KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY, KUMASI

COLLEGE OF ART AND SOCIAL SCIENCES

SCHOOL OF BUSINESS

OPERATIONAL RISK MANAGEMENT IN THE GHANAIAN BANKING ENVIRONMENT

BY

ERZUAH AHMED SIAM

MAY, 2009

OPERATIONAL RISK MANAGEMENT IN THE GHANAIAN BANKING ENVIRONMENT

by

Erzuah A. Siam

Bachelor of Arts (Hons.)

A Thesis submitted to the Department of Accounting and Finance,

Kwame Nkrumah University of Science and Technology

in partial fulfilment of the requirements for the degree

of

MASTER OF BUSINESS ADMINISTRATION

School of Business

College of Art and Social Sciences

May, 2009

DECLARATION

I hereby declare that this submission is my own work towards the MBA and that, to the best of my knowledge, it contains no material previously published by another person nor material which has been accepted for the award of any other degree of the University, except where due acknowledgement has been made in the text.

Erzuah Ahmed Siam 16/10/09

Student ID: 20065451 Signature Date

Certified by:

Kingsley Appiah (Mr.) ..... 16/10/09.

Supervisor Signature Date

Certified by:

Joseph M. Frimpong (Mr.) 19-10-09

Head of Department Signature Date

ACKNOWLEDGEMENT

I am grateful to and thank sincerely the following persons for their assistance in completing this work.

First and foremost, my sincere gratitude goes to the Almighty God for seeing me through this work.

Again, I would like to take the opportunity to express my appreciation to my supervisor, Mr. Kingsley Appiah for his help and guidance throughout the process of this work.

I also thank sincerely, all the staff of the various banks for their support and willingness to share their experience on this subject with me, they are highly appreciated.

I cannot forget my family and all my friends who contributed in diverse ways throughout this study, may the Almighty God adequately bless you all.

E.A.S

ABSTRACT

In the past, the banking industry thought measuring and managing operational risk was something akin to mission impossible. Consequently, some banks defined operational risk as a non-measurable risk. The last few years has changed that mindset dramatically, to the point where discussions on measuring and managing operational risk now are actually considered to be trendy. Such a reversal of fortune is due, in part, to recent developments within the Basel Committee on Banking Supervision and its decision to allocate regulatory capital for operational risk. This work assesses in detail the status of operational risk management in the Ghanaian banking environment. The study identified operational risk as one of the primary risk types, with its primary risk factors identified as people, processes, systems and external events. Several exposures were identified with each of the aforementioned operational risk factors that contribute to the incidence of operational losses. However risk is still being regarded as an overall responsibility, rather than consisting of specialized areas as most banks are still in the process of demarcating the area of operational risk. Given the close linkage of operational risk with other risk types, as identified in the study, it is very important for banks to first have a clear understanding of the concept of operational risk before designing the operational risk measurement and management framework. The study underscores the need to devote more time and resources if banks desire to efficiently deal with the management of operational risk.

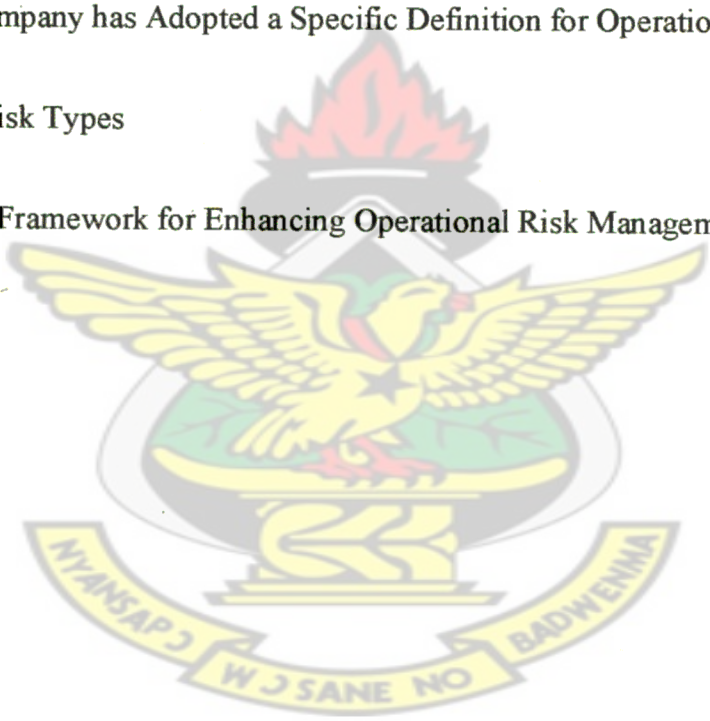
LIST OF ABBREVIATIONS

AAL	Annual Average Loss
AIRMIC	Association of Insurance and Risk managers
ALE	Annual Loss Expectancy
AMA	Advanced Measurement Approach
AMD	Advanced Micro Devices
BCBS	Basel Committee on Banking Supervision
BIA	Basic Indicator Approach
CAPM	Capital Asset Pricing Model
COSO	Committee of Sponsoring Organisations of the Tread way
CRO	Chief Risk Officer
EML	Estimated Maximum Loss
ERM	Enterprise Risk Management
FMAC	Financial and Management Accounting Committee
IRM	Institute of Risk Management.
KRI	Key Risks Indicators
LRAM	Livermore risk analysis methodology
ORM	Operational Risk Management
PERT	Programme Evaluation and Review Technique
PwC	Pricewaterhouse Coopers
SPSS	Statistical Package for the Social Sciences
TSA	The Standardised Approach

TABLE OF CONTENTS **PAGE**

LIST OF TABLES **PAGE**

LIST OF FIGURES **PAGE**



CHAPTER ONE

RESEARCH INTRODUCTION AND CONTENT

1.1 Background to the Research

Operational risk has been around since business began. Although by itself not a new concept, it has by far not received the same amount of attention as other risks (such as credit and market risk) until recent years. The business environment today, evidently, is a more than complex one. Businesses have to live with uncertainties in every aspect of their operations.

According to Hillson et al (2005), cited in Pitinanondha (2008), there is an increasing interest in improving organisational ability to deal with those uncertainties. Geiger (2000), however argues that risk is not understood merely as "uncertainty about the future" or the "probability of sustaining a loss" but as "an expression of the danger that the effective future outcome will deviate from the expected or planned outcome in a negative way.

One of the distinguishing characteristics of the Basel II Framework from Basel I is its separate recognition and explicit measurement of operational risk - although regulators have had longstanding prudential requirements covering operational risk issues such as outsourcing and business continuity management (Lebransky 2008).

Operational risk, according to the Basel Committee (2004) cited in Young (2001), 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," It typically covers a broad range of risks that are internal to an organisation (Corrigan 1998). Frame (2003), cited in Pitinanondha (2008), argues that operational risk is different from other types of risks as it deals with established processes rather than managing unknown circumstances.

Undoubtedly, an organisation's internal processes, people and systems periodically fail. Sometimes, external events can dramatically impact a firm's operations. Usually these failures result in losses or diminished business performances that are dire. Operational risk management (ORM) is a specialty within Enterprise Risk Management (ERM) that seeks to identify, monitor, measure and manage the risk of loss from such operational events.

1.1.1 Operational Risk and Financial Institutions

Financial institutions worldwide began to recognise operational risk in the 1990s, thus making it a recent phenomenon in the context of banking and financial institutions. According to Janakiraman (2008), heightened regulatory interest in operational risk, particularly since the late 1990s, after a series of high profile incidents and losses (Barings, Allied Irish, Daiwa and others) finally culminated in an overt treatment of operational risk under the Basel Accord (2004). He argues that, the Basel Committee's interest in making the New Basel Capital Accord more risk sensitive and the realization that risks other than credit and market could be substantial, led to the explicit recognition of operational risk in the capital adequacy framework.

The increasing complexity of banking activities has been responsible for the growing Operational risk events. Major changes in financial markets, increasing globalization and deregulation, among other factors largely impacted on the enormity and character of operational risks that confronted banks.

As pointed out by an AMD White Paper (2007), financial regulators have long been concerned about the risk of operational losses from failed or inadequate internal processes, people or systems or from external events. As a result, it claims that, with the recent Basel II capital accords, international regulators have for the first time imposed explicit capital charges for operational risk. The argument the paper raises is that this has raised the more embryonic practice of operational risk management up to the level of peer with the more developed disciplines of credit and market risk management.

1.1.2 Operational Risk Management Implementation Systems

The need for an effective Operational Risk Management has led to the development of certain standards and guidelines that informs organisations on effective practices. These are generally international standards and guidelines that are adopted across the business world. According to Pitinanondha (2008), some standards and guidelines have been developed to address ORM in the broadest sense dealing with all types of risks in operations while others have more explicit guidelines to manage certain specific risks.

Table 1.0 (presented in appendix 2), adopted from Pitinanondha (2008) shows certain national and international standards.

1.2 Problem Statement

Concern over operational risk has grown during the past few years, fueled by a variety of factors. These include the use of more highly automated technology; large-scale mergers and acquisitions that test the viability of newly integrated systems; the emergence of banks as very large-volume service providers; and the increased prevalence of outsourcing and the greater use of financing techniques that reduce credit and market risk, but enhance operational risk.

The main part of Basel II, the capital requirement regulations, is aimed at increasing the global financial stability. The current recognition given to it has largely enhanced the management of operational risk, but not without difficulty and inconsistencies. Scarcity of data and measuring techniques, the limitations of holding capital against such risks, and issues of internal controls and market discipline for managing operational risks are major issues the financial industry is still grappling with.

It is hard to predict exactly when these losses will occur, but it is even more important to have an efficient system in place to be able to appropriately mitigate. Research is therefore necessary to explore and analyse the external and internal factors and their impact on operational risk management, and understand the operational risk management systems and processes in the Ghanaian banking environment, to effectively enhance its development, in the light of consistent efforts by the Basel Committee and all other regulatory bodies in the case of Ghana, the Bank of Ghana, to assist financial institutions take proactive measures.

1.3 Research Objectives

This long essay seeks to explain operational risk management systems and practices in the Ghanaian banking environment. The objectives are to:

1. Identify the operational risks inherent in all material products, activities, processes and systems and the banks' vulnerability to these risks (achieved on pages 45-51)

2. Find out the extent of the financial institutions' operational risk exposure (achieved on pages 45-51)

3. Identify operational risk management methodologies, tools and techniques employed by banks in Ghana in dealing with operational risk (achieved on pages 52-57)

4. Identify the level of banks' awareness and adoption of the Basel II framework on operational risk management (achieved on page 57)

1.4 Research Questions

On the basis of the research objectives, the following research questions have been formulated:

RQ 1. What are the operational risks inherent in the banking process?

RQ 2. What is the extent of the financial institutions' operational risk exposure?

RQ 3. What tools and methodologies are being used in dealing with the issue of operational risk?

1.5 Limitation

Due to resource constraints available to the researcher, the effort to obtain the needed insight that would enhance a better understanding to contribute effectively to the management of operational risk was a bit hampered, considering the difficulty in dealing with the issue of operational risk identification. Again, access to some of the banks emerged as a difficult point in the study.

1.6 Justification of the Study

The irony is that, while regulators and institutions' major focus in the financial services sector over recent years has been on developing models for measuring and managing credit risk, most of the large losses in financial institutions over this time have been sourced to operational risk - and more specifically, the actions of single individuals, or small associates of individuals.

The research area will contribute to risk management in the area of operational risks of banks in Ghana. Risk has always been present in banking and, indeed, according to Moody's Investor Service (2003), the raison-d'être of the financial services sector is the commercial transfer of risk to those better able to accept it. However, the increasing rate of change and the level of sophistication have resulted in the need for more responsive approaches to risk management. As argued by Moody's (2003), the assessment of operational risk is becoming increasingly central to the fundamental analysis of a rated bank. This essentially is

to improve and enhance the competitive position of the bank and facilitating its long-term survival.

The Ghanaian economy is not immune to the effects of the global crisis, even though the impact has been relatively less. By identifying and proactively addressing risks and opportunities, banks protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

1.7 Scope of Study

The study looks at operational risk management procedures and processes used by banks in Ghana. This is in the light of approaches to managing these risks put forward by the Basel Committee (Basel II), and currently being used by some advanced countries. The study aims at contributing to an enhanced operational risk management in the Ghanaian banking environment.

1.8 Organisation of the Study

This study is structured into five (5) chapters. Chapter one introduces the background and motivation in the conduct of this research project. It outlines the objectives and scope of the project.

Chapter Two of the study, being the Literature Review, explores existing literature in the area of operational Risk identification and management in order to gain an understanding of the research topic. It also looks at operational risk

assessment models, processes, methodologies, tools and techniques involved in risk assessment and management.

Chapter Three, which is the research methodology, defines the research process employed to accomplish the aim and objectives of the project. It describes the procedures and techniques adopted with activities involved in each stage of the research.

Chapter Four of the research deals with the interpretation of the empirical research results quantitatively and qualitatively. The analysis also compares findings to theories and concepts identified during the review of literature.

Chapter five, which finally concludes the research, summarises all the discussions within the research. The chapter also highlights important issues that emerged from the study, as well as makes recommendations for future work to be carried out.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Chapter two introduces the theories that are pertinent to the purpose of this long essay, largely risk types, operational risk definitions, types, causes, effects, measurement approaches etc.

Risks are usually defined by the adverse impact on profitability of several distinct sources of uncertainty. The types and degree of risks an organisation may be exposed to, depend upon a number of factors such as its size, complexity, business activities, volume etc.

