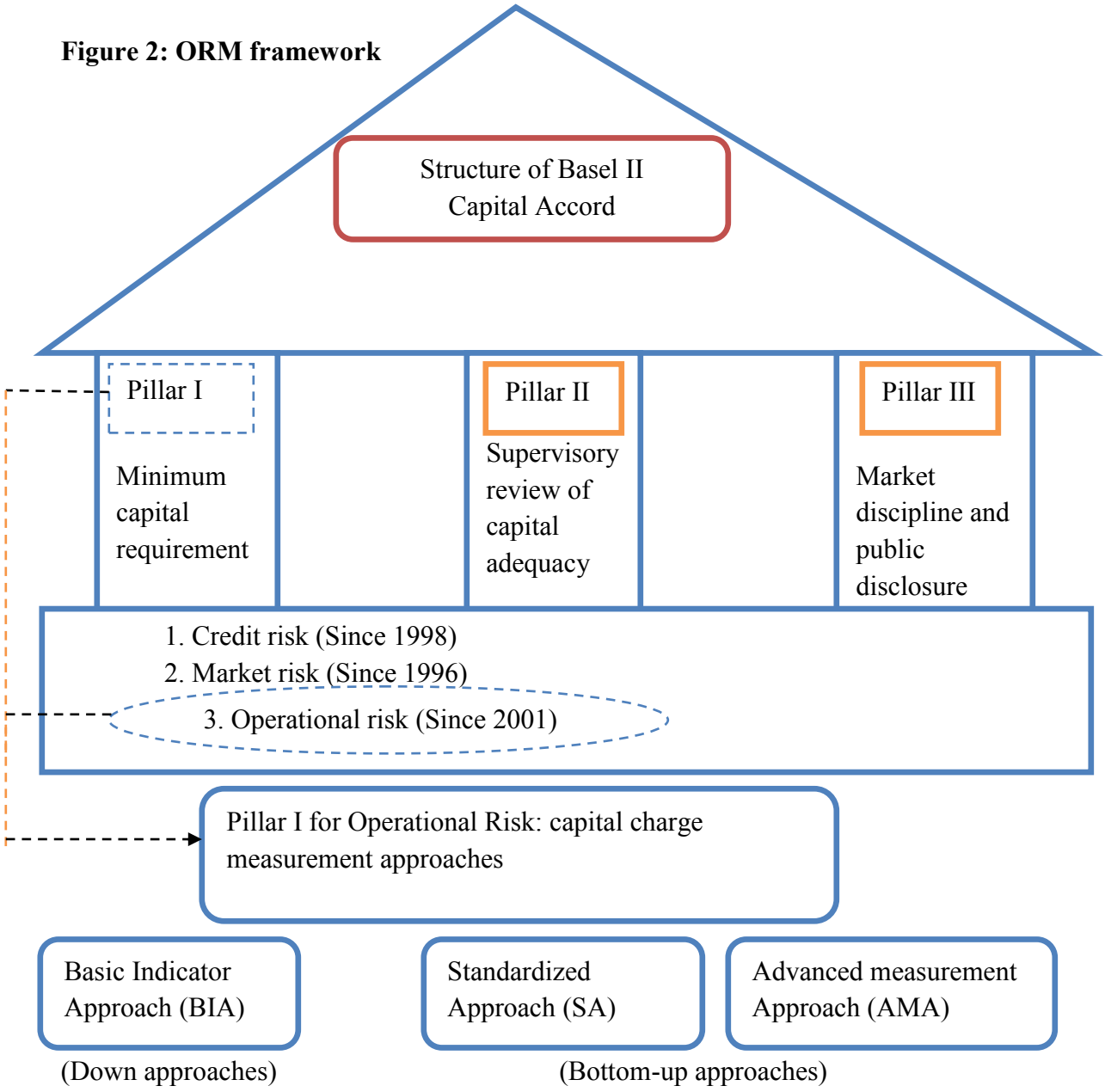
Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

Basel Committee on Banking Supervision (2006) stated that, the aim of Basel II is to promote safety and soundness in the financial system. It means that it should make capital requirement sensitive to bank's risk, maintain current level of firm's capital, focus on international banks and apply comprehensive risk approach.

As of the Basel committee‟s (Basel II) capital accord (BCBS, 2006) proposes three methods for operational risk capital calculation. These are basic indicator approach (BIA), the standardized approach (TSA) and advanced measurement approach (AMA) used by banks in continuum of risk sensitivity and the level of sophistication.

According to Pinedo (2009), the operational risk measurement framework of Basel committee can be shown as follow on the below diagram,

Figure 2: ORM framework



Structure of Basel II Capital Accord and Pillar I for operational risk
(Source: Michael Pinedo, 2009)

2.5 Operational risk management

National bank of Ethiopia (NBE) in its banks risk management guideline (2010) has claimed that, in measuring operational risk and other banking risks, once the risks associated with a particular activity have been identified, the next step is to measure the significance of each risk. Each risk should be viewed in terms of its three dimensions: size, duration and probability of adverse occurrences. Accurate and timely measurement of risk is essential to effective risk management systems. Accordingly, it has stated that, managing operational risk is an important feature of sound risk management practice in any bank.

With regard to the importance of operational risk management (ORM) in financial industries, Yogieta (2011) stated that, failure in Operational Risk Management (ORM) by the financial institutions fuelled the subsequent Credit & Liquidity Crisis and the Financial Meltdown which engulfed the world in the closing months of 2008.

The reserve bank of India (2005) indicated that, operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward but is implicit in the ordinary course of corporate activity and has the potential to affect the risk management process. Adding to this concept, it has been indicated that management of specific operational risks is not a new practice; however, what is relatively new is the view that operational risk management is a comprehensive practice comparable to the management of credit and market risks.

Whether the operational risk is a new concept and why is the emphasis need to be given to it, Gunther and Christian (2005) have argued that, although operational risk is by itself not a new concept, it has by far not received the same amount of attention as credit and market risk until recent years.

Fundamental changes in financial markets, increasing globalization and deregulation, as well as corporate restructuring had a large impact on the magnitude and nature of operational risks confronting banks.

Operational risk is a pure risk associated with inadequate/failed internal processes, people, system or external factors which, unlike that of credit and market risk, cannot be assumed for a direct reward rather it‟s implicit that assumed in the ordinary course of banks operations. Operational risk is a multiplier that could lead the businesses to the consequential consequences. For instance, Credit risk arises as a result of the failure of the counter party who unable to pay the loan as per credit agreement terms and conditions, but at the same time it could happen due to operational failure, such as inaccurate credit appraisal and poor collateral management Yogieta (2011) has argued that, an analysis of credit crisis and failure of financial organization across the globe makes it apparent that underlying their failure were improperly managed operational risk.

She has also argued that, greed, increasing complexity of banking & financial products, major advances in technology, rapid expansion of bank operations, increasing vulnerability of financial institutions, poor modeling were amongst the causes of this meltdown.

It‟s clear that in banks risk management system, managing operational risk could largely contribute towards management of other risks and to safety and soundness of bank‟s risk profile as it has indicated in the bank‟s risk management guideline of NBE, 2010.

Furthermore, Indian reserve bank (2005) has mentioned that,

> *The quantification of operational risk is an important ingredient for undertaking cost-benefit analysis and estimating the impact of management actions. In categorizing an operational risk, operational risk manger is in addition to categorizing the risk; he/she has also interested in the frequency and severity of the operational risk losses.*

With regard to operational risk identification and measurement Yogieta (2011) has argued, the identification and measurement of operational risk at its evolutionary stage compared to the maturity that both credit and market risk have achieved. Moreover, she has argued that, the existence of wide recognition of operational risk management among the institutions on the globe. The major areas of concern include definition of operational risk, its measurement and formalization in theory culture.

For each risk category the number of loss events (frequency) and the magnitude of the losses (severity) occurring over a specific time period could be noted. As of Heru (2005), based on the three characteristics of operational risk namely, time of occurrence, when it has discovered and when it has recognized it is possible to determine the frequency and severity of operational risk losses.

Moreover, Balestra (2006) has indicated, based on frequency and severity of operational risk losses, there could be medium risk at high frequency low severity and low frequency high severity. But, the existence of low frequency low severity and high frequency high severity indicates low and high operational risk level respectively.

With regard to the availability of data on operational risk losses frequency and severity Balestra (2006) indicated that, there might be some difficulty of obtaining sufficient internal data on low frequency high severity; however, low impact high frequency operational losses should be well documented within the company and hence allow to use their whole set of statistical tools.

2.6 Quantification approach to operational risk measurement

"…. operational risk measurement is not the same as operational risk management. Quantifying those operational risks that lend themselves to quantification and neglecting the rest that does not constitute best practice…" (Cagan, 2001)

As it has stated in state bank of Pakistan"s commercial banks risk management guideline (2003), which underpins the level of difficulty of quantifying operational risk,

"… While a number of techniques are evolving, operating risk remains the most difficult risk category to quantify…."

Cumming and Hirtle (2001:3) have argued that there is a difference between risk management and measurement as cited by Khan and Ahmed (2001). Hence, there is a difference between risk measurement and risk management. While risk measurement deals with quantification of risk exposures, risk management refers to "the overall process that a financial institution follows to define a business strategy, to identify the risks to which it is exposed, to quantify those risks, and to understand and control the nature of risks it faces"

Operational risk measurement focuses on the calculation of capital for operational risk. Basel II provides three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity: (i) the Basic Indicator Approach; (ii) the Standardized Approach; and (iii) Advanced Measurement Approaches (AMA).

As of Basel II capital accord (June, 2006), proposes 3 measurement approaches. Each measurement approaches shall be discussed up next in the following sub-sections. As it has mentioned under paragraph 645 of the document, the three approaches are used to calculate the operational risk capital charges in a continuum of sophistication and risk sensitivity.

Furthermore, paragraph 646 dictates that, Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices. Qualifying criteria for the Standardized Approach and AMA see paragraph 660-679.

2.6.1 The basic indicator approach (BIA)

Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income. Figures for any year in which annual gross income, negative or zero should be excluded from both the numerator and denominator when calculating the average.

The charge may be expressed as follows:

$$K_{BIA} = [\sum(GI_{1\ldots n} X\ \alpha)] \Big/ n$$

Where:

K_{BIA} = the capital charge under the Basic Indicator Approach

GI = annual gross income, where positive, over the previous three years

N = number of the previous three years for which gross income is positive

α = 15%, which is set by the Committee, relating the industry wide level of required capital to the industry wide level of the indicator.

The Basel Committee proposes the gross income as the only exposure indicator. The Gross income is defined as net interest income plus non net interest income. The broad explanation of Gross incomes has been described in paragraph 650 of the document (BCBS, June 2006).

Paragraph 651 moreover indicated that, as a point of entry for capital calculation, no specific criteria for use of the Basic Indicator Approach are set out in this Framework. Nevertheless, banks using this approach are encouraged to comply with the Committee‟s guidance on *Sound Practices for the Management and Supervision of Operational Risk*[8], February 2003.

2.6.2. The standardized approach (TSA)

As of Basel Capital Accord (Basel II) the second operational risk capital charge calculation approach is the Standardized Approach (TSA). In the Standardized Approach, banks‟ activities are divided into eight business lines: corporate finance, trading & sales, retail banking, commercial banking, payment & settlement, agency services, asset management, and retail brokerage. Within each business line, gross income is a broad indicator that serves as a proxy for the scale of business operations and thus the likely scale of operational risk exposure within each of these business lines. The capital charge for each business line is calculated by multiplying gross income by a factor (denoted beta) assigned to that business line. Beta serves as a proxy for the industry-wide relationship between the operational risk loss experience for a given business line and the aggregate level of gross income for that business line.

It should be noted that in the Standardized Approach gross income is measured for each business line, not the whole institution, i.e. in corporate finance, the indicator is the gross income generated in the corporate finance business line.

As mentioned under paragraph 654 of Basel II, the total capital charge is calculated as the three-year average of the simple summation of the regulatory capital charges across each of the business lines in each year. In any given year, negative capital charges (resulting from negative gross income) in any business line may offset positive capital charges in other business lines without limit. However, where the aggregate capital charge across all business lines within a given year is negative, then the input to the numerator for that year will be zero.

[8] Please look up appendix 6

The total capital charge may be expressed as:

$$K_{TSA} = \{\sum_{Years1-3} \max [\sum(GI_{1-8} X \beta_{1-8}), 0]\} / 3$$

Where:

K_{TSA} = the capital charge under the Standardized Approach

GI_{1-8} = annual gross income in a given year, as defined above in the Basic Indicator Approach, for each of the eight business lines

β_{1-8} = a fixed percentage, set by the Committee, relating the level of required capital to the level of the gross income for each of the eight business lines. The values of the betas are detailed below.

Table 1: Beta values for TSA

Business lines	Beta Factors
Corporate finance (β1)	18%
Trading and sales (β2)	18%
Retail banking (β3)	12%
Commercial banking (β4)	15%
Payment and settlement (β5)	18%
Agency services (β6)	15%
Asset Management (β7)	12%
Retail Brokerage (β8)	12%

It is possible that in any given year, negative capital charges - resulting from negative gross income in any business line may offset positive capital charges in other business lines without limit (national supervisors may implement a more conservative action to negative gross income) .

Nevertheless, when the capital charge sum from all business lines within a given year is negative, the input to the numerator for that year will be zero (as given by the *max* function in the Equation above). It is further noted in [(BCBS, June 2006), footnote 99] that if negative gross income distorts a bank‟s Pillar 1 capital charge under the Basic Indicator and Standardized Approach, supervisors will consider appropriate supervisory action under Pillar 2.

The use of the Standardized Approach (TSA) as a measurement of operational risk is subject to the qualifying criteria listed out under paragraph 660-663 of the Basel document, *"International Convergence of Capital Measurement and Capital Standards"* June, 2006.

2.6.3. Advanced measurement approaches (AMA)

Paragraph 655 of the Basel II, 2006 describes, under the AMA, the regulatory capital requirement will equal the risk measure generated by the bank‟s internal operational risk measurement system using the quantitative and qualitative criteria for the AMA as listed under paragraph 664-679. Use of the AMA is subject to supervisory approval.

Moreover, as mentioned under paragraph 658, the appropriateness of the allocation methodology will be reviewed with consideration given to the stage of development of risk-sensitive allocation techniques and the extent to which it reflects the level of operational risk in the legal entities and across the banking group. Supervisors expect that AMA banking groups will continue efforts to develop increasingly risk-sensitive operational risk allocation techniques, notwithstanding initial approval of techniques based on gross income or other proxies for operational risk

2.7 Basel committee's operational risk loss events[9] and business lines[10]

Rippel and Teply (2011) claimed that, there are most widely known operational risk events of severe magnitude that occurred in the last few years; most publicly known examples of operational risk include a loss of of $7.3 billion at Société Générale in 2007 or more recently the $65 billion Ponzi scheme by Mr. Bernard Madoff and the $8 billion bank fraud of Sir Allen Stanford. Besides, Teply (2010) has stated that during global financial crisis that engulfed the world in 2008, the operational risk events had occurred , such as failed risk management processes or mortgage frauds committed by applicants when cheating on their income in order to secure a loan.

[9] Please, refer to appendix **5**
[10] Please, refer to appendix **4**

As it has mentioned in the Basel II operational risk framework (2003), business lines/functions are corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency service, asset management and retail brokerage. The event types include internal fraud, external fraud, employment practices and work place safety, clients, products and business practices, damage to physical assets, business disruption and system failures, execution, delivery and process management.

According to BCBS (February, 2003), operational risk event types that the Committee in cooperation with the industry – has identified as having the potential to result in substantial losses includes:

- Internal fraud (IF). For example, intentional misreporting of positions, employee theft, and insider trading on an employee‟s own account.
- External fraud (EF). For example, robbery, forgery, cheque kiting, and damage from computer hacking.
- Employment practices and workplace safety (EPWS). For example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability.
- Clients, products and business practices (CPBP). For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank‟s account, money laundering, and sale of unauthorized products.
- Damage to physical assets (DPA). For example, terrorism, vandalism, earthquakes, fires and floods.
- Business disruption and system failures (BDSF). For example, hardware and software failures, telecommunication problems, and utility outages.
- Execution, delivery and process management (EDPM). For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

Depending on the business functions (business lines) and event types, operational risk losses can be modeled in terms of its frequency and severity. Besides, using the three characteristics of operational risk namely, time of occurrence, when it has discovered and when it has recognized it is possible to determine the frequency and severity of operational risk losses.

With regard to the availability of data on frequency and severity of operational risk losses Balestra (2006) has indicated that, there might be some difficulty of obtaining sufficient internal data on low frequency high severity; however, low impact high frequency operational losses should be well documented within the company and hence allow to use their whole set of statistical tools.

2.8 Empirical review

This part discusses some of the empirical evidence of the previous study undertaken by different individuals with regard to banking operational risk, taking into account the regulatory body set of guidelines and standards that ensures sound risk management practice.

Let first see these two authors who have discussed the importance and use of operational risk management tools in case of South African banking industry. Key risk indicator (KRI) is one of the operational risk management tools that can clearly indicate the area of risk exposure in routine banking operations. In fact, among the other tools, KRI shows the current risk exposure that immensely helps tracking of operational risk factors (Loss events). First, Young (2012) on his article entitled „the use of key risk indicators by banks as an operational risk management tool: A South African perspective" has came up with the following conclusion, banks, in general, are not suitably prepared to implement a key risk indicator management process. There seems to be a general lack of understanding of the underlying theory and concept of the criteria to use key risk indicators and the advantages of using key risk indicators are not fully exploited. Furthermore, he has also discussed the importance of KRI, it is crucial that banks ensure that a sound key risk indicator (KRI) management process is embedded to serve as an operational risk management tool and that all employees are knowledgeable and therefore prepared to exploit the benefits of a KRI management process for the organization.

Even though the purpose of this study is not about operational risk management tools, among the existing operational risk management tools KRI indicates the current risk exposures while the other indicates either the past or future risk exposures. Hence, as it has already mentioned that as long as banks continuing to operate operational risk is inevitable and the best way of identifying, categorizing and measuring operational risk factors (Loss events) are by prudently exercising the use of key risk indicator (KRI). Thus, to manage operational risk carefully and in calculated manner the use of KRI is an essential in banking operational risk management process.

Second, according to Modiha (2011) study on critical evaluation of operational risk tools of South African AMA banks, though she has found gaps in usage of operational risk tools of respective banks, she has deduced that the operational risk tools are largely integrated in to day-to-day business process and represent the operational risk exposures and profile of the AMA banks. Moreover, she has indicated that inaccurate calculation of operational risk capital charge could lead to huge reputational and financial risk for these banks. Here it‟s arguable that, the use of operational risk management in once banking risk management should indicate the inherent operational risk exposures and should extremely supports the computation of capital charge (economic capital) to protect against operational risk consequences.

Above all, in operational risk management the presence of awareness among employees, as well as, the attention paid to it in the bank‟s risk management process is very crucial. And banks need to have strong risk management structure and committed management. Here are two studies undertaken in order to determine the awareness and due importance given to operational risk of banking industry: A study undertaken by Yogieta (2011) has identified an evidence of heightened awareness and due emphasis given to operational risk by Indian banks. Moreover, she has determined that, the practices of average and small sized public sector and old private sector banks were be lagging behind that of new private sector banks in usage of business environment and internal control factors (BEICFs) such as (RCSA, KRIs), usage of scenarios, updating of these indicators and collection and usage of external loss data. She has also identified the existence of wide gap in the range of practices followed by Indian Banks and the advanced measurement approach (AMA) compliant banks worldwide.

Meanwhile, Kwasi (2010) on his risk based assessment of Ecobank Ghana limited has revealed that, the bank had adequate risk management structure to ensure sound risk management of operational risks, which can be supported with the fact that existence of Strong risk culture in the bank as all staff are conscious about the risks inherent in their activities are always on the lookout to avoid or minimize the incidence of risk. This has been made possible through extensive regular education and training on risk issues in the bank coupled with the central role risk awareness play in the performance base remuneration system.

After all, as the causes (sources) of operational risk are people, internal process, system failure and external events, all operational risk factors (Loss events) are categorized in one of these sources. Thus, it‟s very crucial in creating an awareness among the staffs like by providing an education and training regularly and update them timely with the new events happening in the banking operations. Similarly, by following the existing formal procedures and guidelines in undertaking ones activities it‟s possible to overcome the contributory operational risk factors that could lead to unforeseen consequences.

Commercial banking business involves accepting deposits from its savers and lends these deposits to the borrowers subject to a certain regulations. Risk taking is an integral part of banking businesses; hence, mostly banks pay attention to liquidity, credit and market risks in their risk management processes. However, loss could also occur as a result of risks other than credit and market risk in banking day-to-day functions attributed to failure in its operations. The study undertaken by (Gunther and Christian, 2005; Anna, 2006) have indentified that, recent banking failures clearly attributed to losses unrelated to credit and market risk as a result of fundamental changes in financial markets, increasing globalization and deregulation, corporate restructuring and revolutionary technology innovation. And these paves the way for the development of operational risk awareness, as those factors had huge impact on the magnitude and nature of operational risks confronting banks.

Based on the two dimensions of operational risk events, namely frequency (likelihood) and severity (impact) it is possible to quantify operational risk. However, it could be difficult to have a data on low frequency and high severity loss events. But, banks can capture and store loss data on high frequency and low severity that can help the quantification of loss events.

Heru (2005) has indentified non existence of linear relationship between the two variables of operational risk loss events, namely: (1) the loss amount and (2) the time interval between the moment an event is discovered and the moment an event is recognized as an operational risk loss event. However, he has found out that the variable (2) is more related to the characteristic of a business unit and the method to recognize the operational loss events in that business unit.

As far as operational risk quantification approaches concerned which has already discussed, its use differs among banks based on the risk sensitivity and increasing continuum of sophistication in banking activities. To deal with management of operational risk it is inevitable to measure it first, what is said in management "what you can‟t measure, you can‟t manage", however, it‟s difficult to quantify all operational risk factors (Loss events). Thus, experts suggest the use of quantitative and qualitative mechanisms whenever it is appropriate. The developed world have made some step forward with the use of the Basel Committee‟s operational risk quantification approaches, as the findings of observed range of practice in key elements of AMA (Loss data collection exercise, 2008) conducted by the Basel committee has shown. Likewise, they do have consortium called operational risk exchange where the member banks are expected to report their internal losses to this consortium so that other member banks will make use of this external losses in measuring their inherent operational risk losses. Thus, in such a way they deal with the potential consequences of operational risk besides strengthening their internal control and follow up mechanisms.

To my knowledge, most of the developing world including Ethiopia, the practice of operational risk management is at its infant stage as most risks the banks gives due care are credit, liquidity and interest rate risk. It is undeniable fact that these risks are an integral part of the banking businesses; however, the operational risk is too significant in banking industry‟s functions.

In Ethiopia‟s case, most dominantly due emphasis to banking risk management in general was initiated after the incidence of financial crisis in the closing month of 2008 that engulfed the western world (Specifically USA) of Mortgage banks. In fact, the regulatory body of the country has first issued the commercial banks risk management guidelines in 2003 and revised it in 2010 to include the latest development in the areas which is being in use.

But, as far as operational risk concerned, it‟s different from the customary banking risks due to its characteristics of the time of occurrence, discovery and recognition. As the identification of these characteristics takes time its potential materialization will lead banks to incur huge losses or even force them to bankruptcy. Thus, in order to measure and manage the operational risk in prudent manner it is very crucial to deal with the operational risk factors (Loss events) as all of them could be as a result of internal inefficiency, people errors, system failure and/or external events. Besides, it‟s very crucial to inspect and review the routine banking operations so as to clearly explore the contributory operational risk factors that would significantly contributes to the effectiveness of banking industry‟s operational risk management.

Generally, in Ethiopia‟s case, to my knowledge as operational risk management is at its infancy stage, it‟s very essential to have committed management and good internal control that takes in to account the identification, categorization and measurement of operational risk factors (loss events) by cross checking all banking activities to clearly indicate possible risk exposure areas. Moreover, it is very important to stick to banks guidelines and procedures of operational risk management in performing ones activity and management are expected to supervise, follow-up and revise the guidelines whenever and wherever necessary to include latest development in banking activities. Hence, in such a way that the contributory operational risk factors that would have been prevented but happened and affected the banking operations can be managed ultimately.