All organisations perform processes either in the form of a project or operations. There is a general acknowledgement that risk cannot be discussed without mentioning project or operations management. This is because risk does not exist alone but is found within projects and business operations. Archer (2002) observed that "the successful operation of any business depends on risk management."

Financial firms, as pointed out by an AMD whitepaper (2007) deal with very large amounts of money, most often electronically. Instructions are incessantly sent to execute a particular payment, loan, insurance, security, derivative or financing transaction. Over time, significant policies, procedures, systems and controls have been instituted to help ensure that operations are carried out as

expected. It continues that, 'With very high regularity, this is indeed the case. However, when the processes, people or systems fail, the losses to a financial institution can be quite significant'.

2.2 Risk

The general understanding of the term risk is "the possibility of suffering from harm or loss or exposure to this" (Carter et al., 1994). This is corroborated by Frost et al., (2001) who claim that risks are uncertain future events which could influence the achievement of an organisation's objectives, including strategies, operational, financial and compliance objectives". Knechel (2002) defined it as "the likelihood that outcome from a process will not meet expectations." As Jallow (2006) puts it, others also defined it by considering risk and uncertainty in projects and business processes. Knight (1981) distinguished between risk and uncertainty according to economist and decision theorist ideologies as:

Risks: "those for which the probability of occurrence can be calculated either on a rational, or priori basis, or on the basis of the statistical analysis of a number of similar events that have occurred in the past."

Uncertainties: "those for which analysis is impossible by virtue of the fact that they are either a 'one-off' event or because their occurrence does not follow an apparent pattern of events."

Regardless of the difference between these two concepts as pointed above, Raftery (1994) cited in Jallow (2006) argued that "Risk and uncertainty

characterize situations where the actual outcome for a particular event or activity is likely to deviate from the estimated or forecast value." Implying that any uncertainty of how a particular business process will be executed can be termed as a risk to the business operations. He depicts risk and uncertainty as being at either end of the continuum as shown in Fig: 2.1

The risks-uncertainty continuum

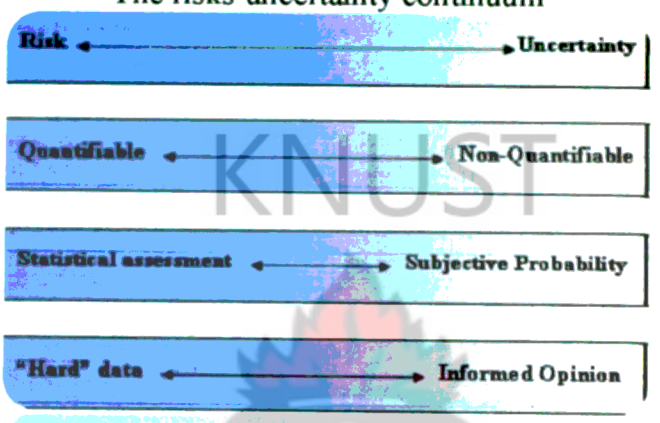


Fig: 2.1. Adapted from: Raftery (1994)

As Jallow (2006) further indicates, risk has factors or attributes attached to it. These he identifies as:

Impact: being the consequence of the event happening within the project or business operations, and

Probability: being the relative chance that the event will occur over time during the project or operations of the business.

On this basis, Link et al., (2004) cited in Jallow, defined risk mathematically as "the impact multiplied by the probability of occurrence" - Risk = (impact x probability).

Risk management in any organisation is a critical requirement for success. Its importance is evidently emphasized in modern banking environments. The Basel Committee provides examples of possible risks a bank may face as listed below:

- **Market/price risk**: described as the risk of a decrease in the value of a financial portfolio as a result of adverse movements in market variables such as prices, currency exchange rates and interest rates.
- **Credit risk**: described as the risk that a counterparty to a financial transaction will fail to perform according to the terms and conditions of the contract.
- **Country risk**: described as measured credit and market risk exposures, both cross-border and local currency denominated. A bank is exposed to this risk through transactions with counterparties in foreign countries.
- **Liquidity risk**: described as the risk that a bank will be unable to meet its funding requirements, and that the ultimate responsibility for setting liquidity policies and reviewing liquidity decisions lies at the bank's highest level of management.
- **Interest-rate risk**: described as the risk that a bank's earnings, expenses and the economic value of its assets will be affected as a result of fluctuations in interest rates. It is by nature a speculative type of financial risk since interest rate movements can result in profits or losses.
- **Legal risk**: described as the risk to earnings or capital arising from violations or non-conformance with laws, rules, regulations, prescribed policies or ethical standards.

- **Reputation risk**: described as the potential that a negative publicity about a bank's business practice or internal controls, whether true or not, will cause a decline in customer base, reduced revenue, or reduced liquidity.
- **Operational risk**: described as the risk of loss occurring as a result of inadequate systems and control, human error, or management failure.

2.3 Operational Risk

A major event which resulted in an increased focus on operational risk was the Barings Bank saga during 1995. Many authors and reporters argued that ineffective operational risk management caused the fall of Barings Bank. Freeman (1999:58) also states that the collapse of Barings Bank led many competitors to question their own vulnerability to an operational failure.

2.4 Definition

Operational Risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk," [Basel Committee (2004)]. The definition is a causative one, inasmuch as it talks about the causes of operational risk-- people, policies, procedures and systems and external events. It further suggests that Operational Risk may materialise directly, as in the case of say, wire transfer (transfer of funds to the wrong person) or could result indirectly as a credit or market loss. For example, in the Barings case, operational risk events (fraud, lack of demarcation of responsibilities and inadequate oversight of dealer's activities) resulted in a market loss.

Buchelt and Unteregger (2004) contend that whether or not a loss event is to be classified as an operational loss event is determined by the causes rather than the consequences of the event. Moosa (2007) argues that the factor between pure market and credit losses and those linked to operational risk must be the cause. Moosa (2007) arguing that distinction should be made between the cause and the factor driving severity, states that the cause of the Barings disaster was an operational loss event but movements in the market aggravated the severity of the loss.

Morgan and Anderson (1997:48) cited in Young (2001) state that operational risk is the uncertainty related to losses resulting from inadequate systems or controls, human error, or management failure. Chew (1996:299) points out that it is the unexpected losses arising from deficiencies in management information, support and control system. Smith (1997:322), cited in Young (2001), corroborated this and further stated that an objective of operational risk management should be to recognize these factors and to address it to mitigate its adverse effects.

The Chase/Risk magazine (1996:48), cited in Young (2001), defines operational risk as the risk run by a firm where its internal practices, policies and systems are not rigorous or sophisticated enough to cope with adverse market conditions, human or technological errors. Kingsley et al. (1998:1), cited in Young (2001), corroborate this and state that operational risk is the risk of loss caused by failures in operational processes or the systems that support them, including those adversely affecting reputation, legal enforcement of contracts and claims.

Venkat (2000:587) looks at operational risk from a firm-wide risk management framework and define it as the risk of loss resulting from human acts (intentional and unintentional), technology failure, and breakdown in internal controls, disaster, or the impact of external factors. Freeman (1999:58) contends that although many firms choose to define operational risk as "everything else", there has been significant progress in getting to grips with defining its scope and possible impact. He argues that the wider the definition of operational risk adopted by a firm, the more vulnerable it is to a loss of business.

Goldman et al. (1998:37) explain that operational risk covers a broad range of risks that are internal to the firm, and has in the past received rather less attention than other aspects of risk Alexander (2000:1) states that operational risks include many different types of risk, from the simple "operations" risks of processing transactions, unauthorized activities, and system risks, to other types of risk that are not included in credit or market risk, such as human risk, legal risk, information risk and reputation risk. Crouhy et al (2000:344) state that operational risk is associated with operating the business and can be divided into:

Operational failure risk: arises from the potential for failure in the course of operating the business.

Operational strategic risk: arises from environmental factors, such as new competitor that changes the business paradigm, a major political and regulatory regime change, earthquakes and other factors that are generally outside the control of the organisation.

Two Broad Categories of Operational Risk

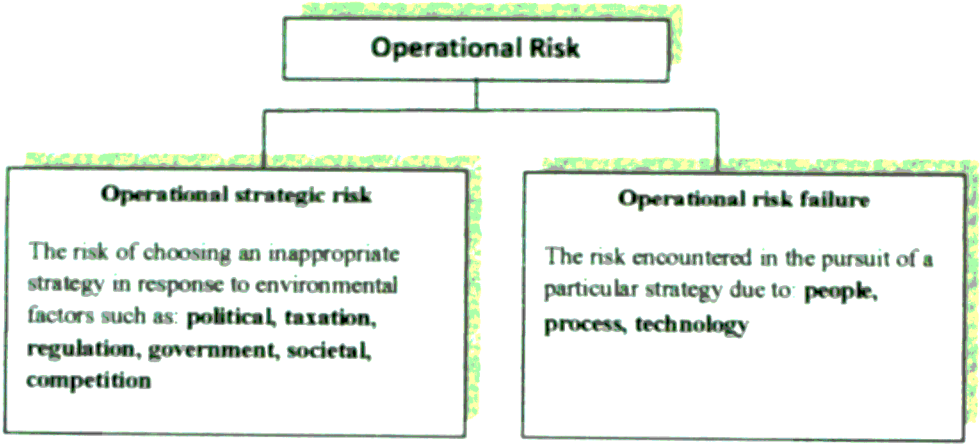


Fig: 2.3.1 Source: Crouhy & Mark (2000:345)

2.5 Identifying Operational Risk

Risk identification is the process of establishing which risks are likely to erupt from the project or business operations. It is important to acknowledge that risk is found everywhere and that "every project has risk" (Kendrick, 2003). Some of these risks may be internally caused but there are external drivers that could force risks into projects and operations. The quality of risk information generated in risk identification determines how well the results or outcomes of the quantification will be.

As Williams (2000:17) points out, determining operational risk depends on a particular firm. She contends that "The key thing is that firms really need an internal definition of operational risk. She emphasizes that risk identification, as the first step of a risk management process, provides an important foundation for the firm to rely on in the future. Furthermore, if there is not a clear understanding of what operational risk means to the individual business units and the corporation

as a whole, the ability to build any technology systems for the measurement and management of the risks will not be possible.

Identifying Key Risks Indicators (KRIs) and performing risk mapping of processes and activities according to Jallow (2006), is a good way of performing risk assessment of business processes. "KRI is an operational or financial variable that provides a reliable basis for estimating the likelihood and the severity of one or more operational risk events" (Scandizzo, 2005).

Likelihood/Severity Risk Map /Grid

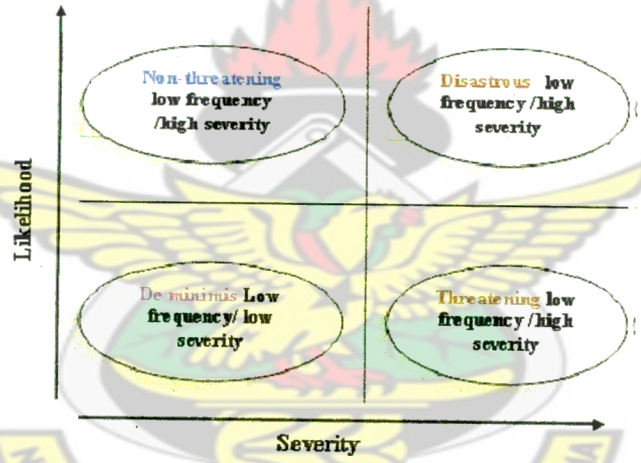


FIG: 2.4.1 Adapted from: Scandizzo (2005)

Risk mapping is a starting point for identification and management of different business process risk factors. It will help risk analysts understand the different resources used within a business processes and activities, the risk drivers as well as the consequences of the risk occurring (as presented in fig 2.4.2). It is of great benefit when doing risk analysis and management.

Objective of Risk Mapping

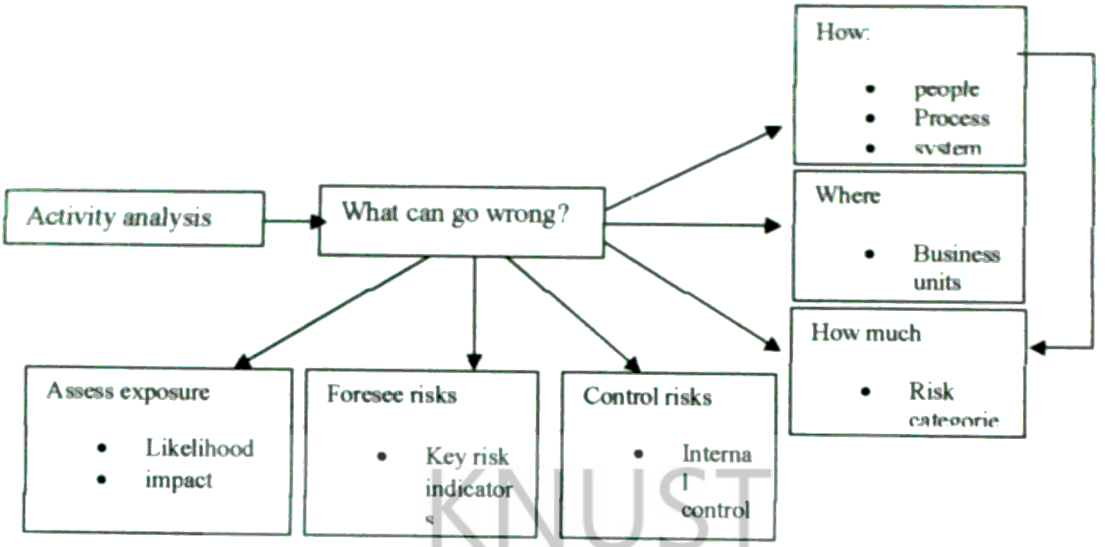


Fig: 2.4.2 Source: Scandizzo (2005)

2.6 Causes and Effects

Crouhy et al (2000:357) state that an organisation should analyse the causes and effects of an operational loss such as they depict in the table below:

Table: 2.5.1 Causes and effects of an operational loss

Risk factor	Causes	effects
People(human resource)	Loss of key staff due to defection of key staff to competitor.	Variance in revenue(for example, cost of recruitment, training, disruption to existing staff)
Process	Declining productivity as value grows	Variance in process costs from predicted levels(excluding process malfunction).
Technology	Application development	Variance in technology running costs from predicted levels.