2.9 Conceptual framework of the study

For the sake of clear depiction and understanding of operational risk management, the researcher has adapted Samad-Khan‟s model as the study conceptual framework. The Basel committee believes that,

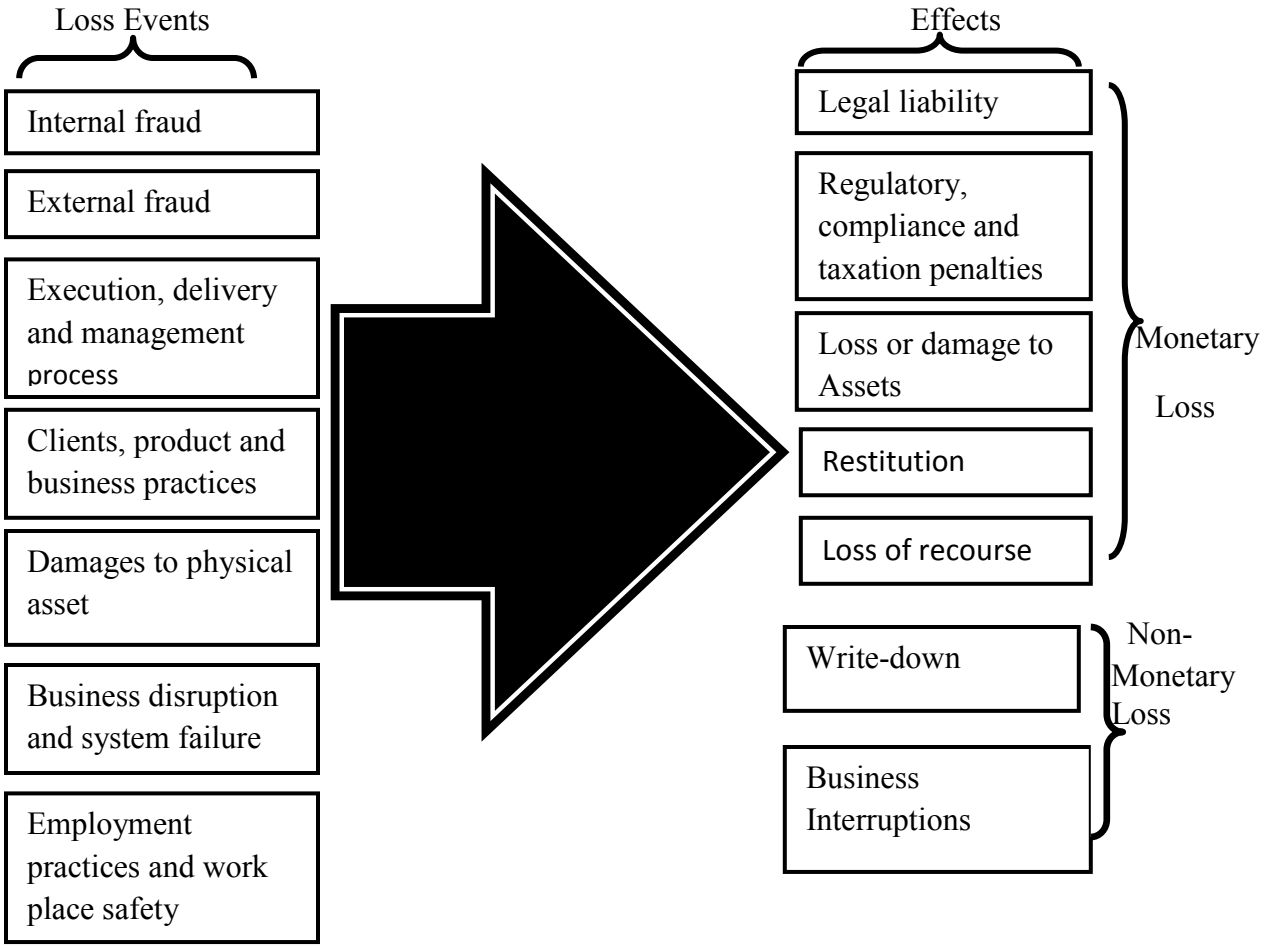
“Similar rigor should be applied to the management of operational risk, as is done for the management of other significant banking risks.”

The generic risk management model consists of risk identification, evaluation, estimation and mitigation practices. Of course, risk management can be described by the mitigation practices one can undertake. As it has mentioned in banks risk management guideline of National Bank of Ethiopia (2010), there is no single risk management system that would fit for all banks.

Consequently, the NBE requires each bank to develop its own comprehensive risk management system tailored to its needs and circumstances, however, must cover all banking risk indicated in the guideline[11].

The guideline has stated the operational risk management besides the other banking risks guidelines. However, for the purpose of this study some of the banks in the country have selected to determine the correlation of operational risk events and its effect, to explore contributory factors and to determine the board‟s approval of policies and procedures of operational risk management.

Hence, the Samad Khan‟s (2007) graphical depiction of operational risk factors and effects was adapted for the purpose of this study.



[11] Ibid

Chapter 3: Research approach and methodology

3.1 Introduction

This chapter outlines the rationale of research approach and methodology used in this study. It includes research approach, research design, data type, research method, sampling design, unit of analysis, variables of the study, data analysis methods , reliability and validity.

3.2 Research approach

Data collection techniques for assessing operational risk management can be classified as either quantitative or qualitative method. Non-numeric data such as observational or interview data represents the qualitative measures, whereas, numeric assessment such as numeric scores and metric like questionnaire is used as quantitative measures (Bhattacherjee, 2012). Likewise, (Griffin et al., 2010) has claimed that, qualitative research is not about applying specific numbers to measure variables or using statistical procedures to numerically specify a relationship‟s strength. Hence, the research approach employed in this study is mixed approach which is claimed by (Creswell, 2010:21) as,

> *A mixed methods approach is one in which the researcher tends to base knowledge claims on pragmatic grounds (e.g., consequence-oriented, problem-centered, and pluralistic). It employs strategies of inquiry that involve collecting data either simultaneously or sequentially to best understand research problem. The data collection also involves gathering both numeric information (e.g., on instruments) as well as text information (e.g., 00on interviews) so that the final database represents both quantitative and qualitative information.*

Particularly, among the types of the mixed method approaches, the researcher has employed the concurrent triangulation approach/strategy. Creswell (2010:248) has explained that, the model is selected when a researcher uses two different methods in an attempt to confirm, cross validate or corroborate findings within a single study.

Besides, the model generally uses separate quantitative and qualitative methods as a means to offset the weaknesses inherent within one method with the strength of the other method. Ideally, the priority would be equal between the two methods, but in practical application the priority may be given to either quantitative or the qualitative approach. Moreover, continuing with his explanation, the concurrent triangulation approach integrates the results of the two methods during interpretation phase.[12] Thus, this study has integrated both approaches in interpretations of the analysis of the data findings.

3.3 Research Method

This study was employed the survey research which has defined by Bhattacherjee (2012) as, research method involving the use of standardized questionnaires or interviews to collect data about people and their preferences, thoughts, and behaviors in a systematic manner.

Survey method can be used for descriptive, exploratory, or explanatory research. It has also shown that though the method best suited that have an individual people as the unit of analysis, other unit of analysis such as groups, organizations or dyads (Pairs of organizations, such as buyers and sellers), are also studied using surveys, such studies often use a specific person from each unit as "key informant" or a "proxy" for that unit[13].

Hence, in this study based on sources of data primary method of data collection was performed. The primary data was collected by distributing a structured questionnaire to respondents (the bank"s risk management department employees (Risk Experts) and internal auditors**.** As the study is at institutional level, the risk management department employees and internal auditors were asked their view on a series of questionnaires distributed to them. Besides, as a primary data collection means, the structured interview has also been used.

[12] Ibid.
[13] Ibid.

3.4 Research design

Bhattacherjee (2012) defined a research design, a comprehensive plan for data collection in an empirical research project. It has also indicated the two categories of data collection techniques used in scientific research, quantitative and qualitative design. Despite the apparent separation of these techniques, it should be noted that quantitative design does not necessarily exclude collection of qualitative data, or vice versa. And, hence "mixed-mode designs" that combine features of quantitative and qualitative designs and collect both types of data may be desirable.

In this study both qualitative (Structured interview) and quantitative (Questionnaire) methods were used in order to collect a data to explore the operational risk management of the selected commercial banks. Thus, the study has used the mixed mode designs.

3.5 Data type

In this study both qualitative and quantitative data for which its sources is primary was employed. In order to get primary data both structured questionnaire and structured interview were used. Since, the questionnaire items have an ordinal measurement scale an ordinal (quantitative) and structured interview (qualitative) data were integrated under data interpretation section.

3.6 Unit of analysis

According to Bhattacherjee (2012), the unit of analysis may be a person, group, organization, country, object, or any other entity that you wish to draw scientific inferences about.

In this study unit of analyses are commercial banks which the researcher has opted for using particularly, risk management department staffs as a „key informant" or „proxy" for the banks as the study focus is at institutional level. Moreover, the only section that can provide the reliable data on the subject matter is technically the risk management department staffs as the other department will not have enough knowledge or know-how about the study subject.

3.7 Sampling design

The study was confined to commercial banks operational risk management evaluation at institutional level (Top down model) as Smithson (2003) described,

"Most of the published descriptions of operational risk modeling subdivide the models into two ***groups****: "Top down" models estimate operational risk for the entire institution."*

The sampling frame, also known as a working population opted is a non-probability sampling method, containing units or people who are most conveniently available (Griffin et al., 2010). Hence, purposive (Convenience) sampling technique as Bhattacherjee (2012) defined, a technique in which a sample is drawn from that part of the population that is close to hand, readily available, or convenient, has been used to select the banks to be studied.

For the sake of this study 12 commercial banks in Ethiopia have considered. The researcher used their years of establishment and the structure of risk management department as a criterion in selection to correctly fit the objectives of the study. For this study the most conveniently available respondents are respective banks staffs working at the institutional (Headquarter) level. However, a researcher has selected the risk management department staffs and internal auditors as he thought that those individuals/staffs have in depth insight with regard to the study subject, and consequently will provide reliable information which could indicate the real situation of the respective banks operations. Thus, the sample of the study comprises of operational risk officers, risk experts and internal auditors of the banks.

The sample size differed per the structure of the risk management of the respective banks as it is at infancy stage. The minimum estimated sample size (n) of the risk management staffs of the selected banks was 60. That is, it has presumed that there will be five staffs at each banks risk management department.

3.8 Research Instrument

The research instruments used in this study were both questionnaire and personal interview. The questionnaire has carefully designed in such a way that the respondents would understand easily. Due care has also taken in developing the questionnaire items. Accordingly, it has developed by taking in to account the following regulatory body and Basel committee‟s risk management documents,

- National Bank of Ethiopia‟s (NBE) (2010), Commercial banks risk management guidelines.
- Basel Committee on Banking Supervision (2011): "principles for the sound management of operational risk", Banks for International Settlements, Basel
- Basel Committee on Banking Supervision (June 2006): "International Convergence of Capital Measurement and Capital Standards"

The questionnaires were arranged on the following range:

- 1 (Strongly disagree), 2 (Disagree), 3 (Somewhat agree), 4 (Agree), and 5 (Strongly agree).
- 1 (Very insignificant), 2 (Insignificant), 3 (Moderately significant), 4 (Significant), and 5 (Very Significant)
- Also, it consists of closed ended questions coded as: 0 (No) and 1 (Yes).

The questionnaire has three parts, the first part focused on the rating of operational risk factors (Loss events) and operational risk effects, the second part constitute contributory operational risk factors and the last part focused on risk management guidelines and procedures of the banks. **(See Appendix 2)**

Likewise, the personal interviews were conducted with officers (Risk experts) on a structured base to have an overall view of the practices of ORM.

3.9 Variables of the study

The variables of the study are **operational risk effect** (dependent variable) which measured on five point likert scale (its significance level) and **operational risk factors (loss events)**[14] (independent variables) similarly measured on five point likert scale (their significance level).

From the banks perspective the materialization of operational risk (whatever its cause people, system failure, internal process or external events) would result into both monetary and non-monetary losses. The monetary losses may be in the form of loss or damage to physical assets, legal liability, regulatory, compliance and taxation penalties. Likewise, the non monetary loss could be reputational (public image) and business interruptions.

According to BCBS (2003) as it has already been discussed under chapter two, the operational risk factors (Loss events) are those factors that could lead to losses (monetary or non monetary) due to management incapability or ineffective monitoring and control mechanisms. For loss events classification and detailed description, please **refer appendix 5.**

3.10 Methods of data analysis

As the study constituted numeric data (ordinal data) that have collected via questionnaire and text data (Interview), spearman correlation coefficient, descriptive data analysis and multi factor analysis method was used in order to analyze the collected data.

As the collected data was having an ordinal scale of measurement (measured on 1 up to 5 points) and close ended questions (Coded as 1 for „yes" and 0 for „no"), it has captured onto **SPSS 20** to support the presentation of the data.

As **descriptive data analysis method**, tables and charts were used to represent the results as well as to interpret the findings clearly. Moreover, the spearman correlation was used to determine the correlation significance between operational risk effect and operational risk events. The justification for the use of spearman correlation coefficient (Rho) over the Pearson correlation coefficient as claimed by Kossowski and Hauke (2011) states,

[14] For detail explanation, Please refer appendix 5

"Unlike Pearson"sproduct-moment correlation coefficient, it does not require the assumption that the relationship between the variables is linear, nor does it require the variables to be measured on interval scales; it can be used for variables measured at the ordinal level."

As an **inferential analysis method**, factor analysis has been also used to explore the contributory operational risk factors that accounted for variance in operational risk management. Decoster (1998) stated that, factor analysis is a collection of method used to examine how underlying constructs influence the response on a number of measured variables.

Even though there are different types of factor analysis methods, the researcher has opted for the most often used factor analysis method called principal component analysis (PCA). Decoster (1998) claimed that, the purpose of PCA is to derive a relatively small number of components that account for the variability found in a relatively large number of measures. This procedure, called data reduction is typically performed when a researcher does not want to include all of the original measures in analysis but still want to work with the information that they contain.

Moreover, Webster (2010) has argued that, the goal of factor analysis is to explain multiple variables by a lesser number of factors. Besides, in principal component analysis in the initial solution, each is standardized to have a mean of 0.0 and a standard deviation of $\pm$ 1.0. Thus, the variance of each variable is equal to 1.0. Since a single variable can account for 1.0 unit of variance a useful factor must account for more than 1.0 unit of variance, or have an Eigen value $\lambda > 1.0$. Otherwise the factor extracted explains no more variance than a single variable.

3.11 Reliability and validity of the study variables

3.11.1 Reliability

As of Bhattacherjee (2012) reliability is the degree to which the measure of a construct is consistent or dependable. In other words, if we use this scale to measure the same construct multiple times, do we get pretty much the same result every time, assuming the underlying phenomenon is not changing?

In order to make sure that the questionnaires are reliable and internally consistent the Cronbach‟s alpha was used and computed for each variable with multi item scales. For instance, the dependent variable, operational risk effect has four items; hence operational risk effect Cronbach‟s alpha value was computed from these four items as discussed under chapter four. With the same fashion, the reliability of the independent variables was computed using Cronbach‟s alpha.

3.11.2 Validity

As of Marczyk, DeMatteo, and Festinger (2005), the concept of ***validity*** refers to *what* the test or measurement strategy measures and *how well* it does so. Conceptually, validity seeks to answer the following question: "Does the instrument or measurement approach measure what it is supposed to measure?" Similarly, as of Bhattacherjee (2012), **Validity**, often called construct validity, refers to the extent to which a measure adequately represents the underlying construct that it is supposed to measure. Hence, to make measurement approach or instrument robust thorough analysis of both theoretical and empirical literatures were performed and consequently the study variables were developed.

With regard to **internal validity (causality),** tough this study is not about causal relationship between variables, the constructs and its attributes/items are developed taking into account international standards and guidelines of operational risk management documents besides the regulatory guidelines of commercial banks risk management that includes operational risk management.

Marczyk et al (2005) has stated that, **external validity** is concerned with the generalizability of the results of a research study. Thus, the external validity (generalizability) of this study has made robust as the identified constructs and its attributes/items are what an international financial institutions, banks, are most often faces and they are identified and categorized by BCBS, which is the world oldest and known financial organization that provides banking supervision and guidance including banking risk management guidelines. Moreover, the regulatory body of the country has also adapted this BCBS documents in its commercial banks risk management guidelines.

As long as **construct validity** concerned Marczyk et al (2005) discussed the focus of construct validity by saying, the focus of construct validity is usually on the study‟s independent variable. In essence, construct validity asks the question of whether the theory supported by the findings provides the best available explanation of the results. Likewise, Bhattacherjee (2012) has explained that, **construct validity** examines how well a given measurement scale is measuring the theoretical construct that it is expected to measure. In this study the independent variables were the seven operational risk factors (loss events) which could lead the banks to incur a loss (monetary or non monetary) as classified and known operational risk factors by Basel Committee. In fact, the seven variables were measured by their attributes/items ranging from 2-5 and were used in Spearman correlations analysis to determine the direction and strength of association they have with operational risk effect.

According to Bhattacherjee (2012), **Statistical conclusion validity** examines the extent to which conclusions derived using a statistical procedure is valid. In this study for the sake of analyzing the numeric (quantitative data) two statistical methods were employed as per the study objectives.

The first one is the **Spearman correlation coefficient** as descriptive statistics (Bivariate statistical analysis)**,** it has used to determine the direction and strength of association between variables of the study. The justification for using this correlation has already mentioned above. As it has already mentioned the variables of the study are the operational risk effect (dependent variable) and the seven loss events (independent variables). The dependent variable was measured on four scale items, where for each respondent the **median** of his/her response has calculated and used. Likewise, as independent variables have their own measurement scale items ranging from 2-5 and their median were computed and used similarly. The way the median of each variable computed has shown under results and discussions of chapter four.

The second statistical data analysis method used in this study was **factor analysis (Principal Component Analysis)** as an inferential statistics. By referring and analyzing thoroughly both theoretical and an empirical literatures 20 operational risk factors (loss events) were developed and the respondents‟ were asked to rate each factors on five point likert scales ranging from strongly disagree (1) to Strongly agree (5). The justification for the use of principal component analysis has already mentioned above under method of data analysis section.

Chapter Four: Results and Discussions

This chapter introduces the research results and discussions. And it includes the introduction, validity and reliability analysis and discussion of the research questions.

4.1 Introduction

The questionnaires were distributed to a population of 96 risk management department staffs and internal auditors of 12 both public and private commercial banks[15] in Ethiopia. 85 questionnaires were returned on the due date, which represented a response rate of 88.5% but unfortunately 5 questionnaires were found incomplete and have been discarded consequently. This enhances the completeness and integrity of the data. Thus, only 80 questionnaires were used as 100% in data analysis.

The returned questionnaires are more than initially estimated minimum sample of 60. The extra responses were used as large sample adds more value and boost the quality of the result.

4.2 Validity and Reliability analysis

To make sure the validity of the questionnaire, the items of the questionnaire were developed based on thorough review of both theoretical and empirical literatures. Likewise, repeated discussions were held with one of the banks risk expert to have depth insight in order to contextualize the study variables. Moreover, the pilot test was made at Commercial bank of Ethiopia to obtain the respondent"s feedbacks, which were ultimately used in the final preparation of the questionnaire.

With regard to internal consistency, Cronbach alpha values were computed for multi item scales. Accordingly, the operational risk effect and operational risk events (Loss events) were computed as indicated below. **(See Table 2)**

As of Kehoe (1995) reliable scales can have minimum Cronbach Alpha (**α**) of **0.5**:

An Alpha value of at least 0.5 should be achieved for accepting the items "as is" within a dimension, as long as they are within a short instrument (10-15) items.

On the other hand, a rule of thumb that has been advocated in the literature (Nunnally, 1998) is to require *Cronbach alpha (**α**)* to equal **0.70** or exceed it before the items are considered internally consistent.

[15] For the list of banks contacted, please refer to appendix 1

Table 2: Reliability coefficient of the study variables

Variables	Number of items[16]	Cronbach alpha (α) values
Operational risk effect (ORE)	4	0.787
Internal fraud (IF)	4	0.881
External fraud (EF)	4	0.916
Employment practice and work place safety (EPWS)	3	0.784
Business disruption and system failure (BDSF)	4	0.887
Damage to physical asset (DPA)	2	0.965
Execution, delivery and process management (EDPM)	3	0.763
Clients, products and business practice (CPBP)	5	0.884
Total	**29**	**0.959**

Source: Own survey, 2013

Likewise, overall cronbach"s alpha for first part of the questionnaire was calculated and became 0.959 for all 29 items of the questionnaire as shown on the above table. Therefore, as per the requirement of the cronbach"s alpha to be 0.7 or greater, all items of the questionnaire are reliable and sufficient accordingly.

[16] For each factors number of items, please refer to **appendix 2**

4.3 Discussion of the study findings

The formulated questionnaire consists of demographic and basic research questions. The rationale for the inclusion of demographic questions was to determine the respondents‟ involvement and his/her experience in risk management department.

Hence, it can be concluded that their response to the questionnaire could be taken as valid due to the respondent‟s role and involvement in risk management department as about 65% of them have a service year within a range of 5-15.

The response to the questionnaire has categorized as follow, and in such a way analysis has made for each category under the next sub section.

- The analysis of correlation significance between the operational risk effect and operational risk factor (Loss events).
- The factor analysis of operational risk contributory factors.
- The analysis of banks board approval of operational risk management policies and procedures.

4.3.1 Analysis of the correlation significance between the operational risk effect and Loss events

As it has discussed under chapter three, the variables of this study are operational risk effect (dependent variable) measured on four items and the seven loss events (independent variables) likewise measured on different number of items ranging from 2-5[17]. Both variables items were coded and the median of items responses were computed and used to measure each variables.

For instance, there are four items to measure operational risk effect and to have a single value of an operational risk effect, the four items were coded as ORE_1, ORE_2, ORE_3, and ORE_4, then the median of these responses were computed and used accordingly. That is, to say for each respondent, from his/her response to ORE_1, ORE_2, ORE_3, and ORE_4 all together the median was computed for the first respondent and it continue similarly for the rest. With the same fashion, the median of all respondents‟ were computed for the each loss events.

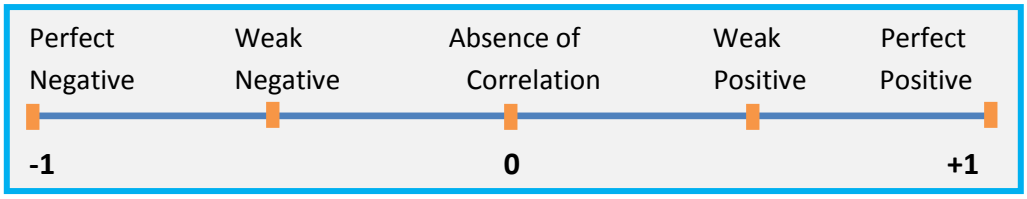
[17] For the number of items under each variable, please refer appendix 2

Here, Spearman (Rho) correlation coefficients were employed and computed to determine the strength and direction of association between the mentioned variables.

Intercorrelation[18] among the loss events (independent variables) was performed to make sure the existence of collinearity among variables. Thus, the result has shown none existence of serious multicollinearity problems.

Below, the Spearman correlation coefficient of each loss events and operational risk effect has been computed and interpreted similarly. According to Francis (2005), the Spearman correlation coefficient (r_s) can take any values on a scale from -1 to +1.

Table 3: Spearman correlation coefficient values



4.3.1.1 Operational risk effect Vs Internal fraud[19]

Table 4: Correlations between Operational risk effect and internal fraud

Correlations				
			Operational risk effect	Internal fraud
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.514****
		Sig. (2-tailed)	.	**.000**
		N	80	**80**
	Internal fraud	Correlation Coefficient	**.514****	1.000
		Sig. (2-tailed)	**.000**	.
		N	**80**	80
**. Correlation is significant at the 0.01 level (2-tailed).				

[18] Please, refer appendix 10
[19] Please, refer appendix 11a

As depicted on the table 4, there is relatively strong association between both variables having r_s = 0.514 and p-value of 0.000, which is less than 0.01. Hence, it justifies the existence of significant correlation between the two variables.

The correlation coefficient is evident as most banks worldwide lost huge amount of money or even might gone bankrupt as a result of employee dishonesty.

Thus, the management of respective banks should strive for making staffs trustable by creating conducive working environment as well as instill sense of belongingness among its staffs. Internal fraud as one of the loss events might take time to identify due to operational risk characteristics of time of occurrence, discovery and recognition variations.

Here, risk education and training come into play as an interview analysis has indicated awareness creation should start from the top (president) to the bottom (security guard) in the hierarchical level of an institution is very essential as it was underscored by the interviewees for efficient and effective ORM. In an interview analysis the interviewees (banks officers) did mention none existence of a database management system to capture and store loss events including an internal fraud. However, relatively as an internal fraud is more frequent in most of banks in Ethiopia as interview participants replied, banks need to establish a database for accurate capture and store of all loss events.

As internal fraud solely is a result of dishonesty or rogue behavior of employees which could be in the form of intentional misreporting of position, theft, insider trading on employee‟s own account and intentionally overlooked transactions, the management should seriously follow up and supervise the banking operations as there is a time gap between occurrences, discovery and recognition of such fraud.

4.3.1.2 Operational risk effect Vs External fraud.[20]

Table 5: Correlations between operational risk effect and External fraud

Correlations				
			Operational risk effect	External fraud
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.451****
		Sig. (2-tailed)	.	**.000**
		N	80	**80**
	External fraud	Correlation Coefficient	**.451****	1.000
		Sig. (2-tailed)	**.000**	.
		N	**80**	80
**. Correlation is significant at the 0.01 level (2-tailed).				

More visibly, the spearman correlation values shows there is significant correlation between the variables under consideration with $r_s = 0.451$ and p-value of 0.000. Hence, the correlation value of 0.451 means that there is relatively moderate positive association between the variables.

External fraud would also have a devastating effect on the entire bank‟s performance as the correlation coefficient has shown on the above table. It could be happens as a result of mistrust of the bank employee to engage in some sort of fraud by cooperating with an external party besides the fraud might be committed by external parties. Hence, it is strongly recommended to have good control mechanisms, which cannot create any space for fraud (internal or external).

[20] Please, refer to appendix 11b

4.3.1.3 Operational risk effect Vs EPWS[21]

Table 6: Correlations between operational risk effect and EPWS

Correlations				
			Operational risk effect	EPWS
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.240***
		Sig. (2-tailed)	.	**.032**
		N	80	**80**
	EPWS	Correlation Coefficient	**.240***	1.000
		Sig. (2-tailed)	**.032**	.
		N	**80**	80
*. Correlation is significant at the 0.05 level (2-tailed).				