Source: Crouhy and Mark (2000:358)

According to them, the effect of a risk like human fallibility may be a financial loss, however, that may be the final outcome of a chain of effects. They argue that A bank should attempt to identify all the links in that chain to ensure that they are addressed during the managing of the risk. They however note that the causation of risk is invariably complex, and that it could take a particular combination of causes to produce an effect. Laycock (1998) identifies six categories of causes (in table**: 2.5.2,** shown on appendix 3) that could give rise to operational risk.

Laycock (1998:133) classifies the causes and effects as follows:

- High-frequency/low impact events
- Low-frequency/high impact events such as wrongful trading, potentially involving several factors, for example, poor or ineffective controls in addition to the propensity for an individual to commit one or more wrongful acts

Laycock stresses that high-frequency/low-impact events are usually distinguished from low-frequency/high-impact events by the time lag between the operational events itself and the moment when its effect is felt by the organisation.

2.7 Underlying Risk Factors

Risk factors need to be identified so that adequate risk management tools can be put in place. According to Davies et al. (1998:76), a central requirement of risk allocation process is to be able to assess the extent to which the exposure to a risk factor increases or decreases the expected volatility of earnings. Their position

stresses the need to identify risk factors with adequate precision to be able to monitor and control them effectively.

2.8 Methods of Risk Identification

According to the Financial and Management Accounting Committee (FMAC) (1999:17) cited in Young (2001), management and other relevant personnel could identify the key risks in a number of ways such as listed below:

- Workshops and interviews
- Brainstorming
- Questionnaires
- Process mapping (which involves identifying and mapping the core business process/value chains and identifying the dependencies on internal enablers such as personnel and technology, and external factors such as regulations, customers and service providers, that cut across the process).
- Comparisons with other organisations
- Discussion with peers.

2.9 Evaluation of Operational Risk

Valsamakis et al. (1996:104) cited in Young (2001), state that risk evaluation fulfills a dual role: facilitating the method of treatment, the other measuring the effect or degree of success following implementation. Crouhy et al (2000:351) state that during the evaluation of risk, one can assess operational risk in terms of the likelihood of operational failure and the severity of potential loss. They

contend that the assessment should include the options available to manage and take appropriate actions to reduce the risk.

Measuring operational risk requires both an estimate of the probability of an operational loss event and the potential size of the loss. Most approaches rely largely on risk indicating factors to provide an indication of the likelihood of an operational loss event occurring. According to the Basel Committee (1998a:4), operational risk factors are largely internal to a bank and a clear mathematical and statistical link between risk and factors and the likelihood and size of the operational losses does not exist.

Crouhy and Mark (2000:351) suggest that clear guiding principles for the operational risk measurement process should be set to ensure that it provides an appropriate measure of operational risk across all business units throughout a bank. They again suggest the following key tasks to be considered in a measurement method:

- Identification of an approach to clearly describe operational exposures, risk factors and potential losses.
- Establishment of a relationship between exposures, risk factors and potential losses.
- Control of high-frequency/low-impact events and low-frequency/high-impact events.
- Incorporation of the resulting model and reports into the key business and management processes of the firm.

They further describe a four – step measurement process for operational risk as shown below:

- **Step 1 – Input**: gather the information needed to perform a complete assessment of all significant operational risks.
- **Step 2 – Risk assessment framework**: Analyse and process information gathered through a risk assessment framework (as shown in the diagram below).
- **Step 3 – Review and validation**: Senior management and the operational risk committee should review the summary report that will be generated.
- **Step 4 – output**: Formally report the final assessment of operational risk to management. This will provide better operational risk information to management to use in risk management decisions and to reflect the extent of the exposure of the business unit to operational risk.

2.10 Approaches to Measuring Operational Risk

According to Junji Hiwatashi (2002), there exist both top-down and bottom- up methods in measuring operational risk (Table: 2.9.1 & 2.9.2). The author explains that the former seeks to estimate it on a macro basis without identifying events or causes of losses, while the latter measures it based on identified events that explain the mechanism of how and why operational risk occurs. He continues that advanced international banks commonly employ these two methods in the following ways:

They may start with the top-down method temporarily, in order to allocate their economic capital to operational risk, and then shift to bottom-up methods such as statistical measurement approach and scenario analysis by establishing robust event and loss databases. Or, they may directly start with a combination of bottom-up methods such as statistical measurement approaches and scenario analyses to measure operational risk. In other words, it is necessary to measure operational risk based not only on historical data, but also scenario data with forward looking approaches, given the rapid change in environment surrounding the banking industry.

Table: 2.9.1 **Examples of Top-Down Method**

Approaches	Way to Measure Operational Risk
Indicator Approach	It is assumed that, for example, gross income or cost is a proxy, and that a certain percentage is regarded as operational risk of banks.
CAPM Approach	It is assumed that all the risks are measured based on Capital Asset Pricing Model (CAPM); then, market risk and credit risk, measured separately, are deducted from all risk measured by CAPM.
Volatility Approach	Volatility of income is regarded as a risk. For example, volatility of non-interest income, which is regarded as operational risk, is measured.

Source: Junji Hiwatashi (2002)

Table: 2.9.2 **Examples of Bottom-Up Method**

Approaches	Way to Measure Operational Risk
Statistical Measurement Approach	The maximum amount of operational risk is measured based on individual events with frequency and severity using Monte Carlo simulation or an analytical solution.

Scenario Analysis	As for events with low frequency and high severity, losses would be estimated based on scenarios, with reference to external data and events that occurred at other banks
Factor Analysis Approach	Factors related to losses such as transaction volume and error ratios are identified and are taken into account with correlation analysis
Bayesian Network Model	Causes and effects of operational risk are modeled. There are cases where this model is used in settlement risk management

Source: Junji Hiwatashi (2002)

2.11 Operational Risk Measurement Methodologies in Basel II

The Basel framework (2004) proposes a range of approaches for setting aside regulatory capital for operational risk under Pillar 1. The Basic Indicator Approach (BIA), The Standardised Approach (TSA) and the Advanced Measurement Approach (AMA). All the three approaches differ in their complexity and the banks are encouraged to move along the spectrum of approaches as they obtain more sophistication in their risk management practices.

2.11.1 The Basic Indicator Approach According to Janakiraman (2008), seen as the simplest approach for estimating regulatory capital, where banks are required to set apart an amount equal to the average over the previous three years of 15% of positive annual gross income. This approach, he argues, links the capital demand for operational risk to the institution's operating income. It sets the capital demand for operational risk to 15% of the average operating income (defined as the average of the last three years operating income, taking only

positive yearly operating income into account). Here, the operating income is defined as net interest, net leasing, net financial transactions, dividend received, and other operating income.

$$K_{BIA} = \left[\sum (GI_{1\ldots n} \times \alpha)\right]/n$$

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

Table: 2.10 Constitution of Gross Income

Included in Gross Income	Excluded from Gross Income
1. Interest and leasing income 2. Interest and leasing costs 3. Dividends 4. Income from commissions (including provisions from the selling of insurance products) 5. Costs for commissions 6. Net result from financial transactions 7. Other income	1. Leasing costs for leasing that is not part of the leasing business 2. Dividends from associated and group companies 3. Realised profit/loss from selling of assets in "other business" 4. Income from insurance 5. Fees from outsourced services supplied by a third party which is not the mother company or subsidiary to a mother company which is also the mother company of the institute

Source: Gunilla Delin (2007)

2.10.2 The Standardised Approach: Again, Janakiraman (2008) explains that the Standardised Approach is a slightly modified version of the Basic Indicator Approach. In The Standardised 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. While gross income continues to be the main indicator of operational risk as under the Basic Indicator Approach, the specific amount to be set apart as a percentage of the gross income varies between business lines, ranging from 12 to 18% , as compared to the 15% overall under the Basic Indicator Approach.

The income indicator is based on the Operating Income for the business area and is calculated in the same manner as in the Basic Indicator Approach. The business areas and percentage levels are given in the table below:

$$K_{TSA} = \left\{ \sum_{years 1-3} \max \left[\sum (GI_{1-8} \times \beta_{1-8}), 0 \right] \right\} / 3$$

Where:

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

GI_{1-8} = annual gross income in a given year, as defined 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: 2.10.1 value of betas allocated to various business lines

Business area	Percentage level
Corporate finance (β_1)	18%
Trading and Sales (β_2)	18%
Retail Banking (β_3)	12%
Commercial Banking (β_4)	15%
Payment and Settlement (β_5)	18%
Agency Services (β_6)	15%
Asset Management (β_7)	12%
Retail Brokerage (β_8)	12%

Source: Gunilla Delin (2007)

2.11.3 The Advanced Measurement Approach (AMA): The Advanced Measurement Approach (AMA) is based on the banks' internal models to quantify operational risk (BCBS 2006). The framework gives flexibility to the banks in the characteristics of the choice of internal models, though it requires banks to demonstrate that the operational risk measures meet a soundness standard comparable to a one-year holding period and a 99.9% confidence level, which means that a bank's capital charge should be equal to at least 99.9% quantile of their annual aggregate loss distribution.

Banks are required to factor in four key elements in designing their Advanced Measurement Approach framework: internal loss data, external loss data, scenario analysis and bank specific business environmental and internal control factors.

The methodologies under the advanced approach are evolving and there are a range of methods in practice in banks internationally (BCBS 2006). In order to qualify for using the AMA a bank must ensure its supervisor that, at a minimum:

- Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;
- It has an operational risk management system that is conceptually sound and is implemented with integrity; and
- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

The bank's measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that

creates incentives to improve business line operational risk management. In essence however, banks are allowed considerable freedom in implementing their own method for assessing their exposure to operational risk, as long as it is sufficiently comprehensive and systematic.

Kingsley et al (1998:7) believe that methodologies for measuring operational risk range from simplistic to much more detailed calculations. According to them operational risk is one that does not lend itself to easy quantification. Stoll (1996) cited in Young (2001) agrees to this assertion and argues that this could pose a problem, especially if a bank requires visible benefits of a risk adjusted performance measure and wants to determine the allocation of capital relating to operational risk.

As Alexander (2000:2) puts it, choosing the best methodology for any given category of operational risk is less of an issue than the application the methodology or model to produce meaningful measures of operational risk. He claims that the major problem with any model for operational risk is the adequacy of data as he depicts in the instances given below:

- Internal loss event data for low-frequency/high-impact risks such as fraud may be too incomplete to estimate an extreme value distribution for measuring the tail loss. Augmenting the database with external data may also not be appropriate.
- Operating costs have a tenuous relationship with operational loss and therefore the proportional charges that regulators are considering for

operational risk, based on a fixed percentage of operating costs may be very inaccurate.

- Internal risk ratings are based on assessments of the size and frequency of operational losses from the different activities in a business unit. The data may be inaccurate because of its subjective nature.
- Regression models of operational risk that are based on the CAPM framework produce betas that are based on many subjective choices of data.

He argues that the inadequacy of the data means that subjective choice is much more of an issue in operational risk than it is in market or credit risk assessment.

Hoffman's approach (1998:84) to quantify operational risk looks at identifying a number of possible conceptual foundations for operational risk modeling as described below:

- Factor-derived models: These apply loss and/or causal factors to build a bottom-up prediction of loss expectancies.
- Economic pricing models: These are base forecasts on economic models, such as the CAPM to suggest a relative distribution of pricing for operational risk among the other price determinants for capital.
- Scenario analysis/subjective loss estimate models: Used to capture diverse opinions, experiences or expertise of key managers in matrix/graphic form
- Statistical/actuarial loss potential models: These use actual loss data to construct representations of loss frequencies and severity in the form of

statistical probability distributions. Simulation techniques are then used to combine the distributions in modeling possible loss scenarios for the future.

Peterken (1998:15) cited in Young (2001), proposes as an approach to quantify operational risk, the catastrophic risk as one of the external factors of operational risk. According to him, catastrophic models produce individual forecasts of losses known as Estimated Maximum Loss (EML). He argues that by taking the EML across a large number of different scenarios, in terms of location of the hazard and its intensity, loss exceedance curves may be derived. The curves give the probability of a loss equal to or greater than a specified amount and may be used to calculate limits for insurance and other risk - transfer methods. They may also identify areas for risk - reduction programmes and assist in prioritizing management efforts.

In Peterken's model, the area under a loss exceedance curve gives the annual average loss (AAL), which is the expected loss over a long period to the business. This he claims is equivalent to the pure technical cost of risk (being the cost of transferring risk but before an amount for the uncertainty in those estimates and the randomness of their outcome is made).

Regardless of the approaches, Young (2001) says the following are the most used approaches to quantify operational risk:

Risk indicators: These, according to PwC (1999:61), cited in Young(2001), are quantitative measures intended to provide insight to the effectiveness of

operational risk management and controls, example, the number of failed trades or number and severity of errors and omissions (Table 2.10.2 shown on appendix 3 and 2.10.3 on appendix 4). They may also include measures and metrics that are used to monitor the level of operational risk. PwC (1999:62), however points out that, current trends require organisations to develop "leading" indicators (often in the form of stand-alone reports, usually on monthly basis) which provide management with early warning signals of operational risk issues.

Escalation triggers: These are used as a basis to communicate potential problems to management. The starting point for escalation trigger points is a set of risk indicators with set goals or limits. On reaching the set limit, the indicators are highlighted and given to the predetermined appropriate business unit. The triggers are sometimes set low and used as a warning signal to the first level of management. They are at other times set at higher levels and therefore may have increased importance when reached.

A loss-event database: A loss event database captures and accumulates individual loss events across business and risk types. The data have three potential applications as described by PwC (1999:67) cited in Young (2001):

- Performing an empirical analysis so that institutions can assess current policies and controls and gain comfort on their effectiveness,
- Quantifying the loss from operational risk to show the progress over time,

- Modeling of operational risk, where the raw data may be used to develop a predictive and causal model of risk and as input into the capital models. Managers are then able to use the data to determine the most effective level of mitigation and investment.

The causal modeling of operational risk: This approach sets out the framework to determine regulatory capital. An important requirement is to observe causes as well as effects or losses. Wilson (2000:390) says this approach comprise the following steps:

- Define operational risk,
- Document and collect data,
- Build a prototype of the system
- Refine data collection,
- Finalize prototype and roll out throughout the organisation

This enhances the understanding of the losses and provides a means for performing stress testing and simulations similar to the existing credit and market techniques.

2.12 Qualitative and Quantitative Approaches to Measuring Operational Risk

Different approaches and models to measure operational risk can also be looked at or considered under the qualitative and quantitative approach.

2.12.1 Qualitative Approach: Young (2001) points out that most approaches to operational risk and internal control are qualitative in that the identification of operational risk is measured in words rather than numbers. This is corroborated by Wilson (2000:388) who states that a common approach is to perform a review of the way a business manages operational risk and then to perform a risk assessment based upon the "objective" judgment of an experienced reviewer.

Qualitative methods are unable to measure the impact or loss in terms of a discrete value. Suh (2003), says that they attempt to express the risk in terms of descriptive variables (assessment on a Likert scale from 1 to 5, for example) based on the knowledge and judgment of an analyst. These methods as identified by Suh (2003) include:

- Delphi techniques
- Scenario Analysis
- Fuzzy metrics
- Comparison risk ranking, and
- The questionnaires."

A more common method for qualitative assessment of risk according to Suh (2003) uses the following techniques:

- Risk probability assessment
- Risk impact assessment
- Risk matrices and tables

2.12.2 Quantitative Approach: This method measures the risk based on a monetary or discrete value. "Quantitative methods strive for greater precision, and they reveal more about each risk" (Kendrick, 2003). According to Kendrick, quantitative analysis also provides data one can use to assess overall project risk and to estimate schedule and/or budget reserves for risky projects and operations. Suh (2003) stated that quantitative analysis methods usually calculate annual loss expectancy (ALE) for each threat. The methods include:

- Courtney Method
- Livermore risk analysis methodology (LRAM)
- Stochastic dominance method, and
- PERT & Simulation e.g. Monte Carlo Simulation is one of the most used simulation methods used in risk analysis.

2.13 Control of Operational Risk

Risk control activities are aimed at preventing losses and minimizing the consequences of losses that may arise from all risks facing the organisation or financial institution, and dealing with an adverse event in advance or as it occurs. Valsamakis et al. (2000:107) cited in Young (2001), explain in their work that all risk control activities or events are directed towards minimizing losses that potentially might result. Valsamakis et al. (2000:107) categorise these activities as follows:

- Activities aimed towards controlling the possible adverse occurrence of an event and then endeavoring to eliminate it; and
- Activities directed towards minimizing the loss after it occurred.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The following chapter discusses and validates the choice of methodology used in the long essay, which has guided the researcher in how the subject should be approached, as well as how the required information should be collected and processed. It includes choice of subject, research approach, data collection, value of study, and chosen methodology.

Data collection and analysis were conducted following the framework from Creswell (2007) in order to achieve quality of the research. The study was developed from reviewing related literatures from reliable and accessible sources, such as BNET that provides thousands of e-journals and hundreds of databases.

3.2 Research Approach

In a research, the researcher may choose between two approaches; qualitative and quantitative method. The qualitative method involves the gathering of a lot of information from few examination units through interviews and observations, while the quantitative method entails that, the researcher collects little information from many investigation units through, for instance questionnaires.

For the purpose of this long essay the quantitative method was largely applied, and thus necessitating the use of a questionnaire, and then again in necessary

conditions, qualitative data was collected in accordance to the purpose of the study

The study started from literature review that summarizes and synthesizes sources within each paragraph as well as throughout the review, and consequently moved towards concrete empirical evidence that involved studying the extent in which different international and local factors exist and are being applied. Finally, the findings were analyzed in relation to theory

As a result, a deductive approach was applied, which implies that the researcher "begins with a theoretical or applied research problem and ends with empirical measurement and data analysis" (Neuman 2003, p. 267).

3.3 Literature Review

As stated, the literature review provides the foundation and framework for the research, and allows the researcher to be brought up to date regarding the state of the research in the field, and familiarizes with any contrasting perspectives and viewpoints on the topic. The research areas that are looked for are related to operational risk management, and risk assessment in the banking industry

Oates (2005), says that data collection can be conducted from many sources of data such as books, journals, conference and workshop proceeding, reports, newspapers, magazine, resource catalogues and online database, and internet literature reviews. The researcher combined several activities that are generally

used to conduct literature reviews, which includes searching, obtaining, assessing, reading, critical evaluating, and writing a critical review. This information was used with the data obtained from the interviews to analyze the study in the next phase.

3.4 Data Collection

Data is one out of two types, either primary which is collected by the researchers, or secondary data which is gathered by other researches (Andersen, 1998). The researcher decided to use a questionnaire as the main source of data (primary) collection.

Multiple sources of evidence were used along the data collection process of this research to ensure the validity. This is because according to Yin (2003), multiple sources of evidence methodology involves in the internal validity basically because the method provides data from many sources to analyze and discuss the research questions. Document, archival records, open-ended interviews, structured interviews and observation were considered to be the choices of investigation.

Due to the limited timeframe and research location, some of the sources of evidence, such as observation or surveys, were not suitable in the study. While not all the sources were ready, each possible source was intensively investigated to make sure that the researcher had enough information to analyze, to be able to answer the research question reasonably.

3.4.1 Questionnaire

The questionnaire as used by the researcher is a combination of frameworks used by Moody's (2003), and Young (2001). It allowed the researcher to gather specific information on the general approach and management of operational risk in the study area, as well as the different factors that influence it. A questionnaire is seen as a self contained, self-administered instrument for asking questions.

The researcher accordingly divided the questionnaire into largely structured and unstructured questions. A structured question may entail either multiple choices, dichotomous questions, or a scale, whereas an unstructured question is an open-ended question, which implies that the respondents answer in their own words (Malhotra, 2004).

The structured questions are either dichotomous or scales. In dichotomous questions, the respondents could only choose between two response alternatives, such as Yes or No, making it easy to code and analyze. A ratio scale was also used which allowed the respondents to classify or rank order the objects, i.e. 1 – 5, where 5 represents "strongly agree" and 1 indicates "strongly disagree". Finally, in combination with the structured questions, unstructured questions were asked, where the respondents were able to make any other necessary comments (Neuman, 2003).

3.4.2 Sample Selection

The population chosen to investigate in order to reach the desired purpose was chosen from 20 out of the 25 banks in Ghana, and thus the researcher decided upon a combination of quota sampling and convenience sampling from this population. Quota sampling implies that a researcher can choose to have a specified proportion of the investigated elements in the study. These respondents were chosen as a result of easy access.

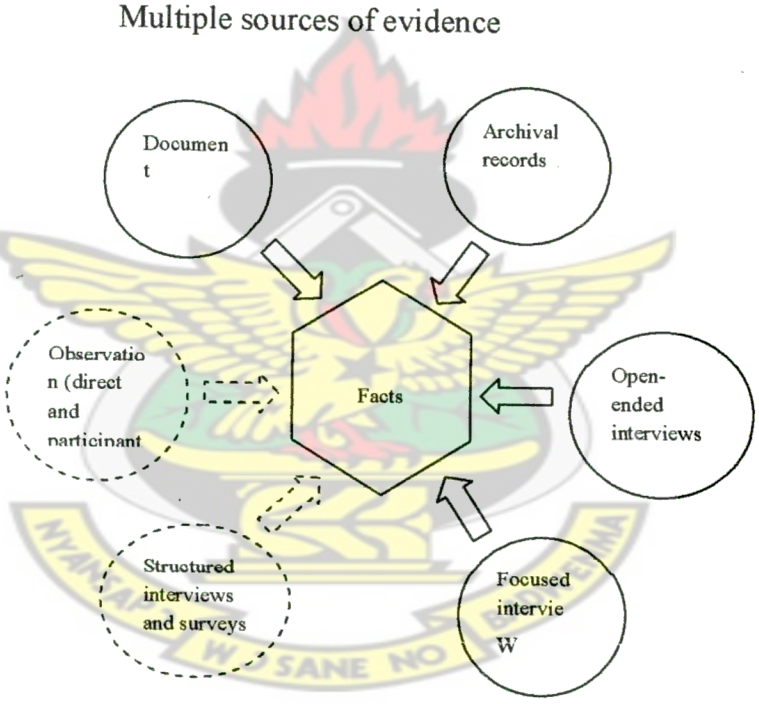


Fig 3.1 Yin 2003, (page 100)

3.4.3 Interviews

In order to investigate the study, interviews were used to gain information from people who have experience or knowledge about the system in place as far as the issue of operational risk and its management was concerned. The semi-structure

interview is the interview type that the researcher selected for this study. Themes to cover and questions to ask were prepared beforehand, but could be changed to best match the flow of conversations.

The questions were open-end that will help explore the interviewees' experiences. The questions and interview guide will provide a direction of the interview conversation to focus on operational risk and risk management. In the same time the researcher could get more additional data or issues from interviewee beyond the interview questions.

As Oates (2005) describes about the semi-interview structure that additional questions might be asked when new issues or interesting topics were unexpectedly raised by the interviewees. This justifies the use of Semi-structured interview framework along the interviewing research phase for the reasons stated.

3.4.4 Data Analysis

Themes to conduct the research were identified for the data collection process. The needed theme was related to assessing operational risk and management. As Oates (2005) suggests, obtained data were grouped by their relevance to the research. Some group of data provides general descriptive information that was needed to describe the research context for the readers. Analysis took place differently in several phases, which will be intensively discussed in the empirical findings chapter.

3.4.5 Statistical method

The statistical analysis of the data collected was largely done with the SPSS, and the pie charts generated with Excel, as the researcher found it very convenient.

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSIONS

4.1 Introduction

This chapter encompasses the empirical data collected through the questionnaires with the 41 respondents. The questionnaires were sent to the twenty banks listed on appendix 5. To facilitate the statistical analysis, questions with similar content or relating to a specific topic are combined by the researcher. This reflects grouping of related questions under sections 2 and 3, to enhance a more ordered analysis of the research data.

4.2 Statistical Analysis of Data

A total number of 60 questionnaires were sent to the banks selected for the study. The returned questionnaires totaled 41, representing 68.3% response rate. The response rate covered 76.9% of all banks registered in Ghana, though not equally represented. The coverage is significant as far as representation in the sample is concerned.

Given the percentage representation of 76.9% stated above, it can be deduced therefore that the banks are well represented in the sample and findings may thus be generalized to be relevant and significant.

4.2.1 Respondents

The percentage distribution of respondents to the questionnaire is as shown in table (4.1) and fig (4.1) respectively:

Table: 4.1 practical banking experience of respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-3 years	13	31.7	31.7	31.7
	4-6 years	11	26.8	26.8	58.5
	7-9 years	11	26.8	26.8	85.4
	10-12 years	2	4.9	4.9	90.2
	more than 13 years	4	9.8	9.8	100.0
	Total	41	100.0	100.0	

Source: field data

Fig: 4.1 Source: field data

The relatively large percentage of risk managers (43.9%) who responded to the questionnaire is an indication that risk is being regarded as an overall

responsibility, as alluded to by Young (2001), rather than consisting of specialized areas. It is a further indication that operational risk management in the banking environment in Ghana is not being vigorously attended to, though some recognition is given to it, considering the 24.3% respondents to the questionnaire who were operational risk managers.

4.3 Definition

As depicted in fig 4.2, 43.9% and 19.51% agreed and strongly agreed respectively that their banks have adopted a specific definition for operational risk. It is an indication therefore that most banks are still in the process of formally adopting a definition or demarcating the area of operational risk. This is an important step in an effective management of operational risk, as described by Young (2001).