The correlation coefficient between these two variable indicated on the table 6 shows weak positive correlation with $r_s = 0.240$ and p-value of 0.032.

Employment practice and work place safety (EPWS) includes workers compensation claims, violation of employee‟s health and safety rules and organized labor activities and discrimination claims. Hence, as the correlation value is an evident this loss event could have detrimental consequences on the banking operations.

[21] Please, refer to appendix 11c

4.3.1.4 Operational risk effect Vs. CPBP[22]

Table 7: Correlations between operational risk effect and CPBP

Correlations				
			Operational risk effect	CPBP
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.505****
		Sig. (2-tailed)	.	**.000**
		N	80	**80**
	CPBP	Correlation Coefficient	**.505****	1.000
		Sig. (2-tailed)	**.000**	.
		N	**80**	80
**. Correlation is significant at the 0.01 level (2-tailed).				

As the table 7 shown clients, products and business practices has also a significant association with the operational risk effect at $r_s = 0.505$ and p-value of 0.000. Hence, the correlation coefficient value is a strong evidence for the presence of moderately strong positive association between the two variables.

Clients, products and business practice (CPBP) as a loss event involves activities such as fiduciary breaches, misuse of confidential customer information, improper trade on bank‟s account and money laundering. specifically, money laundering is what challenges the traditional banking culture of confidentiality as bank account of customer could be seen by third party when a need arise under the existing rules and regulations to curb unknown and illegal source of money.

[22] Please, refer to appendix 11d

4.3.1.5 Operational risk effect Vs DPA[23]

Table 8: Correlations between operational risk effect and DPA

Correlations				
			Operational risk effect	DPA
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.364****
		Sig. (2-tailed)	.	**.001**
		N	80	**80**
	DPA	Correlation Coefficient	**.364****	1.000
		Sig. (2-tailed)	**.001**	.
		N	**80**	80
**. Correlation is significant at the 0.01 level (2-tailed).				

It‟s evident from the table 8 that, there is a weak positive association between the variables under consideration with $r_s = 0.364$ and p-value of 0.001. Here, it has shown that damage to physical asset have weak positive association with operational effect in Ethiopian commercial banking industry context.

As damage to physical asset also imposes its own risk to banking operations as the correlation coefficient value has indicated above, it is highly suggested to have safety measures to make sure its potential consequences will be mitigated. Even though the correlation coefficient above has shown a significant association between operational risk effect and damages to physical asset (DPA), an interview analysis has indicated that, in Ethiopian context DPA do not impose a big threat to the banking operations. DPA as a loss event could happen in the form of natural disaster losses and human losses from external sources.

[23] Please, refer to appendix 11e

4.3.1.6 Operational risk effect Vs BDSF[24]

Table 9: Correlations between operational risk effect and BDSF

Correlations				
			Operational risk effect	BDSF
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.545****
		Sig. (2-tailed)	.	**.000**
		N	80	**80**
	BDSF	Correlation Coefficient	**.545****	1.000
		Sig. (2-tailed)	**.000**	.
		N	**80**	80
**. Correlation is significant at the 0.01 level (2-tailed).				

It‟s visible that, there is a significant correlation present between the two variables as justified by r_s = 0.545 and p-value of 0.000. Thus, it shows there is a relatively strong positive association between the two variables.

Hence, it‟s a strong indication that business disruption and system failure (BDSF) highly affects the bank operation and eventually will lead to huge loss or might be even result into bankruptcy. Now days, a banking industry becomes technology based in order to enhances the service delivery capability and speed of the industry.

But it also imposes some level of risks unless and otherwise dealt with it prudently. As service delivery that based on the modern banking infrastructure technology sometimes gone out of service due technical problem or breakage, it should be taken in to account all possible precaution measures to have happy and satisfied customers. BDSF as a loss event could lead to operational losses due to hardware and software failures, telecommunication problems or utility outage/disruptions.

[24] Please, refer to appendix 11f

This statistical conclusion is consistent with an interview analysis which has shown that the number of customer complaint is used as one of the key risk indicator as the interviewees replied. Because, one possible reason for customers complaint could be incompetent service delivery, system failure or poor network connection which make them to wait too long for the services in need.

4.3.1.7 Operational risk effect Vs. EDPM[25]

Table 10: Correlations between operational risk effect and EDPM

Correlations				
			Operational risk effect	EDPM
Spearman's rho	Operational risk effect	Correlation Coefficient	1.000	**.357****
		Sig. (2-tailed)	.	**.001**
		N	80	**80**
	EDPM	Correlation Coefficient	**.357****	1.000
		Sig. (2-tailed)	**.001**	.
		N	**80**	80
**. Correlation is significant at the 0.01 level (2-tailed).				

Finally, the seventh loss event on the table 10 indicates the existence of moderate positive association between the execution, delivery, and process management with that of operational risk effect. Hence, the rating of operational effect has significant correlation with the rating of execution, delivery and process management at $r_s = 0.357$ and p-value of 0.001.

Execution, delivery and process management (EDPM) should be emphasized in order to mitigate the risk associated with it. It can be manifested in terms of data entry errors, collateral management, client record keeping system and legal documentation of the institution. Particularly, as interviewees were underscored failure in collateral management highly affecting the banking operations and costs it hugely. Hence, failure in these activities would lead to both monetary and non monetary losses.

[25] Please, refer to appendix 11g

4.3.2 The factor analysis of operational risk contributory factors

This sub section presents and discusses the second research question by using the principal component analysis (PCA) as factor analysis method. And the use of the principal component factor analysis for this study has been justified by two tests as indicated below. **(See table 11)**

Table 11: KMO and Bartlett's test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		**.731**
Bartlett's Test of Sphericity	Approx. Chi-Square	555.103
	df	190
	Sig.	**.000**

As shown on the above table, KMO measures the adequacy of the number of respondents considered for the analysis in order to assure the use of factor analysis method is viable.

Webster (2010) has listed the interpretation of KMO as follow:

Table 12: KMO Interpretations

KMO Value	Degree of Common Variance
0.90 to 1.00	Marvelous
0.80 to 0.89	Meritorious
0.70 to 0.79	**Middling**
0.60 to 0.69	Mediocre
0.50 to 0.59	Miserable
0.00 to 0.49	Don't Factor

Hence, KMO value in our case is **0.731** which is having a degree of common variance of "**middling**" justifies the use of factor analysis for this study. Likewise, the Bartlett"s test of sphericity determines the intercolleration matrix among factors under consideration.

A Webster (2010) state that, Bartlett"s test of sphericity calculates the determinate of the matrix of the sums of products and cross-products (S) from which the intercorrelation matrix is derived. The determinant of the matrix S is converted to chi-square statistic and tested for significance.

The null hypothesis is that the intercorrelation matrix comes from a population in which the variables are noncollinear (i.e. an identity matrix). Thus, the null hypothesis has rejected as p-value is less than 0.001 underpinning the existence of correlation among factors under consideration.

Cronbach alpha which tests the reliability in terms of internal consistency of the questionnaire has also computed and yielded **0.839** or **83.9%.** Thus, it is sufficient and internally consistent as the minimum requirement has already discussed above under reliability analysis.

The result of the factor analysis (Principal component analysis) has indicated that the 20 initial factors has been extracted and reduced to 6 factors which accounts for about 64% of total variance in operational risk management which may well be explained by those extracted factors.

Table 13 Total Variance Explained by components of operational risk contributor factors

Total Variance Explained									
Component	Initial Eigen values			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	**5.639**	28.197	28.197	5.639	28.197	28.197	4.135	20.673	20.673
2	**1.911**	9.553	37.750	1.911	9.553	37.750	2.236	11.181	31.854
3	**1.699**	8.493	46.243	1.699	8.493	46.243	2.012	10.060	41.914
4	**1.449**	7.246	53.489	1.449	7.246	53.489	1.718	8.588	50.502
5	**1.113**	5.567	59.056	1.113	5.567	59.056	1.493	7.467	57.969
6	**1.040**	5.198	64.255	1.040	5.198	**64.255**	1.257	6.285	**64.255**
7	.991	4.954	69.209						
8	.805	4.024	73.233						
9	.735	3.673	76.905						

10	.680	3.401	80.307
11	.645	3.224	83.531
12	.566	2.831	86.361
13	.522	2.611	88.972
14	.506	2.529	91.501
15	.438	2.192	93.694
16	.367	1.836	95.529
17	.290	1.448	96.978
18	.248	1.240	98.217
19	.203	1.016	99.233
20	.153	.767	100.000

Extraction Method: Principal Component Analysis.

As it has already been discussed under chapter three, each Principal component analysis has a standardized variance value = 1.0, but a factor to be a useful factor must account for more than 1.0 unit of variance, or must have an Eigen value $\lambda > 1.0$. Hence, factor having an Eigen value more than 1.0 has been considered and 6 factors have Eigen value of greater than 1.0 as it has indicated on above table. These 6 factors explain more variance or variability in operational risk management that accounts for about **64%** all together as has shown on the above table.

The level of correlation the initial 20 factors (variable) having with the extracted factors can be explained as follow by using the component matrix also known as **factor loading.**[26]

For instance, the first factor internal control and reporting system has 0.691 correlation with factor 1, -0.339 with factor 2, 0.013 with factor 3, -0.077 with factor 4, -0.309 with factor 5, and 0.125 with factor 6. For the remaining factors correlation values, **please refer appendix 7.**

[26] For the detail, please refer appendix 7

It‟s also possible to determine for how much each factor‟s variance accounted by the extracted factors. This is can be explained by using **communalities.**[27] For instance, for the first factor (variable), internal control and reporting system about **0.709** or **70.9%** variance is explained by the extracted 6 factors. To compute the variance percentage, we can use the component matrix values of each extracted factors. To compute it, sum of the squared correlation values of each factors have with the extracted factor has used as follow:

$$(0.69)^2 + (-0.339)^2 + (0.013)^2 + (-0.077)^2 + (-0.309)^2 + (0.125)^2 = \mathbf{0.709}$$

For the remaining factors variance value explained by the extracted 6 factors, **please refer to appendix 8.**

To clearly identify the **6** extracted factors which accounts for the most variance of about **64%** out of the initial 20 contributory operational factors (variables) from the component matrix has some cumbersome, but factor pattern can be rotated to indicate the extracted factors.

Webster (2010) has stated that, sometimes one or more variables may load about the same or more than one factor, making the interpretation of the factors ambiguous.

Ideally, the analyst would like to find that each variable loads high (⇒ 1.0) on one factor and approximately zero on all the others (⇒ 0.0). Sometimes the factor pattern can be clarified by "rotating" the factors in F-dimensional space[28].

Here, the rotation method used is a varimax that attempts to achieve loadings of ones and zeros in the columns of the component matrix (1.0 & 0.0). Accordingly, the rotated component matrix[29] has been used to determine the six factors extracted out of the total initial factors (variables). Then, the highest value associated with each factors has been selected in locating these factors.

[27] For the detail, please refer appendix 8
[28] Ibid.
[29] For the detail, please refer appendix 9

As it has clearly depicted on the **appendix 9**, the 6 factors extracted for the contributory operational risk factors are management supervision and follow-up, effective communication among risk management staffs including that of operational risk staffs, the accurate and on time capture of internal loss data**,** the use of external loss data, the existence of high unsuccessful or failed transactions and the use of risk scenario analysis**.**

If we put these factors in terms of their variance contribution to overall (cumulative) variance of about **64%**, **bank's management supervision and follow** up accounts for about 28%, **the use of risk scenario analysis** about 9.5%, **capturing and storing of an internal loss data** about 8.5%, **the existence of high unsuccessful or failed transactions** about 7%, **the presence of effective communication among risk management staffs including that of operational risk staffs** about 5.5% and **the use of external loss data** accounts for about 5%.

Hence, the management of respective banks would pay attention to those contributory operational risks so as to manage the operational risk effectively and efficiently. Particularly, the use of scenario analysis, capturing and storing of internal loss data, the presence of high unsuccessful or failed transactions as one of the key risk indicators and the use of external loss data represents the operational risk management tools. So, giving enough emphasis to these tools would help the respective banks to measure and manage inherent operational risk that would arise as a result of routine banking operations.

With regard to extraction of the capturing and storing of loss data up on discovery as one of the useful factors is consistent with interview result which states that, the interviewed banks are using risk incident report format as a mean of identifying and categorizing of inherent loss events. Moreover, the incident report is used in order to indicate the losses as actual (happened), near miss (attempt) and potential (future state) that helps the banks to prepare precautionary measures accordingly. Likewise, the interviewees were replied that, the banks use three lines of defense for effective operational risk management such as performers (functional units) role, risk management department role and auditors" role.