Company has adopted a specific definition for Operational Risk

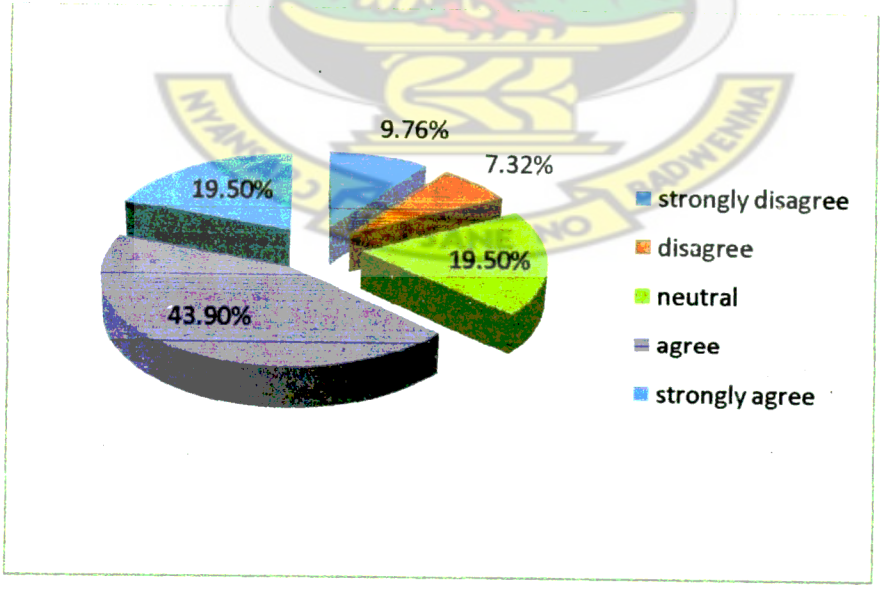


Fig: 4.2 **Source: field data**

4.4 Risk Types

Questions on this item sought to ascertain the risk types that the banks are currently managing as primary risk types, and what the respondents consider ideal. The responses show that the following percentage (fig. 4.3) of respondents indicated the risks as primary risk types: credit risk (75.6%), market risk (85.3%), liquidity risk (80.5%), operational risk (82.9%), interest rate risk (90.3%), country risk (63.4%), legal risk (80.5%), and reputational risk (78%). What they considered ideal showed the following percentages respectively: 87%, 85.4%, 82.9%, 87.8%, 87.8%, 68.3%, 82.9%, and 80.5%.

The relatively high percentage of 82.9% for operational risk for both the current situation and what the respondents considered ideal is an indication that some recognition is given to the fact that operational risk is being recognized as a primary risk though the banks are not pursuing it vigorously.

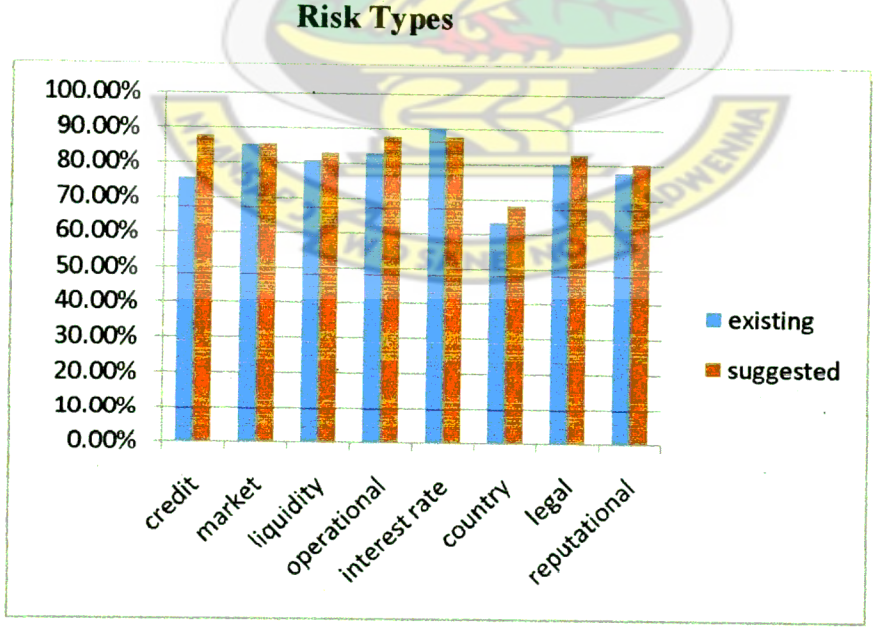


Fig: 4.3 **Source: field data**

4.5 Primary Operational Risk Factors

This item tried to ascertain what the banks currently consider as primary operational risk factors, and how important in their opinion they should be. Again, it was to determine which exposures, relating to these operational risk factors, are currently recognized by banks and the extent to which in their opinion, they should be managed as part of the underlying risk factors of operational risk.

The primary risk factors as identified by young (2001) and captured in the literature were: people, processes, systems and external events. The response as presented in table 4.2, indicate that more than 80% of the respondents demonstrated that the banks clearly understand that people, processes, systems and external events, are critical underlying risk factors of operational risk, thus agreeing to what has been described by the Basel Committee (2004).

Table: 4.2 **Primary Operational Risk factors (%)**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
people	7.3	0	7.3	36.6	48.8
processes	7.3	0	7.3	34.1	51.2
systems	4.9	2.4	9.8	31.7	51.2
External events	2.4	0	17.1	36.6	43.9

Source: field data (2009)

4.6 Operational Risk Exposures

The operational risk exposures identified under each primary risk factor are presented in the tables below. The objective was to determine to what extent banks currently give recognition to the various exposures (as identified in the

literature) underlying the above mentioned risk factors, and the extent to which in their opinion, it should be recognized. The level of their recognition of these exposures represents the extent of their own exposure to these risks.

4.6.1 People exposure: It was identified (see tables 4.3 & 4.4) that the extent to which banks recognised the following people exposures are: incompetence (63.4%), negligence (68.3%), human error (82.9%), low moral (63.4%), high staff turnover (53.6%), fraudulent activities by employees (61%) and lack of training (73.2%). What the respondents suggested saw the percentages changing to 87.9%, 87.8%, 78.1%, 70.8%, 68.3%, 82.9% and 80.5% respectively.

This clearly indicates that the banks recognise the risk exposures identified under people as a risk factor, though they also reocognise that they need to do more, which reflected in what they suggested as the extent to which the banks should recognise these exposures.

Table: 4.3 People Exposures (Existing) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
incompetence	7.3	4.9	24.4	46.3	17.1
negligence	0	4.9	26.8	53.7	14.6
human error	0	2.4	14.6	75.6	7.3
low moral	2.4	19.5	14.6	61.0	2.4
high staff turnover	12.2	17.1	17.1	46.3	7.3
fraudulent activities by employees	2.4	9.8	26.8	51.2	9.8
lack of training		24.4	2.4	63.4	9.8

Source: field data (2009)

Table: 4.4 **People Exposures (Suggested) (%)**

	strongly disagree	Disagree	neutral	agree	strongly agree
incompetence	7.3	2.4	2.4	65.9	22.0
negligence	7.3	0	4.9	61.0	26.8
human error	7.3	0	14.6	53.7	24.4
low moral	4.9	4.9	19.5	61.0	9.8
high staff turnover	2.4	0	29.3	53.7	14.6
fraudulent activities by employees	7.3	4.9	4.9	63.4	19.5
lack of training	7.3	0	12.2	56.1	24.4

Source: field data (2009)

4.6.2 Process Exposure: Similarly, it was identified from the results (see tables 4.5 and 4.6) that the extent to which banks recognised the following process exposures are: errors in procedure (87.2%), execution errors (78%), documentation error (82.9%), product complexity (63.5%), and security risk (82.9%). Again, what the respondents suggested saw the percentages changing to 80.5%, 82.9%, 80.5%, 85.4%, and 90.2%, respectively.

This is a further indication that the banks recognise the risk exposures identified under process as a risk factor, though they also reocognise that they need to do more, which again, reflected in what they suggested as the extent to which the banks should recognise these exposures. It however appeared that security risk appeared to be of a major concern, considering the relatively high percentage

(90.2%) they suggested as ideal. This was closely followed by product complexity which increased from 63.5% to 85.4%.

Table: 4.5 Process exposure (Existing) (%)

	strongly disagree	Disagree	neutral	agree	Strongly agree
errors in procedures		4.9	7.3	73.2	14
execution errors		9.8	12.2	75.6	2.4
documentation errors		2.4	14.6	75.6	7.3
product complexity		31.7	4.9	53.7	9.8
security risk		7.3	9.8	68.3	14.6

Source: field data (2009)

Table: 4.6 Process exposure (Suggested (%)

	strongly disagree	Disagree	neutral	agree	strongly agree
errors in procedures	7.3	0	12.2	58.5	22.0
execution errors	7.3	2.4	7.3	58.5	24.4
documentation errors	4.9	0	14.6	51.2	29.3
product complexity	2.4	2.4	9.8	65.9	19.5
security risk	7.3	2.4	0	56.1	34.1

Source: field data (2009)

4.6.3 System Exposure: Again, it was identified (see tables 8 and 9) that the extent to which banks recognised the following system exposures are: system infiltration (65.9%), system failures (87.8%), fraud (82.9%), programming errors (87.9%), information risk (82.9%), and obsolescence of system (73.2). Further, what the respondents suggested saw the percentages changing to 85.3%, 80.5%, 85.3%, 75.6%, 82.9%, and 78.1% respectively.

This establishes the banks recognition of the risk exposures identified under system as a risk factor, though also reocognised that they need to do more, which again, reflected in what they suggested as the extent to which the banks should recognise these system exposures.

Table: 4.7 System exposure (Existing) (%)

	strongly disagree	Disagree	neutral	agree	strongly agree
system infiltration		7.3	26.8	43.9	22.0
system failures			12.2	56.1	31.7
fraud		4.9	12.2	39.0	43.9
programming errors		4.9	7.3	65.9	22.0
information risk		2.4	26.8	56.1	14.6
obsolescence of systems	7.3	2.4	17.1	53.7	19.5

Source: field data (2009)

Table: 4.8 System exposure (Suggested) (%)

	strongly disagree	Disagree	neutral	agree	strongly agree
system infiltration	7.3	2.4	4.9	58.5	26.8
system failures	7.3	0	12.2	43.9	36.6
fraud	7.3	0	7.3	39.0	46.3
programming errors	7.3	0	17.1	43.9	31.7
information risk	7.3		9.8	56.1	26.8
obsolescence of systems	7.3	2.4	12.2	56.1	22.0

Source: field data (2009)

4.6.4 External Exposure: Here too, it was identified (see tables 10 and 11) that the extent to which banks recognised the following external exposures are: acts of God (39.5%), external criminal activities (70.8%), regulator and compliance (83%), legal actions (75.6%), business environment changes (80.5%), strike

(78%), and money laundering (78.1%). Again, what the respondents suggested saw the percentages changing to 40%, 68.3%, 80.5%, 80.5%, 82.9%, 68.3%, and 73.1% respectively.

This establishes a clear inconsistency in the banks recognition of the risk exposures identified under 'external' as a risk factor, though some recognition was given to exposures such as external criminal activities, legal actions, business environment changes, strike and money laundering. Acts of God which was not highly recognised may be due to recognition of the fact that very little can be done about that.

Table: 4.9 **External Exposure (Existing) (%)**

	strongly disagree	Disagree	neutral	agree	strongly agree
acts of God	2.4	4.9	51.2	19.5	22.0
external criminal activities	7.3		22.0	48.8	22.0
regulator and compliance	7.3		9.8	65.9	17.1
legal actions	7.3		17.1	46.3	29.3
business environment changes	7.3	2.4	9.8	51.2	29.3
strikes	7.3	7.3	7.3	51.2	26.8
money laundering	7.3	4.9	9.8	48.8	29.3

Source: field data (2009)

Table: 4.10 **External Exposure (Suggested) (%)**

	strongly disagree	Disagree	neutral	agree	strongly agree
acts of God	9.8	9.8	36.6	22.0	22.0
external criminal activities	4.9	12.2	14.6	53.7	14.6
regulator and compliance		7.3	12.2	61.0	19.5
legal actions		12.2	7.3	70.7	9.8
business environment changes		12.2	4.9	75.6	7.3
strikes	9.8	14.6	7.3	56.1	12.2
money laundering	2.4	19.5	4.9	46.3	26.8

Source: field data (2009)

4.7 Formal Risk Management Approach

The study sought to understand the formal risk management approaches being used by the banks in managing operational risks. As stated by the Basel Committee (2004), appropriate approaches will allow a good bank or financial institution to get a more just picture and improved control and management of its operational risks. The following discusses the methodologies and tools being used by the Ghanaian banks in managing their operational risks.

4.8 Elements of an Operational Risk Management Process

This item sought to ascertain the extent of adoption of the following elements of an operational risk management process as identified in the literature. The responses show that the banks appropriately recognise the elements of operational risk management, though they suggested that they could do a lot more to improve current standards, as presented in tables (4.11 and4.12) respectively.

Table: 4.11 **Elements of an Operational Risk Management Process (Existing) (%)**

	strongly disagree	disagree	neutral	agree	strongly agree
risk identification	7.3	2.4	9.8	63.4	17.1
risk evaluation / measurement	7.3	2.4	9.8	58.5	22.0
risk control	7.3	2.4	9.8	53.7	26.8
risk financing	7.3	7.3	4.9	68.3	12.2

Source: field data (2009)

Table: 4.12 Elements of an Operational Risk Management Process (Suggested) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
risk identification	7.3	0	4.9	56.1	31.7
risk evaluation / measurement	7.3	0	4.9	61.0	26.8
risk control	7.3	0	2.4	58.5	31.7
risk financing	7.3	0	4.9	61.0	26.8

Source: field data (2009)

4.9 Identification of Operational Risk: This item sought to identify the methods used by the banks in the identification of their operational risk , based on what the Young (2001) suggested as a step in effectively managing operational risk. The response showed a more than 70% extent of the usage of each of the methods presented, which is quite significant although in their opinion they could do more as reflected in the higher percentages suggested (see tables 4.13 and 4.14 respectively).

Table: 4.13 Identification of Operational Risk (Existing) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
workshops	0	2.4	17.1	63.4	17.1
brainstorming	0	0	14.6	65.9	19.5
questionnaires	2.4	2.4	9.8	68.3	17.1
process mapping	7.3	0	9.8	68.3	14.6
comparisons with other organisations	7.3	2.4	7.3	65.9	17.1
discussion with peers	7.3	9.8	9.8	51.2	22.0

Source: field data (2009)

Table: 4.14 Identification of Operational Risk (Suggested) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
workshops	0	2.4	17.1	63.4	17.1
brainstorming	0	0	14.6	65.9	19.5
questionnaires	2.4	2.4	9.8	68.3	17.1
process mapping	7.3	0	9.8	68.3	14.6
comparisons with other organisations	7.3	2.4	7.3	65.9	17.1
discussion with peers	7.3	9.8	9.8	51.2	22.0

Source: field data (2009)

4.10 Measuring Operational Risk

4.10.1 Qualitative Methods : There was an evidence of some qualitative methods being used. The response indicate that self risk assessment is the most used, followed by risk maps and process flow and then historical data.

Table: 4.15 Qualitative Methods (Existing) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
historical data to forecast the likelihood of a potential loss	0	7.3	26.8	61.0	4.9
self-risk assessment	0	12.2	14.6	68.3	4.9
risk maps / process flow	0	12.2	19.5	63.4	4.9

Source: field data (2009)

Table: 4.16 Qualitative Methods (Suggested) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
historical data to forecast the likelihood of a potential loss	7.3	2.4	4.9	70.7	14.6
self-risk assessments	7.3	0	9.8	65.9	17.1
risk maps / process flows to measure OR	4.9	0	14.6	61.0	19.5

Source: field data (2009)

4.10.2 Quantitative Methods The response to the quantitative methods identified in the study also indicate that risk indicators is the most important, followed by escalation triggers and then loss event database before apparently little known causal modeling. Respondents however suggested as shown in Table 4.16, that escalation triggers should be the most important.

Table: 4.17 Quantitative Methods (Existing) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
causal modeling	0	14.6	48.8	36.6	0
risk indicators	7.3	7.3	2.4	65.9	17.1
escalation triggers	7.3	2.4	9.8	63.4	17.1
loss-event database	9.8	2.4	7.3	63.4	17.1

Source: field data (2009)

Table: 4.18 Quantitative Methods (Suggested) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
causal modeling	2.4	7.3	31.7	41.5	17.1
risk indicators	7.3	2.4	12.2	58.5	19.5
escalation triggers	7.3	0	7.3	63.4	22.0
loss-event database	12.2	0	9.8	48.8	29.3

Source: field data (2009)

4.11 Operational Risk Control: This item aimed at ascertaining the banks' usage and recognition of the control measures identified according to Young (2001) to be policy and procedures, internal controls and risk reporting. The response identified policy and procedures as the existing most used, followed by internal controls and risk reporting respectively. The response however suggested that risk reporting should be the most important, followed by policy and procedures and then internal controls.

Table: 4.19 Operational Risk Control (Existing) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
policy and procedures	7.3	0	7.3	68.3	17.1
internal controls	7.3	4.9	4.9	63.4	19.5
risk reporting	9.8	2.4	7.3	63.4	17.1

Source: field data (2009)

Table: 4.20 Operational Risk Control (Suggested) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
policy and procedures	7.3	0	4.9	61.0	26.8
internal controls	7.3	0	7.3	53.7	31.7
risk reporting	7.3	0	2.4	58.5	31.7

Source: field data (2009)

4.12 Financing Techniques: The aim of this item was to ascertain the financing techniques used by the banks relative to what the literature suggests to be: risk transfer, risk retention (funded) and risk retention (unfunded) The responses to the methods identified in the study indicate that risk transfer is the existing most used financing technique, followed by risk retention (unfunded) and then risk retention (unfunded). Respondents suggested as shown in table 4.22 that the existing ranking is ideal.

Table: 4.21 Financing Techniques (Existing) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
risk transfers	2.4	12.2	26.8	53.7	4.9
risk retention (funded)	2.4	12.2	41.5	43.9	0
risk retention (unfunded)	2.4	9.8	41.5	46.3	0

Source: field data (2009)

Table: 4.22 Financing Techniques (Suggested) (%)

	strongly disagree	disagree	neutral	agree	strongly agree
risk transfers	0	4.9	7.3	82.9	4.9
risk retention(funded)	0	0	19.5	78.0	2.4
risk retention(unfunded)	2.4	4.9	14.6	75.6	2.4

Source: field data (2009)

4.13 Awareness of the Basel Approaches to Operational Risk Management:

The study also sought to find the level of awareness of banks of the existence of the Basel Committee's (currently Basel II) framework for determining the capital requirement ratio of banks and other financial institutions, and then again, its proposal on operational risk management. It was evident that 100% of respondents were aware of Basel proposals of some sort. However, less than 10% of the respondents were aware of and had studied the content of the Basel proposals. The rest indicated that their banks were aware of the proposals but had not spent time on the proposals or were vaguely aware of the proposals.

4.13.1 Adoption of Basel Approaches: It was obvious, judging from the responses from all the respondents used in the study that the banks are yet to fully adopt any of the approaches or proposals of operational risk management made by the Basel Committee.

However, that may be changing in the not too distant future as the Central Bank, as identified by the study, is re-orienting its supervisory focus away from just

compliance with norms to a system of risk-based supervision. This, according to findings, will involve re-orienting its approach towards implementing a risk-based supervision process. Its supervisory effort in this framework will be directed towards how well banks assess their risks and how actively they manage these risks and their capital, thereby minimizing systemic problems for the entire banking system.

The Central Bank has already rolled out some aspects of the Basel proposals in the form of its "Know Your Customer Policy", which The Basel Committee on Banking Supervision (BCBS) in its paper on Customer Due Diligence for Banks published in October 2001 issued guidelines for the implementation of Customer Due Diligence for Banks.

The document, as the Central Bank acknowledges, was also intended to provide the framework that will serve as benchmark for supervisors to establish national practices and for banks to design their own programmes.

The requirements of the document were consistent with Principle 15 of the Basel Core Principles Methodology which states that "Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict 'know-your-customer' rules that promote high ethical and

professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.

CHAPTER FIVE

CONCLUSION SUMMARY AND RECOMMENDATION

5.1 Introduction

This chapter presents a summary of the literature study and empirical research, and draws conclusions on the study and finally makes recommendations on further research to enhance operational risk management in Ghana's banking environment.

5.2 Summary of Major Findings

Operational risk is a major risk area, usually standing for 15-20 % of all losses a company is facing. While it is relatively straightforward for an organisation to set and observe specific, measurable levels of market risk and credit risk it is by contrast relatively difficult to do so for operational risk. Historically, organisations have simply accepted operational risk as an unavoidable cost of doing business. The summary of findings is outlined below as follows:

5.2.1 Defining Operational Risk: The study identified that all banks used in the research have adopted a formal definition for operational risk which is consistent with the Basel Committee's recognition of operational risk as resulting from inadequate or failed internal processes, people, and systems or from external events.

What emerged from the study was that awareness of operational risk as a separate risk category was relatively recent in most of the banks surveyed. While the major

banks in advanced countries have made considerable progress in the area of operational risk management over the last decade, the awareness of operational risk is a recent phenomenon in Ghana.

Also noted was the fact that losses from external events, such as a natural disaster that damages a firm's physical assets or electrical or telecommunications failures that disrupt business, are relatively easier to define than losses from internal problems, such as employee fraud and product flaws. Again, just a few of the banks actually have operational risk management structures and processes in place, which obviously does not enhance operational risk management.

5.2.2 Risk Types: The study also identified that banks recognize operational risk as a primary risk type in a banking environment, just as the other often-mentioned risk types such as credit risk, market risk, liquidity and interest rate risk. It however still requires some development to really take care of its status as a primary risk type. The yet to be adopted Basel proposals might adequately handle the situation, though not without some challenge.

5.2.3 Primary Operational Risk Factors: The primary risk factors as identified by young (2001) and captured in the literature were: people, processes, systems and external events. The study identified that more than 80% of the respondents demonstrated that the banks clearly understand that people, processes, systems and external events, are critical underlying risk factors of

operational risk, thus agreeing to what has been described in the literature. It was also identified that banks very well recognized the operational risk exposures identified under each primary risk factor, given the objective of determining the extent to which banks currently give recognition to the various exposures underlying the above mentioned risk factors, and the extent to which in their opinion, it should be recognized.

5.2.4 Identifying Operational Risk: The study revealed that consistent with the literature, banks used in the study, especially those that had a separate operational risk management structures and processes also, identified operational risks through workshops, brainstorming, questionnaires, process mapping, comparisons with other organisations and discussion with peers, just as identified in the literature.

5.2.5 Measuring operational risk: A key component of risk management is measuring the size and scope of the firm's risk exposures. As yet, however as the study revealed, there is no clearly established, single way to measure operational risk on a firm-wide basis. Instead, several approaches have been developed. In this way, a bank can hope to identify which events have the most impact across the entire firm and which business practices are most susceptible to operational risk.

5.2.6. Qualitative Risk Analysis: Qualitative risk analysis methods according to Suh (2003) "determine loss based on the knowledge and judgment of a risk

analyst rather than on a precise monetary values." In most cases, the analysis of the probability and impact is carried out by the risk owners as they should be people able to analyse, plan and manage risk. Certain people should be involved in this type of analysis. These include: relevant stakeholders, subject matter experts and the person who identified the risk.

The analysis should measure the probability of the impact of identified risk in terms of time, cost, and performance. The study revealed that banks methods such as: historical data to forecast the likelihood of a potential loss, self-risk assessments and risk maps / process flows to measure Operational Risk.

5.2.7 Quantitative Methods: A number of quantitative methods of risk measurement are also being used by the banks, consistent with the literature. These include: causal modeling, risk indicators, escalation triggers and loss-event database

5.2.8 Operational Risk Control: The study identified that policy and procedures as well as internal controls and risk reporting are some of the operational risk control measures being used by the various banks used the study in controlling operational risk. These methods are consistent with that identified in the literature.

5.3 Recommendations

Given the close linkage of operational risk with other risk types, it is very important for banks to first have a clear understanding of the concept of operational risk before designing the operational risk measurement and management framework.

The following requirements should govern the Operational Risk Management framework:

5.3.1 Comprehensive framework linked to management: A framework that explicitly monitor, manage and reports on operational risks should be established in each institution, above and beyond internal control and audit processes.

5.3.2 Board and senior management responsible and tightly involved: It is the responsibility of the Board and Senior Management to assure that the framework is implemented and managed effectively, and to actively follow results.

5.3.3 Internally audited: This framework should be periodically internally audited by internal, but operationally independent, staff.

5.3.4 Supervised by a regulatory body: Regulatory supervisors should conduct regular evaluations of an institution's policies, procedures and practices related to operational risks.

5.3.5 Under public scrutiny: The Institutions should make sufficient public disclosure to allow the market to assess their approach to operational risk management.

It is necessary for banks to employ such an enhanced, robust framework when putting quantitative methods into practice. The framework is useful because challenging issues are clearly identified on a firm-wide basis and possible solutions are pursued based on robust coordination and cooperation clearly defined among the board of directors, senior management, risk management sections and business line managers. The study therefore adopts and recommends a framework proposed by Junji Hiwatashi (2002).