The management supervision and follow-up as one of the extracted factors is consistent with the discussion of most literatures, which strongly recommends strengthening the internal control and management quality should be emphasized in operational risk management besides other possible mechanisms. From an interview analysis, the interviewees were replied that, the banks do have operational risk management framework endorsed by NBE for application. They also added that, one of the controls and follow up mechanism in tracking of operational risk losses is via incident report format, which has indicated as operational risk matrix on **appendix 12** that lists all loss events on two dimensions, frequency and impact**.**

The extraction of the factors has also shown the role of communication among risk management staffs including that of operational risk staffs in management of the risk is very crucial. Likewise, the existence of high unsuccessful or failed transactions as one of the extracted factor represent **key risk indicator**, which is one of operational risk management tools. Hence, the key risk indicator should be given more emphasis in managing the operational risk as the analysis has shown.

Scenario analysis is also the other extracted factor which deals with future state. It‟s some sort of „what if‟ analysis of what should be done under different scenarios would in case the risk be happened under the considered scenarios. This study finding is consistent with that of Rippel and Tepy (2001) discussions, which stated, using the scenario analysis can help the financial institution to mitigate the operational risk and to decrease the impact of potential losses.

The extraction of these 6 factors is clearly an indication of the importance of the factors in operational risk management, but this does not mean the other factors (variables) are need to be neglected. Rather, the extracted factors should be given more emphasis or priority over the remaining variables so that it would be possible to deal with inherent operational risk factors that underpin the risk management process.

4.3.3. Analysis of banks board approval of operational risk management policies and procedures

This subsection presented the analysis of the third research question. Thus, the respondents‟ response is organized in the following tables and charts for clear presentation and discussion.

Table 14: Respondents' response towards banks board approval of policies and procedures of ORM

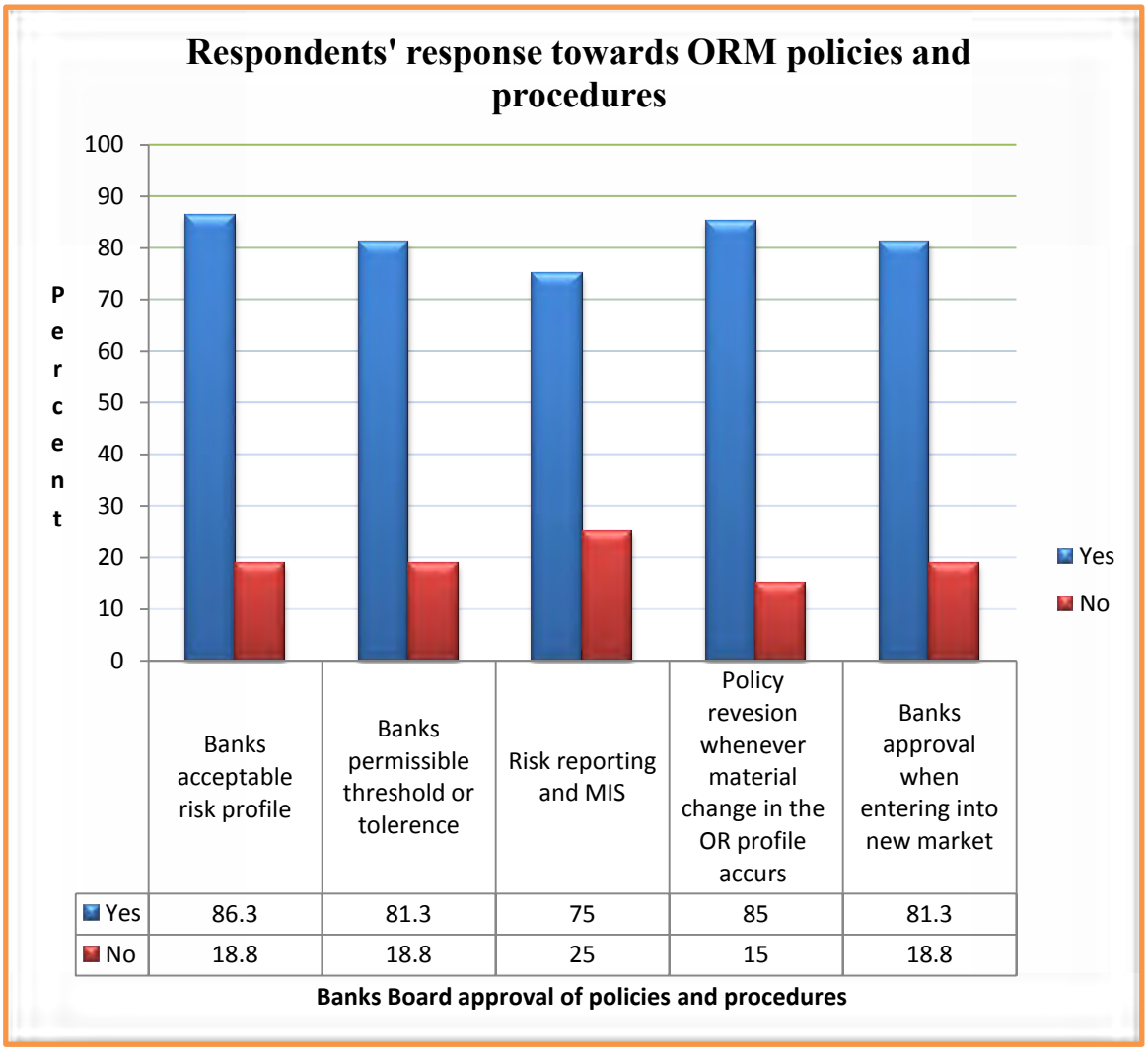
Answer "Yes" or "No"				
Does the bank have board that approves policies and procedures which defines the following:		Yes Frequency	No Frequency	Total (N)
1.	i) The bank‟s acceptable risk profile	69	11	80
2.	ii) The bank‟s permissible thresholds or tolerances for inherent and residual risks, and approved risk mitigation strategies and instruments	65	15	80
3.	iii) Risk reporting and management information system (MIS)	60	20	80
4.	iv) The policies to be revised whenever a material change in the operational risk profile of the bank occurs?	68	12	80
5.	v) Bank approval process for new products, when entering unfamiliar markets, when implementing new business processes or technology or system.	65	15	80

As it has briefly shown on the table 14, the frequency (number) of respondents to each question is presented. Accordingly, as the response provided to "Yes" option by far most outweighs the "No" option, which indicates that the respective banks under consideration do have operational risk management policies and procedures approved by their Board on the issues indicated on the above table.

It‟s obvious that having policies and procedures of operational risk management is one step forward in managing both the inherent and residual risks though it could not be taken for guarantee unless and otherwise the stakeholders are engaged in understanding and applying these policies and procedures.

More visibly, the respondents‟ response is presented on the below figure.

Figure 3: Respondents' response to banks Board's approval of ORM policies and procedures



	Banks acceptable risk profile	Banks permissible threshold or tolerence	Risk reporting and MIS	Policy revesion whenever material change in the OR profile accurs	Banks approval when entering into new market
Yes	86.3	81.3	75	85	81.3
No	18.8	18.8	25	15	18.8

With regard to the bank‟s board approval of operational risk policies and procedures responses are discussed as follow:

Having an acceptable risk profile about 86%, banks permissible threshold or tolerance for inherent and residual risk about 81%, operational risk reporting and management information system 75%, policy revision whenever material change in the operational risk profile occurs 85%, and when entering into unfamiliar business or new market about 86% had responded “yes” respectively.

Particularly, the operational risk reporting and management information system lags behind as per the response (25% responded “No”). Here, as banking services are more and more becomes technology dependent now a days, change in mind set up is required here to clearly and accurately capture the loss events as they happens. Thus, management should make sure the efficient use of management information system infrastructure which could support in quantification of loss events and could makes the prediction somehow possible.

Chapter 5: Summary, Conclusions and Recommendations

5.1 Summary of the findings

From the data interpretation and analysis made under the preceding chapter the following major findings can be summarized as follow:

- Starting from the simple demographic presentation, majority of the respondents were male (73.8%), likewise, majority of the respondents‟ **(65%)** were have a service year (tenure) within a range of 5-15, which was used as a good indication of the respondents role and involvement in risk management section considered as valid for this study.
- Since questionnaire was employed as a research instrument, the cronbach‟s alpha value of the questionnaire items were computed and became reliable and internally consistent (all items were exceeded the minimum requirement of **70%)** which justifies the reliability of the questionnaire items.
- The Spearman correlation coefficient (Rho) analysis of operational risk effect and loss events has shown the presence of significant correlation between the variables. Where, business disruption and system failure (BDSF) had shown the highest correlation coefficient **(r_s = 0.545)** and employment practice and workplace safety has yielded the lowest correlation coefficient **(r_s = 0.240)** among the others. Thus, it‟s a strong indication that business disruption and system failure highly affects the banking industry operations and will eventually lead to huge loss or might force to bankruptcy as a result.
- The use of factor analysis (principal component analysis) was justified at KMO value of **0.731** and Bartlett‟s test of sphericity (P-value = 0.000). Likewise, the cronbach‟s alpha was became **0.839**, which was sufficient to affirm the questionnaire‟s reliability. Hence, the **component matrix** of the analysis has reduced and extracted 6 factors from the initial 20 operational risk contributory factors by using principal component analysis (PCA). To clearly indicate these 6 extracted factors **rotated matrix** was performed and the extracted factors were identified.

The 6 factors extracted for the contributory operational risk factors are bank‟s management supervision and follow-up, capturing and storing of internal loss data, presence of effective communication among risk management staffs including that of operational risk staffs, the use of external loss data, the existence of high unsuccessful or failed transactions and the use of risk scenario analysis.

- The analysis of operational risk management board approval of policies and procedures of the banks has resulted into major "yes" response to all sub items of the questionnaire. However, risk reporting and management information system approval and use a little bit lags behind as about 25% of the respondents‟ were responded "no" towards it.
- Finally, the respondent‟s response is an evident for the existence of operational risk management policies and procedures in their respective banks tough it could not be taken for guarantee for the presence of efficient and effective operational risk management process.

5.2 Conclusions

From the analysis of the study findings, the following conclusions can be made.

- The demographic analysis of the study findings has shown majority of the respondents‟ (65%) were has a service year (tenure) of within a range of 5-15 years. And this has taken for guarantee that the role and involvement of the respondent in the risk management department for the validity their responses. Moreover, the respondents‟ are familiar with the subject and the risk of misinterpretation of the questionnaire might be well minimized.
- One of the objectives of the study was to determine whether there exist significant correlation between the variables of the study, operational risk effect and operational risk factors (Loss events). And the result of the analysis has showed the existence of significant correlation between the two variables as the findings has shown. The Spearman correlation coefficient (Rho) analysis has resulted into the presence of positive correlation coefficients between the variables though the degree of the strength of an association differs. Hence, the hypothesis has been accepted at level of significance (α) = 0.05.

- Even though Spearman correlation coefficient has resulted business disruption and system failure as having the highest coefficient value **(r_s = 0.545)** showing the existence of strong and positive association, the factor analysis didn‟t indicate it as among the extracted factors. Probably, it could be suspected that the introduction and using of modern banking infrastructure is a recent phenomenon and might not be seen as the major factor for the moment from the banks perspective.
- The employment practice and workplace safety yields the lowest correlation coefficient with operational risk effect (r_s = 0.240). This is an indication of presence of weak positive association between the variables.
- The principal component analysis (PCA) has resulted into reduction of the initial 20 operational risk contributory factors in to 6 extracted factors based on an Eigen value λ>1.0 as it has already mentioned. Thus, it can be deduced that these factors can account for the most variance (64%) of the operational risk management over the remainders. And, this can be a useful input for the practitioners in determining the focus area that deserves most attention than the others in their banks operational risk management process. Hence, the management should pay attention to those contributory operational risks so as to manage the operational risk effectively and efficiently, particularly, to operational risk management tools as the extracted factors has shown.
- The analysis of the interview in which the respondents‟ were underscored the importance of awareness creation and accurate on time capturing of internal loss data are in consistent with factor analysis findings of management supervision and follow-up and capturing of internal loss data as both are among the extracted factors.
- Finally, Even though it was summarized that majority of the respondents‟ were positively responded to the board approval of operational risk policies and procedures of the banks, this will not justify the efficient and prudent management of operational risk. There should be a checking mechanism (assurance) over the better application of policies and procedures through review of comprehensive risk profile of the bank, expert‟s opinion or stakeholder‟s feedback (Questionnaire).

5.3 Recommendations

Based on the study findings and conclusions, the researcher would like to forward the following recommendations, which could be useful for the study unit (Commercial Banks), as well as, to the regulatory body.

- The respective banks should pay a greater attention to the operational risk factors (Loss events) as the correlation coefficient values had explained the existence of significant correlation with the operational risk effect (monetary and/or non monetary loss) for adequate management of an inherent operational risk. These loss events might have already listed and discussed in the banking risk management policy document, but much need to be done in order to realistically realize their consequences on their routine banking operations as correlation coefficients has witnessed.
- Risk management section of the bank should give emphasis to the key risk indicators of the bank as it immensely support the operational risk management. The extraction of factor using principal component analysis has already resulted in to six useful factors, among which the existence of high unsuccessful or failed transactions is one of the key risk indicators. Thus, the researcher would like to encourage the respective banks to use key risk indicator to its utmost in operational risk management.
- As a matter of fact the main activities of the commercial bank is deposit mobilization be it public or private bank, that‟s taking a deposit from savers and providing loan to the borrowers where the type of risk they most vulnerable to it are credit, market and liquidity risks. However, only focusing to these risks will not pay off well by ignoring the operational risk unknowingly or carelessly, as it is a multiplier risk that is inevitable as long as bank continues to operate. Hence, the banks need to make sure appropriate mechanisms are on the ground for measurement and management of their inherent operational risks ultimately.