A Framework for Enhancing Operational Risk Management

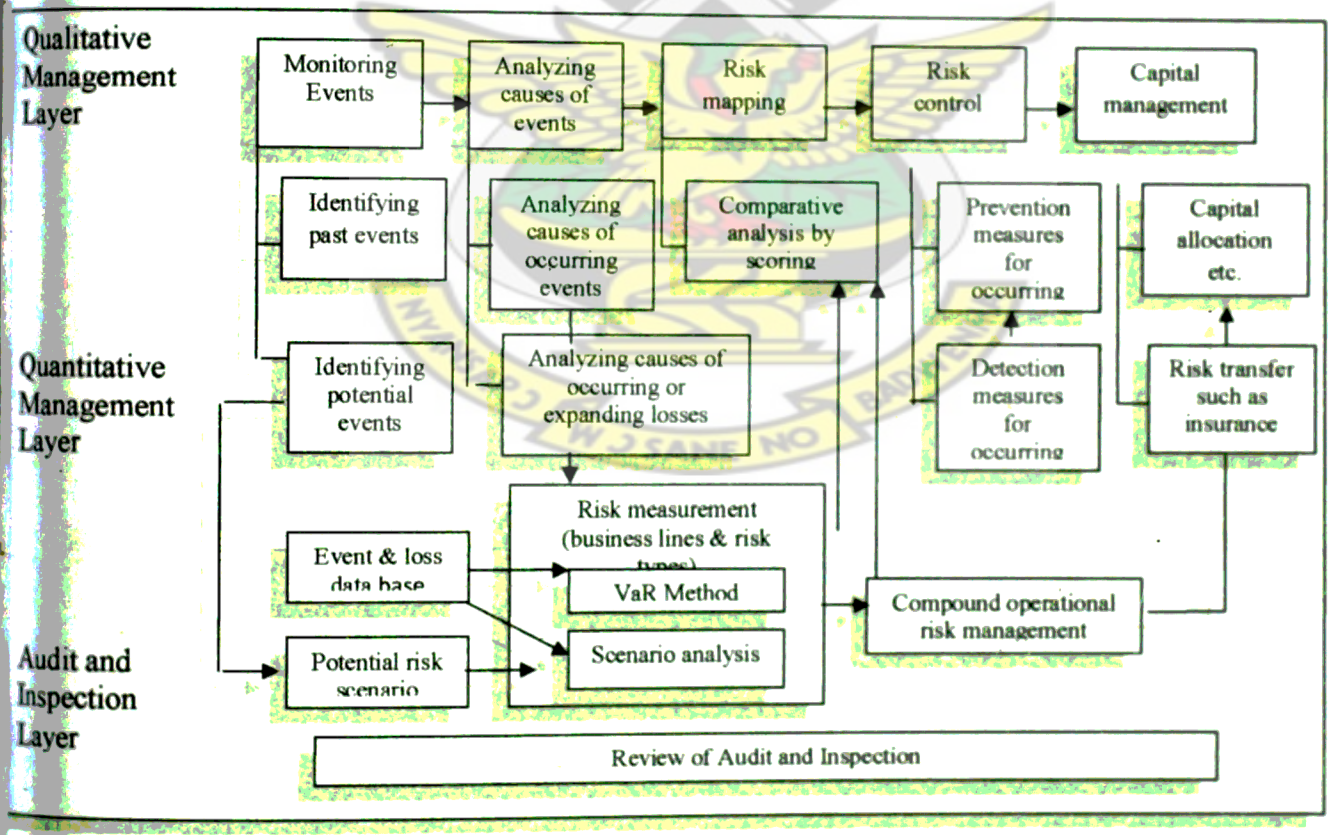


Fig 5.1 **source** Junji Hiwatashi (2002)

5.4 Recommendations for Further Studies

This long essay made a study into how operational risk is being managed in the Ghanaian banking environment. The findings as well as its implications have been discussed. However, one important proposition as far as the management of operational risks is concerned, is that put forward by the Basel Committee in its Basel II proposals. Approved in June of 2004, the Basel II Accord (officially International Convergence of Capital Measurement and Capital Standards - A Revised Framework) revised the international standards for measuring the adequacy of a financial institution's capital.

It was created to promote greater consistency in the way lenders and regulators approach enterprise risk management across national borders. The Minimum Capital Requirements section is part of the "Three Pillars" approach that seeks to improve the risk sensitivity in the way that capital requirements are calculated for each of three principal risks a financial firm faces: credit, market and operational risk.

Basel II will in one way or another touch many people working in the finance industry. Its impact is far reaching, and its effects will change the way risks are managed and communicated going forward.

This is the cutting edge in risk management and what companies and supervising authorities are focusing on. The researcher therefore proposes that a further study

is conducted into the successful adoption and use of the Basel II proposals by banks in Ghana. This will complement the Central bank's risk based supervision process, and effort at ensuring the health of financial institutions in the country, which largely has a direct bearing on the performance of the economy.

Further, Basel II is a framework for determining the capital requirement ratio of banks and other financial institutions. On the 1st of January 2007 it was introduced in 25 European countries, and national supervisory authorities are currently implementing the framework.

The strong focus on capital requirements in regulations has a very simple explanation. It is the best guarantee found so far against so-called systemic risk, i.e. the risk for uncontrolled spread of a crisis throughout the financial system. The capital buffer, or the needed level of equity for banks, should be able to absorb a temporary market crisis.

The conclusion is that a standardization of the capital requirements form one of the most efficient measures to ensure financial stability. It limits the spread of disturbances within the system - this regardless of where a bank is operating. This is the reason for the strong focus within the banking sector on implementing these requirements, and the very reason why the study recommends that banks prepare adequately to embrace these proposals that are already being used in the advanced countries.

5.5 Conclusion

It is believed that operational risk management is most effective when an institution's culture stresses strong ethical behaviour at all levels, both in words and in actual actions, starting at the top.

Operational risks when considered from the perspective of threat-events are numerous. A lot of effort is required to maintain the currency and validity of systems and mechanisms to appropriately monitor and mitigate these risks.

The Basel Committee's interest in making the New Basel Capital Accord more risk sensitive and the realization that risks other than credit and market could be substantial is an important step that will ultimately inure to the benefit of all economies because of the pivotal role financial institutions play in every economy.

As already stated, The main part of Basel II, the capital requirement regulations, is aimed at increasing the global financial stability. Ghana banks are currently being encouraged by the central bank to be positioning themselves for the adoption of the Basel proposals, which is also an important step.

Financial institutions are in the business of risk management and reallocation, and they have developed sophisticated risk management systems to carry out these tasks. The basic components of a risk management system are identifying and

defining the risks the firm is exposed to, assessing their magnitude, mitigating them using a variety of procedures, and setting aside capital for potential losses.

REFERENCE

AMD White Paper , (2007), '*Operational Risk Management*', viewed May 10 2009, enterprise.**amd**.com/downloads/.../42318a_vertwp_op**risk**mgt.pdf.

Archer, D (2002),'Creating *a Risk Management Framework*', CMA Management; Vol. 76 (1), pg.16-19.

Australian Prudential Regulation Authority (APRA), (2007), '*Draft Prudential Standard APS 115*', viewed May 3, 2009,

www.**apra**.gov.au/Policy/upload/ARP-**2007**-2008-July-**2007**.pd

Basle Committee on Banking Supervision, (1996), '*Amendment to the capital accord to incorporate market risk*', Bank for International Settlements, *viewed March 03, 2009. http://www.bis.org/publ/bcbs119.pdf*

Basel Committee on Banking Supervision, (2003), '*Operational Risk Management Working Paper on Regulatory Treatment of Operational Risk*', viewed may 03, 2009. http://*www.bis.org/publ/bcbs42.pdf*

Basel Committee on Banking Supervision, (2006), '*International Convergence of Capital Measurement and Capital Standards*', Bank for International Settlements, June 2006. Viewed May 03, 2009 *http://www.bis.org/publ/bcbs107.pdf*

Berkowitz, J (2001),'Testing *density forecasts with applications to risk management*', Journal of Business and Economic Statistics 19, 465-474.

Buchelt, R. and Unteregger, S (2004), '*Cultural risk and risk culture: operational risk after Basel II*', Financial Stability Report 6.
http://www.oenb.at/en/img/fsr_06_cultural_risk_tcm16-9495.pdf.

Chew L (1996), '*Managing Derivative Risks, The use and Abuse of Leverage*', Chichester: Wiley.

Corrigan E G (1998), '*The practice of Risk Management Implementing processes for managing firm wide Market Risk*', Euromoney Publications, London.

Carter, B, Hancock, T, Morin, J, Robins, N (1994). '*Introducing risk management methodology*', The European Project Risk Management Methodology, NCC Blackwell Ltd, Oxford.

COSO (2004), *'Enterprise Risk Management - Integrated Framework, Executive Summary, 16'*, Committee of Sponsoring Organizations of the Threadway Commission.

Creswell J. W. (2007)*'Educational Research'* Prentice Hall, viewed may 03, 2009. www.scribd.com/doc/6901541/**Creswell**-JW-et-al-**2007**

Crouhy, M. and Mark, R. (2000), *'Operational Risk, in The Professional's Handbook of Financial Risk Management'*, edited by M. Lore, and L. Borodovsky, Oxford: Butterworth Heinemann pages: 342 - 376

Davies, J., Fairless, M., Libart, S., Love, J., O'Brien, D., Slater, P., & Shepherd Washington, T (1998), *'Defining and Aggregating operational risk information in operational risk and financial institution'*, edited by Robert Jameson. London: Risk Books

Frame J D (2003), *'Managing Risks in Organisations: A Guide for Managers'*, Jossey Bass, San Francisco

FRBSF Economic Letter, (2002), 'What *is operational risk*' Number 2002-02, January 25, 2002, viewed June 02, 2009.
www.**frbsf**.org/.../**economics/letter/2002/el2002-02**.htm

Freeman, A (1999) *'Strategic risk management: lessons from the 1990*'s', London: The economist intelligence unit UK, viewed July 07 2009.

www.tbs-sct.gc.ca/.../**RiskManagement**/annbiblio2_oct99-eng.asp

Frost, C., Allen, D, Porter, J, Bloodworth, P (2001), Operational risk and resilience: understanding and minimizing operational risk to secure shareholder value, Butterworth Heinemann, Oxford.

Geiger H (2000), *'Regulating and Supervising Operational Risk for Banks'*, viewed March 08, 2009.
www.isb.uzh.ch/publikationen/pdf/workingpapernr26.pdf

Goldman, Sachs & Co and Swiss Bank Corporation (1998), *'The practice of risk management, implementing processes for managing firm wide market risk'*, edited by E.R Corrigan, London: Euromoney Books

Gunilla D 2007, *'Implementing the operational risk framework of Basel II at a Swedish financial institution – A case study, Stockholm School of Economics'*, Sweden, viewed February 03, 2009.

https://studentweb.hhs.se/courseweb/.../Old_Theses.htm.
Hillson D, & Raz, T. (2005), '*A Comparative Review of Risk management Standards, Risk Management*' An International Journal, 7(4): 35-66

Hoffman, D. G. (1998), '*New Trends in Operational Risk Measurement And Management In Operational Risk and Financial Institutions*', edited by Robert Jameson. London: Risk Books

Jallow A. K. (2006), '*Development of a Business Process Risk Assessment Framework for Service Provision*', Cranfield University, viewed January 10 2009 www.springerlink.com/index/12402573R2466211.pdf.

Janakiraman U. (2008), '*Operational Risk Management In Indian Banks In The Context Of Basel Ii: A Survey Of The State Of Preparedness And Challenges In Developing The Framework*', Asia Pacific Journal of Finance and Banking Research Vol. 2. No. 2. 2008, viewed March 29, 2009.
globip.com/pdf_pages/**asiapacific-vol2**-article3.pdf.

Junji Hiwatashi (2002), '*Solutions on Measuring Operational Risk*, Capital Market News, Federal Bank of Chicago, September 2002, viewed April 02, 2009.
www.boj.or.jp/en/type/ronbun/ron/wps/.../fwp00e01.htm

Knechel R. (2002), '*The Role of the Independent Accountant in Effective Risk Management*', Journal of Economics Management, Pg 65–6 8.

Kendrick, T. (2003). Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project, Amacom, New York.

Knight, F.H. (1981). Risk, uncertainty and profit, Houghton Miffin, Boston, Massachusetts.

Lebransky B. (2008), '*Australian Banking Perspective on Managing Operational Risk*', Training Program, Shanghai, China National Australia Bank, viewed January 23 2009. www.apec.org.au/docs/08_TP_BRM/6.4_**LeBransky**.pdf

Link, P, Marxt, C. (2004), '*Integration of risk – and chance management in the co-operation process*', International Journal of production Economics, Vol. 90, Pg. 71-78.

Malhotra, N. K. (2004), '*Marketing research: an applied orientation*', Upper Saddle River, NJ: McGraw-Hill, cop.

Moody's Investor Service (2003), *'Moody's Analytical Framework For Operational Risk Management Of Banks'*, viewed February 02, 2009. www.gloriamundi.org/picsresources/maf.pdf

Moosa, I. A. (2007), *'Misconceptions about operational risk*, Journal of Operational Risk, Vol. 1, No. 4, pp. 97-104.

Neuman, W. L. (2003), *'Social Research Methods- Qualitative and Quantitative Approache*,. Boston: Pearson Education Inc.

Oates, Wallace E. *(2005). "Property taxation and local public spending: the renter effect,"* Journal of Urban Economics, Elsevier, vol. 57(3)

Pitinanondha (2008), *'Operational Risk Management Systems – An Australian Study*, University of Technology Sydney, Australia, viewed May 03 2009. epress.lib.**uts**.edu.au/dspace/bitstream/2100/600/1/01.front.pdf

Raftery J (1994), *'Risk Analysis in Project Management'*, E & FN Spon, London.

Scandizzo, S. (2005), *'Risk Mapping and Key Risk Indicators in Operational Risk Management. Economic Notes by Banca monte dei Paschi di Siena SpA*, Vol. 34, (2) Pg. 231-256.

Stoll, S (1996), 'Why *risk management must be integrated*, American banker, 161(152), august: 18.

Suh, B. Han I. (2003), *'The IS risk analysis based on a business model: Journal of Information and Management'*, Vol. 41, Pg. 149-158.

Venkat S. (2000), *'Implementing a firmwide risk management framework in the professonal's handbook of risk management'*, edited by M. Lore & L. Borodovsky. Oxford Butterworth Heinemann.

Williams, D. L. (2000), *'Selecting and implementing enterprise risk management technologies in the professonal's handbook of financial risk management*, edited by M. Lore & L. Borodovsky. Oxford Butterworth Heinemann.

Wilson, D. (2000), 'Operational *risk in the professional's handbook of financial risk management'*, edited by M. Lore & L. Borodovsky. Oxford Butterworth Heinemann.

Yin, R.K. (2003), '*Case study research: design and methods'*, Thousand Oaks, Calif: Sage Publications cop.

Young J (2001), 'A *Structured Approach to Operational Risk Management in a Banking Environment'*, University of South Africa. South Africa, viewed January 28, 2009. etd.unisa.ac.za/ETD-db/theses/available/etd-02152007.../thesis.pdf

APPENDIX 1

This questionnaire aims at knowing the key operational risks faced by the bank and to understand how these may impact upon the quality and stability of its earnings, and establish best practices to operational risk management in banks that should be pursued by your institution based on modern practices and your experience and knowledge.