- Engaging the stakeholders at every hierarchy of the organization in order to make sure that everyone is aware of the risk associated with his/her activity, as awareness creation is at the heart of operational risk management. The awareness creation mechanisms would be in terms of providing training regularly and by disseminating information through internal magazine, brochures or leaflets to update the staffs on the new development with regard to the risk.
- Try to have a database management system, which will help the banks to record the incidents associated with operational risks timely and accurately that will be strengthen the capability of quantifying those risks, and eventually will boost the prediction capability. This suggestion is in consistent of the findings of factor analysis, in which capturing of **internal loss data** accurately and timely is one of the major factor that impacts operational risk management.
- A regulatory and supervisory body, the central bank should establish a data base management system in which the historic loss data of the peer banks will be stored and used when need arise in the measurement (quantification) of their inherent loss events.
- Above all, as most literatures have suggested the best way to manage operational risk is by strengthening the internal control and quality of management, which are essential ingredients. Thus, practitioners should make sure that the internal control mechanisms are viable from their institution‟s perspective and review it whenever necessary consequently. Likewise, management makes a difference. In other word, the way getting things done in the institution matters for the best operational risk management.

Future research ideas

Due to Ethiopian commercial banks operational risk management infancy, the researcher was unable to have large number of samples, likewise, unable to access secondary data which could have been used to determine the causal interrelationship between the study variables. Thus,

- In the future any one who would like to undertake a research similar to this topic should strive for the inclusion of the remaining banks and for the access of the data to determine the most important factors that affects banking operational risk management, that would help the practitioners to clearly identify the most critical and risk exposure areas.
- Moreover, one can undertake comparative study of Ethiopian commercial banks operational risk management with that of other contries in order to indicate the banks position in terms of effectiveness of measurement and management of the risk.

Bibliography

Bank of Pakistan (2003). „Risk management guidance for commercial banks & DFIs"

Basel committee on banking supervision (2001). „Operational risk-supervisory guidelines for the advanced measurement approach", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (2007). „Overview of the new Basel Capital Accord", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (2008). „Observed range of practice in key elements of Advanced Measurement Approaches (AMA)", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (2011). „Principles for the sound management of operational risk", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (December, 2001). „Sound Practices for the Management and Supervision of Operational Risk", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (February 2003). „Sound Practices for the Management and Supervision of Operational Risk", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (January 2001). „Operational Risk, Consultative Document", Supporting Document to the New Basel Capital Accord.

Basel Committee on Banking Supervision (July 2002). „Sound Practices for the Management and Supervision of Operational Risk", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (June 1999). „A New Capital Adequacy Framework", Consultative Paper.

Basel Committee on Banking Supervision (June 2006). „International Convergence of Capital Measurement and Capital Standards", Banks for International Settlements, Basel.

Basel Committee on Banking Supervision (September 2001). „Working Paper on the Regulatory Treatment of Operational Risk", Banks for International Settlements, Basel

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods and Practices*, 2nd ed., USA: University of South Florida.

Cagan, P. (2001). „Standard operating procedures", Erisk.com

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

de Fontnouvelle,P., DeJesus-RueffJohn,V., Jordan,J. and Rosengren,E.(2003).Using loss data to quantify operational risk. Federal Reserve, Bank of Boston.

Decoster, J. (1998). Overview of factor analysis. Retrieved on June 20, 2013 from http://www.stat- help.com/notes.html

Furrer, H. (2003). „Quantifying Regulatory Capital for Operational Risk"

Gunther, H. and Christian, W. (2005). „Determinants of Operational Risk Reporting in the Banking Industry"

Heru, S., Na (2005). Analyzing and Scaling Operational Risk Loss Data, Erasmus University Rotterdam, Netherlands. Master"s Thesis.

Kehoe, J. (1995). „Basic item analysis for multiple-choice tests: practical assessment, research and evaluation", available at: http://www.pareonline.net/getvn.asp?v = 4&n = 10 (accessed on June 25, 2013).

Khan, T. and Ahmed, H. (2003). "An analysis of issues in Islamic financial industry."

Kossowski, T. and Hauke, J. (2011). „Comparison of values of Pearson"s and spearman"s correlation coefficients on the same sets of data"

Kwasi, M., A (2010). A risk-based assessment of EcoBank Ghana limited (EGH), Master"s Thesis.

Lekatis, G. (2012). *Understanding risk management and compliance.* International Association of risk and compliance Professionals, news letter.

Machiraju, H.R (2008). *Modern Commercial banking*, 2nd ed., New Delhi: New Age International.

Manic, I. (2007). Mathematical Models for Estimation of Operational Risk and Risk Management, Master"s Thesis.

Marczyk, G., DeMatteo, D., Festinger, D. (2005). *Essentials of Research Design and Methodology*, New Jersey: John Wiley & Sons, Inc.

Mauiri, A. (2008). „Origins and early development of banking in Ethiopia"

Modiha, P. (2011). Critical evaluation of operational risk tools used in regulatory capital calculation, Gordon Institute of Business Science, University of Pretoria.

Moosa, I., A. (2007). *Operational Risk Management*. 1st ed., New York: Palgrave Macmillan.

National Bank of Ethiopia (2010). „Commercial banks risk management guidelines"

Nunnally, J.C. (1998). Psychometric Theory, McGraw-Hill, New York.

Osborne, A. (2012). *Risk management Made Easy*. Andy Osborne and Ventus Publishing Aps. ISBN 978-87-7681-984-2

Pinedo, M. (2009). Operational risk in financial services, Stern School of Business, New York University.

Power, M. (2003). „The invention of operational risk"

Raghavan, R. S. (2003). „Risk management in banks"

Reserve Bank of India (2005). „Guidance note on management of operational risk"

Ripeel, M. and Teply, P.(2011). „Operational risk-scenario analysis"

Rothbard, M. N. (2008). *The Mystery of Banking*, 2nd ed., Ludwig von mises institute, Alabama. ISBN: 978-1-933550-28-2

Samad-Khan, A. (2007). Stress testing Operational Risk. OpRisk Advisory, Washington, D.C.

Smithson, C. (2003). „Quantifying Operational Risk"

Vezi P. V. (2007). „Trends in banks operational risk losses"

Webster, G. (2010). „Factor analysis: Principal components factor analysis"

Yogieta, S., M. (2011). „Operational risk management in Indian banks: impact of ownership and size on range of practices for implementation of advanced measurement approach"

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

Zikmund, W. G., Babin, B. J., Carr, J. C. and Griffin, M. (2010): *Business Research Methods*, 8th ed., South-Western.

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

Appendix 1: List of Commercial Banks contacted for this study

Name of the bank	Category	
	Private	Public
Commercial Bank of Ethiopia		√
Construction and business bank S.C.		√
Awash International Bank S. C.	√	
Nib International Bank S. C.	√	
Wegagen Bank S.C.	√	
Oromia International Bank S. C.	√	
Lion International Bank S. C.	√	
Cooperative Bank of Oromia S.C.	√	
Bank of Abyssinia	√	
United Bank S. C.	√	
Abay Bank S. C.	√	
Dashen Bank S. C.	√	

Appendix 2: Questionnaire

Addis Ababa University
College of Business and Economics
Department of Management
MBA program

Objective of the questionnaire:

Dear, Sir/Madam

This questionnaire is prepared by Addis Ababa University graduate student to gather a data on a research topic „**Commercial Bank Operational Risk Management: Exploratory study on selected Ethiopian Commercial Banks.'** The researcher would like to thank you in advance for your kind response in allotting your precious time in filling the questionnaire. As your responses have a great impact on the study findings, you are kindly requested to provide your genuine responses freely. No need to mention your name and the information provided is to be used only for the sake of this study and will be kept confidential.

Thank you very much for your cooperation!!!

Part I. Personal information

Instructions:

Please use this √ mark for each question to indicate your response

1. Sex: Female ☐ Male ☐

2. Age: 18-29 ☐ 30-39 ☐ 40-49 ☐

50-59 ☐ 60 years and above ☐

3. Years of service (Tenure): less than 5 years ☐ 5-15 ☐ 16-25 ☐

26-40 ☐ above 40 years ☐

4. Level of education: Diploma ☐ Bachelor Degree (BA, BSc) ☐

Masters degree ☐ PhD ☐

Part II. Operational risk management items

A. Evaluation questions related to an assessment of operational risk factors (Loss events) and their effect on bank's entire operations.

1. How do you rate the effect of operational risk on your bank"s entire performance in relation to the other banking risks?

Operational risk effects:	Very insignificant	Insignificant	Moderately significant	Significant	very significant
1. Damages to bank"s physical asset.					
2. On bank"s reputation.					
3. Business interruptions.					
4. Make bank"s legally liable.					

2. Please rate how you view, in your bank"s case, the following operational risk factors significance level with each of the following statement by placing a cross/mark in the appropriate box you agree with.

Where, **1= Very insignificant, 2= Insignificant, 3= moderately significant, 4= Significant, and 5= Very significant.**

Operational risk factors (loss events):	**Alternatives:**				
Internal fraud	**1**	**2**	**3**	**4**	**5**
Intentional misreporting of position					
Employee theft					
Insider trading on an employee"s own account					
Transactions not reported (intentional)					
External fraud	**1**	**2**	**3**	**4**	**5**
Robbery					
Forgery					

Check kiting					
Damage from computer hacking and theft of information					
Employment practices and workplace safety	**1**	**2**	**3**	**4**	**5**
Workers compensation claims					
Violation of employees health and safety rules					
Organized labor activities and discrimination claims					
Clients, products and business practices	**1**	**2**	**3**	**4**	**5**
Fiduciary breaches					
Misuse of confidential customer information					
Improper trading activities on bank‟s account					
Money laundering					
Damage to physical assets	**1**	**2**	**3**	**4**	**5**
Natural disaster losses (earth quake and floods)					
Human losses from external sources (terrorism, vandalism)					
Business disruption and system failures	**1**	**2**	**3**	**4**	**5**
Hardware and software failures					
Telecommunication problems					
Utility outage /disruptions					
Execution, delivery and process management	**1**	**2**	**3**	**4**	**5**
Data entry errors					
Collateral management failures					
Legal documents missing or incomplete					
Incorrect client records (loss incurred)					
Inaccurate external report (loss incurred)					

B. Evaluation questions related to an assessment of contributory factors of operational risk.

An assessment of operational risk contributory factors.		Strongly disagree	disagree	Somewhat agree	Agree	Strongly agree
1.	Internal control and reporting system of your bank"s operational risk is strong.					
2.	The bank"s management supervision and follow up is excellent.					
3.	The bank"s staffs are aware of operational risk in their day-to-day operations.					
4.	There is a clear segregation of duties among the bank"s staffs.					
5.	There is an adequate auditing procedure.					
6.	There is an excellent recruitment procedure in your bank.					
7.	There is a conducive and supportive working environment.					
8.	There is effective communication among risk management staffs including that of operational risk staffs.					
9.	The bank"s managements are cooperative.					
10.	The bank"s systems (ICT) are reliable.					
11.	The bank has safety measures against property damages.					
12.	Operational risk training available throughout the business unit/organization.					
13.	Internal loss data are captured and recorded up on discovery.					
14.	External loss data is used in managing the bank"s operational risk.					
15.	There are high unsuccessful or failed					

	transactions.					
16.	There is high level of errors and omissions					
17.	There is high staff turnover rate.					
18.	The bank uses risk control self assessment.					
19.	An internal audit finding is used in operational risk management.					
20.	Risk Scenario analysis is used in managing the bank‟s operational risk.					

Part IV. Policy and procedural approval of operational risk
Answer "Yes" or "No"

Does the bank have board that approves policies and procedures which defines the following:		Yes	No
1.	i) The bank‟s acceptable risk profile		
2.	ii) The bank‟s permissible thresholds or tolerances for inherent and residual risks, and approved risk mitigation strategies and instruments		
3.	iii) Risk reporting and management information system (MIS)		
4.	iv) The policies to be revised whenever a material change in the operational risk profile of the bank occurs?		
5.	v) Bank approval process for new products, when entering unfamiliar markets, when implementing new business processes or technology or system.		

Finally, if you would like to comment or suggest any thing you feel about your bank‟s operational risk management in your bank‟s risk management system, please mention it.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____.

Thank you very much for your cooperation!!!

Appendix 3: Interview questions

Name: _____

Institution/organization: _____

Position: _____

Years of service (tenure): _____

1. To what extent the BOD addresses policies and procedures for management of operational risk in your bank‟s risk management system?

2. Is that operational risk is unique to your bank‟s risk management system?

3. How does the bank identify and categorize the operational risk?

4. How could you measure and manage those operational risks?

5. What are the operational risk management tools you‟re using?

6. Does your bank have reporting system of operational risk losses? If so, how often do you report to show risk profile of the bank?

7. Is there any difficulty your bank has encountered in measuring and managing of operational risk?

8. Does the bank set aside a capital to overcome the consequences of operational risk and how could you determine the amount of the capital to be kept?

9. How do you describe the emphasis given to operational risk relative to other banking risks?

10. How do you track the bank‟s operational risk losses? Do you have advanced database structure?

11. What are the mitigation tools being in use to overcome the operational risk consequences?

12. How do you express the consequences of operational risk on your bank‟s entire performance just in case it could be materialized?

13. How do you view your bank‟s operational risk exposures relative to advancement of bank‟s information technology infrastructure?

14. What can you say in general about your bank‟s operational risk measurement and management practices?

Thank You Very Much for your cooperation!!!

Appendix 4: Mapping of Business lines

Level 1	Level 2	Activity Groups
Corporate Finance	Corporate Finance	Mergers and acquisitions, underwriting, privatizations, securitization, research, debt (government, high yield), equity, syndications, IPO, secondary private placements
	Municipal/Government Finance	
	Merchant Banking	
	Advisory Services	
Trading and sales	Sales	Fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
	Market Making	
	Proprietary Positions	
	Treasury	
Retail banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
	Private Banking	Private lending and deposits, banking services, trust and estates, investment advice
	Card Services	Merchant/commercial/corporate cards, private labels and retail
Commercial	Banking Commercial Banking Project finance, real estate, export finance, trade finance,	factoring, leasing, lending, guarantees, bills of exchange
Payment and Settlement	External Clients	Payments and collections, funds transfer, clearing and settlement
Agency Services	Custody	Escrow, depository receipts, securities lending (customers) corporate actions
	Corporate Agency	Issuer and paying agents
	Corporate Trust	
Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
Retail Brokerage	Retail Brokerage	Execution and full service

Appendix 5: Detailed Loss events classification

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party	Unauthorized Activity	Transactions not reported (intentional) Transaction type unauthorized (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion (willful) Bribes / kickbacks Insider trading (not on firm‟s account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from	Employee Relations	Compensation, benefit, termination issues Organized labor activity
		Safe Environment	General liability

	diversity / discrimination events		(slips and falls, etc.) Employee health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm"s account) Unlicensed activity Money laundering
		Product Flaws	Product defects (unauthorized, etc.) Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural	Disasters and other events	Natural disaster losses Human losses from

	disaster or other events.		external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage / disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model / system misoperation Accounting error / entity attribution error Other task misperformance Delivery failure Collateral management failure Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade	Non-client

		Counterparties	counterparty misperformance Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing Vendor disputes

Appendix 6: Sound Practices for the Management and Supervision of Operational Risk

A. *Developing an Appropriate Risk Management Environment*

Principle 1: The board of directors should be aware of the major aspects of the bank„s operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank„s operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Principle 2: The board of directors should ensure that the bank„s operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organization, and all levels of staff should understand their responsibilities with respect to operational risk management.

Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank„s material products, activities, processes and systems.

B. *Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control*

Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

C. *Role of Supervisors*

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank,s policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

D. *Role of Disclosure*

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

Source: Basel Committee on Banking Supervision (February, 2003)

Appendix 7: Component matrix: the level of correlation of contributory factors of operational risk with the extracted factors

Component Matrix[a]						
	Component					
	1	2	3	4	5	6
Internal control and reporting system	.691	-.339	.013	-.077	-.309	.125
management supervision and follow up	.701	-.341	.211	-.126	-.131	-.089
staffs are aware of operational risk in their day-to-day operations	.706	-.129	.055	.024	-.024	-.217
segregation of duties among the bank‟s staffs	.649	-.190	.145	.221	-.030	-.168
adequate auditing procedure	.584	-.063	-.280	.397	-.084	.115
recruitment procedure	.500	-.029	-.254	.182	.331	.164
conducive and supportive working environment	.635	-.027	.078	-.114	.426	.203
effective communication among risk management staffs including that of operational risk staffs	.428	.180	.240	-.671	-.182	.052
managements are cooperative	.570	-.311	.405	-.221	.000	.234
systems (ICT) are reliable	.617	.048	.136	.157	-.257	-.127
safety measures against property damages	.677	-.085	-.078	-.097	.019	-.072

risk training available throughout the business unit/organization	.507	-.025	.306	.311	.437	-.293
Internal loss data	.448	.238	-.194	-.091	.412	.329
External loss data	.235	-.082	-.014	.509	-.272	.556
high unsuccessful or failed transactions	-.160	.443	.617	.427	-.096	.076
high level of errors and omissions	.014	.403	.697	.063	.134	-.066
high staff turnover rate	.281	.632	-.053	-.196	.029	.315
risk control self assessment	.498	.270	-.374	.014	.124	-.351
internal audit finding	.606	.567	-.112	-.137	-.237	-.017
Risk Scenario analysis	.420	.516	-.284	.180	-.260	-.210
Extraction Method: Principal Component Analysis.						
a. 6 components extracted.						

Appendix 8: Communalities: the operational risk contributory variance explained by extracted factors

Communalities		
	Initial	Extraction
Internal control and reporting system	1.000	.709
management supervision and follow up	1.000	.692
staffs are aware of operational risk in their day-to-day operations	1.000	.566
segregation of duties among the bank‟s staffs	1.000	.556
adequate auditing procedure	1.000	.602
recruitment procedure	1.000	.485
conducive and supportive working environment	1.000	.645
effective communication among risk management staffs including that of operational risk staffs	1.000	.760
managements are cooperative	1.000	.689
systems (ICT) are reliable	1.000	.508
safety measures against property damages	1.000	.486
risk training available throughout the business unit/organization	1.000	.725
Internal loss data	1.000	.582
External loss data	1.000	.705
high unsuccessful or failed transactions	1.000	.800
high level of errors and omissions	1.000	.675
high staff turnover rate	1.000	.619
risk control self assessment	1.000	.600
internal audit finding	1.000	.777
Risk Scenario analysis	1.000	.668
Extraction Method: Principal Component Analysis.		

Appendix 9: Rotated component matrix of operational risk contributory factors

Rotated Component Matrix						
	Component					
	1	2	3	4	5	6
Internal control and reporting system	.729	.060	.056	-.236	.200	.273
management supervision and follow up	**.817**	.004	.082	-.066	.119	.005
staffs are aware of operational risk in their day-to-day operations	.681	.259	.179	-.025	-.032	-.041
segregation of duties among the bank‟s staffs	.678	.180	.141	.079	-.172	.094
adequate auditing procedure	.379	.358	.272	-.161	-.196	.438
recruitment procedure	.226	.170	.579	-.141	-.148	.165
conducive and supportive working environment	.421	-.013	.670	.043	.128	-.028
effective communication among risk management staffs including operational risk	.372	.081	.055	.038	**.742**	-.244
managements are cooperative	.673	-.285	.220	.086	.302	.087
systems (ICT) are reliable	.577	.356	.005	.139	.043	.166
safety measures against property damages	.560	.244	.286	-.148	.095	-.019

risk training available throughout the business unit/organization	.485	.107	.392	.381	-.385	-.178
Internal loss data	.043	.162	**.715**	-.043	.190	.068
External loss data	.134	-.001	.089	.052	-.050	**.821**
high unsuccessful or failed transactions	-.136	.039	-.160	**.837**	-.033	.232
high level of errors and omissions	.043	-.028	.024	.796	.127	-.151
high staff turnover rate	-.145	.377	.374	.189	.519	.104
risk control self assessment	.204	.632	.291	-.153	-.089	-.208
internal audit finding	.237	.693	.184	.098	.440	.064
Risk Scenario analysis	.095	**.800**	.032	.042	.059	.113
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.						

Appendix 10: Intercorrelation among loss events (operational risk factors)

Correlations								
			Internal fraud	External fraud	EPWS	BDSF	DPA	EDPM	CPBP
Spearman's rho	Internal fraud	Correlation Coefficient	1.000						
		Sig. (2-tailed)	.						
		N	80						
	External fraud	Correlation Coefficient	.823**	1.000					
		Sig. (2-tailed)	.000	.					
		N	80	80					
	EPWS	Correlation Coefficient	.449**	.385**	1.000				
		Sig. (2-tailed)	.000	.000	.				
		N	80	80	80				
	BDSF	Correlation Coefficient	.731**	.755**	.377**	1.000			
		Sig. (2-tailed)	.000	.000	.001	.			
		N	80	80	80	80			
	DPA	Correlation Coefficient	.600**	.594**	.409**	.549**	1.000		
		Sig. (2-tailed)	.000	.000	.000	.000	.		
		N	80	80	80	80	80		
	EDPM	Correlation Coefficient	.290**	.358**	.126	.389**	.132	1.000	

		Sig. (2-tailed)	.009	.001	.265	.000	.244	.	
		N	80	80	80	80	80	80	
	CPBP	Correlation Coefficient	.657**	.712**	.354**	.692**	.574**	.337**	1.000
		Sig. (2-tailed)	.000	.000	.001	.000	.000	.002	.
		N	80	80	80	80	80	80	80
**. Correlation is significant at the 0.01 level (2-tailed).									

Appendix 11a: The cross tabulation of Operational risk effect by Internal fraud

Operational risk effect * Internal fraud Cross tabulation							
Count							
		Internal fraud					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	4	5	1	0	1	11
	Moderately significant	3	6	4	1	0	14
	Significant	1	12	16	8	4	41
	Very significant	0	2	3	5	4	14
Total		8	25	24	14	9	80

Appendix 11b: The cross tabulation of Operational risk by External fraud

Operational risk effect * External fraud Cross tabulation							
Count							
		External fraud					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	4	4	1	0	2	11
	Moderately significant	2	7	3	1	1	14
	Significant	2	8	13	10	8	41
	Very significant	0	2	2	4	6	14
Total		8	21	19	15	17	80

Appendix 11c: The cross tabulation of Operational risk by employment practice and work place safety

Operational risk effect * EPWS Cross tabulation							
Count							
		EPWS					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	4	5	0	1	1	11
	Moderately significant	4	5	5	0	0	14
	Significant	6	23	9	1	2	41
	Very significant	1	5	6	1	1	14
Total		15	38	20	3	4	80

Appendix 11d: The cross tabulation of Operational risk by clients, products and business practice

Operational risk effect * CPBP Cross tabulation							
Count							
		CPBP					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	3	6	1	0	1	11
	Moderately significant	1	5	7	0	1	14
	Significant	3	5	21	10	2	41
	Very significant	0	1	3	8	2	14
Total		7	17	32	18	6	80

Appendix 11e: The cross tabulation of Operational risk by damage to physical asset

Operational risk effect * DPA Cross tabulation							
Count							
		DPA					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	9	0	1	0	1	11
	Moderately significant	10	2	1	0	1	14
	Significant	26	5	7	1	2	41
	Very significant	3	2	2	2	5	14
Total		48	9	11	3	9	80

Appendix 11f: The cross tabulation of Operational risk by business disruption and system failure

Operational risk effect * BDSF Cross tabulation							
Count							
		BDSF					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	4	5	1	0	1	11
	Moderately significant	5	3	5	0	1	14
	Significant	2	6	20	10	3	41
	Very significant	0	2	1	7	4	14
Total		11	16	27	17	9	80

Appendix 11g: The cross tabulation of Operational risk by execution, delivery and process management

Operational risk effect * EDPM Cross tabulation							
Count							
		EDPM					Total
		Very insignificant	Insignificant	Moderately significant	Significant	Very significant	
Operational risk effect	Insignificant	1	3	3	4	0	11
	Moderately significant	0	1	4	8	1	14
	Significant	1	1	3	24	12	41
	Very significant	0	0	4	5	5	14
Total		2	5	14	41	18	80

Appendix 12: Operational risk matrix

Metrics of annual loss from operational risk									
		Fraud		FE	DA	SF	HR	OR	Total
		IF	EF						
Credit	Frequency								
	Impact (in „000 Br.)								
Domestic banking	Frequency								
	Impact (in „000 Br.)								
IBD	Frequency								
	Impact (in „000 Br.)								
Accounts & Fin.	Frequency								
	Impact (in „000 Br.)								
Admin. & Gen. Ser.	Frequency								
	Impact (in „000 Br.)								
Total	Frequency								
	Impact (in „000 Br.)								

Key: IF= Internal fraud; EF= External Fraud; FE= Failure in execution, delivery and/or processing; DA= Damage to physical asset; SF= System Failure; HR= Problem related to human resource management; OR= other loss events (Like losses from client initiated legal actions, fines for breaching regulations, and vendor related disputes).