Kindly tick your answer by selecting appropriately from the various options given below:

Section 1: Personal information

1 Indicate your specific portfolio

Risk manager	
Line manager	
Internal auditor	
Operational risk manager	
Other(specify)	

2 Indicate your number of years of practical banking experience

1-3 years	
4-6 years	
7-9 years	
10-12 years	
More than 13 years	

Section 2: Background

Please answer the following questions by ticking your answer according to the scale below:

1 Strongly Disagree 2 Disagree 3 Neutral 4 Agree 5 Strongly Agree

	1	2	3	4	5
1 Your institution has adopted a specific definition for Operational Risk.					

2 Your institution has a risk profile document covering such matters as:	1	2	3	4	5
Corporate governance, culture and ethics					
Strategy, flexibility and earnings stability					

Organisation structure for risk management					
Systems and procedures					
Contingency plans					
Fraud, corruption and financial crime					
Audit and compliance					
Competency and key skills development					
Outsourcing (including insurance)					

3 Your institution realizes the following benefits from its operational risk management	1	2	3	4	5
A lower regulatory capital requirement					
Reduced losses (due to speed of response, actions & oversight, etc.)					
Lower insurance premiums (from improved risk environment)					
Improved share price					
Improved prioritisation and targeting of resources					
Pricing improvements (ability to price risk more accurately)					
Lower cost of finance					
Improved quality and stability of earnings					
Enhanced competitive position					
Improved probability of survival					

4 The following are major limitations to your institution's operational risk management:	1	2	3	4	5
Limited budget					
Difficulty in demonstrating cost-benefit analysis					
Current economic climate, resulting in a concentration on cost-cutting					
Lack of skilled or professionally qualified people					
Bureaucratic organisation structure					
Inappropriate approach by Group Risk					
Technology and infrastructure problems					
Lack of common definitions and categories					
No clear group-wide approach					

5 The following are rated as primary risk types within your institution.	1	2	3	4	5
Credit risk					
Market risk					
Liquidity risk					
Interest rate risk					
Country risk					
Reputational risk					
Legal risk					
Operational risk					

6 Your institution recognizes the following people exposures as an important driving force of operational risk.

	1	2	3	4	5
incompetence					
negligence					
Human error					
Low moral					
High staff turnover					
Fraudulent activities by employees					
Lack of training					

7 Your institution recognizes the following process exposures as an important part of operational risk.

	1	2	3	4	5
Errors in procedures					
Execution errors					
Documentation errors					
Product complexity					
Security risks					

Other:

8 Your institution recognizes the following system exposures as an important part of operational risk.

	1	2	3	4	5
System infiltration					
System failures					
fraud					
Programming errors					
information risk					
Obsolescence of systems					

9 Your institution recognizes the following external exposures as an important part of operational risk.

	1	2	3	4	5
Acts of God					
External criminal activities					
Regulator and compliance					
Legal actions					
Business environment changes					
strikes					
Money laundering					

10 Your organization recognizes the following as important elements of an operational risk management process.

	1	2	3	4	5
Risk identification					
Risk evaluation/measurement					
Risk control					
Risk financing					

11 Your institution uses the following tools and techniques in relationship to operational risk	1	2	3	4	5
Control Risk Self-Assessment					
Score cards					
Key Performance Indicators and Key Risk Indicators					
Loss data collection and analysis					
Extreme Value Theory					
Value at Risk					
Risk-Adjusted Return On Capital					
Event-Cause-Effect Analysis					
Stress Testing & Scenario Analysis					
Bayesian Belief Networks					
Quality and Stability of Earnings					

12 Your organization recognizes the importance of aligning an operational risk management process with its strategy.	1	2	3	4	5

13 Your institution has recognized the importance of and implemented the following qualitative methods to measure OR.	1	2	3	4	5
Historical data to forecast the likelihood of a potential loss					
Self-risk assessments					
Risk maps /process flows					

Other:

14 Your institution has recognized the importance of and implemented the following quantitative methods to measure OR.	1	2	3	4	5
Causal modeling					
Risk indicators					
Escalation triggers					
Loss-event database					

Other:

15 Your institution has recognized the implementation of risk identification as an important ongoing process.	1	2	3	4	5

Other:

16 Your institution has recognized the importance of and implemented the following control measures of OR.

	1	2	3	4	5
Policy and procedures					
Internal controls					
Risk reporting					

Other:

	1	2	3	4	5
17 Your institution has established a separate operational risk management structure.					
18 Your institution involves internal audit to manage operational risk.					
19 Your institution involves business managers in an operational risk management process?					

	1	2	3	4	5
20 Your institution recognizes the importance of and implements the following risk financing techniques:					
Risk transfers					
Risk retention (funded)					
Risk retention (unfunded)					

Other:

	1	2	3	4	5
21 Your institution has been involved in determining a regulatory capital allocation for operational risk.					

22 Your institution has recognized and evaluated the following Basel approaches to assess capital for operational risk.	1	2	3	4	5
Basic Indicator Approach					
Standardised Approach					
Internal Management Approach					

Other:

	1	2	3	4	5
23 Your institution regards the allocation of a regulatory capital for operational risk proposed by the Basel Committee as essential					

Section 3: recommended practices

1 Your bank should manage the following as primary risk types within your organization.

	1	2	3	4	5
Credit risk					
Market risk					
Liquidity risk					
Interest rate risk					
Country risk					
Reputational risk					
Legal risk					
Operational risk					

Other:

2 Your bank should regard the following as primary factors of operational risk management.

	1	2	3	4	5
people					
processes					
systems					
External factors					

Other:

3 Your bank should manage the following people exposures as part of operational risk.

	1	2	3	4	5
incompetence					
negligence					
Human error					
Low moral					
High staff turnover					
Fraudulent activities by employees					
Lack of training					

Other:

4 Your bank should manage the following process exposures as part of operational risk.

	1	2	3	4	5
Errors in procedures					
Execution errors					
Documentation errors					
Product complexity					
Security risks					

Other:

5 Your bank should manage the following system exposures as part of operational risk.

	1	2	3	4	5
System infiltration					
System failures					
fraud					
Programming errors					
information risk					

telecommunication risk					
Obsolescence of systems					

Other:

6 Your bank should manage the following external exposures as part of operational risk.	1	2	3	4	5
Acts of God					
External criminal activities					
Regulator and compliance					
Legal actions					
Business environment changes					
strikes					
Money laundering					

Other:

7 Your bank should implement a formal risk management process?					

8 Your bank should adopt a formal definition for operational risk?					

9 Your bank should regard the implementation of the following elements of an operational risk management system as important.	1	2	3	4	5
Risk identification					
Risk evaluation/measurement					
Risk control					
Risk financing					

	1	2	3	4	5
10 Your bank's management process should be aligned with its strategy and objectives.					

11 Your bank's OR mgt. process should be regarded as an important and integral part of overall mgt. process.					

12 Your bank should recognize the importance of the following methods to identify various risk type.	1	2	3	4	5
workshops					
brainstorming					
questionnaires					
process mapping					
Comparisons with other organizations					
Discussion with peers					

13 Your bank should recognize and implement the following qualitative methods to measure OR.	1	2	3	4	5
Historical data to forecast the likelihood of a potential loss					
Self-risk assessments					
Risk maps /process flows					

14 Your bank should recognize and implement the following quantitative methods to measure OR.	1	2	3	4	5
Causal modeling					
Risk indicators					
Escalation triggers					
Loss-event database					

Other:

15 Your bank should recognize the importance and manage OR as an ongoing process	1	2	3	4	5

16 Your bank should recognize and implement the following control measures of OR	1	2	3	4	5
Policy and procedures					
Internal controls					
Risk reporting					

Other:

17 Your bank should establish a separate operational risk management structure.	1	2	3	4	5

18 Internal audit should be involved and responsible for operational risk management of your bank.	1	2	3	4	5

19 Business managers should be involved in an operational risk management process.	1	2	3	4	5

20 Your bank should recognize the importance and implement the following risk financing techniques.	1	2	3	4	5
Risk transfers					
Risk retention (funded)					
Risk retention (unfunded)					

Other:

21 Your bank should be involved in determining a regulatory capital allocation for operational risk.	1	2	3	4	5

22 Your bank should recognise and implement the following Basel approaches to assess capital for OR.	1	2	3	4	5
Basic Indicator Approach					
Standardised Approach					
Internal Management Approach					

Other:

	1	2	3	4	5
23 Your bank should recognise the importance and necessity to implement a minimum capital requirement for operational risk.					

Any other comment

.....
.....
.....
.....
.....
.....

APPENDIX 2

Operational risk management standards and guidelines

Table 1.1

Reference/title	Author	Date	ORM coverage
National & International standards			
AS/NZS 4360:2004, Risk Management	Standards Australia and Standards New Zealand	2004	All
HB436:2004, Risk Management Guideline companion to AS/NZS 4360:2004	Standards Australia and Standards New Zealand	2004	All
AS/NZS 4801:2001, Occupational Health and Safety Mgt. Systems – specification with Guidance for use	Standards Australia and Standards New Zealand`	2004	Safety risks
CAN/CSA-Q850-97, Risk Management Guideline for Decision Makers	Canada Standards Assoc	1997	All
ISO 9001:2000, Quality Mgt. Systems-Requirements	International Org. for Standardization	2000	Quality risks
ISO 14001:2004, Environmental Mgt. Systems - Requirements with Guidance for use	International Org. for Standardization	2004	Environmental risks
ISO/IEC 17799:2005, Information Technology – Security Techniques – code of practice for information Security Management	International Org. for Standardization and International Electro-technical Commission	2005	IT risks
JIS Q 2001:2001 (E), Guidelines for Development and Implementation of Risk Management System	Japanese Standards Association	2001	All
Professional standards/guidelines			
A Risk Management	Institute of Risk Mgt.	2002	All

Standard	(IRM), Association of Insurance and Risk managers (AIRMIC) and National Forum for Risk Mgt. in Public Sector(ALARM), UK		
Enterprise Risk Management – Integrated Framework	The committee of sponsoring Orgs. of the Treadway Commission (COSO), USA	2004	All
New Basel Capital Accord – Consultative Document	Basel Committee on Banking Supervision, Switzerland	2001	All

Source: Thitima Pitinanondha (2008)

APPENDIX 3

Table: 2.5.2 operational risk causes and events

Causes	events
People/employees	Errors, Misdeeds, Employment law, employer's liability, loss of key staff, organizational structure, corporate governance, wrongful trading
Customer relationships	Client suitability, client capacity/ultra vires, client powers/authority to transact, money laundering
Technology	System failure, system integrity, system age, system suitability, system support, system conformance to corporate standards, model risk, data quality
Assets	Business interruption, asset loss, third party theft, fraud
Regulators/suppliers	Legal risk, compliance with standards, changes in regulatory standards, suppliers 'failure'
Other	Project risk, reputation risk

Source: Laycock (1998:132)

Table: 2. 10.2 Operational Risk Monitoring

	Head office	Business unit
Area	Measures	measures
Human resources	Temporary help Turnover Tenure Management development versus plan	Temporary help Turnover Training budget versus actual Vacation absence
Business	Audit scoring Audit expectations Audit points outstanding Customer complaints	Audit score Customer satisfaction rating Audit points outstanding Customer complaints
IT	System downtime Number of system problems	System downtime Number of system problems
Operations	Physical losses Accounting losses Number of errors Unreconciled accounts	Settlement failures Accounting losses Number of errors Unreconciled accounts Income statement adjusstments Evaluation losses Aged confirmations

Source: PwC (1999)

APPENDIX 4

Table 2.10.3 Operational risks mapped to mitigating factors

Primary source of operational risk	Mitigating systems and controls
Inexperienced, incompetent, unsuitable, negligent and maverick staff	Recruitment procedures, job descriptions, training programmes, disciplinary and appraisal procedures. Compliance at an individual level through training and information. Compliance checks, active management
Working culture creating low morale, high staff turnover, poor concentration, low productivity and industrial action	Competitive pay regime, performance-related pay, career planning, responsive management, line of communication, working environment, disciplinary and appraisal procedures.
Fraud and theft	Segregation of duties, compliance culture, checking procedures and reporting lines. IT and physical security. Supportive culture, Good pay structure with reduced emphasis on performance related pay. Recruitment procedures and holiday policy. Regular internal audit, insurance.
Human error	Checking procedures, segregation of duties and IT systems
Unauthorized and ill-informed decision making at all levels, particularly with regard to business strategy, project management, liquidity and outsourcing.	Lines of authority, reporting lines, breach procedures, Research and market information from IT systems, the internet and up to date libraries, consultation at all levels with both internal and external experts, project management.
Errors in information systems	Up-to-date virus and error free technology, detection systems and limited access for personnel, regular back-ups and protected records, manual copies of essential information, consulting from internal and external experts to ensure that suitable software packages are used, training at all levels.
System failure	Up-to-date virus and Up-to-date virus and error free technology, , regular back-ups and protected records, manual copies of essential information,
System infiltration	Firewalls and regularly altered access codes, error-free software, consultation from internal and external experts, daily account reconciliation and other detection methods.
Acts of God	Insurance, contingency planning, emergency procedures and training
External criminal activities	Security systems, emergency procedures and training, ethical or non-political business strategies, insurance.
Domestic political upheaval	Contingency planning
Regulatory, legal, tax and business environment	Contingency planning, business strategy, internal experts and competent external advisors, flexibility, research, preparation and diversification.
Third parties	Monitoring, reporting lines and regular reviews of contracts, legal protection, business and contingency planning, market research.
Reputational deterioration	Strong individual reputation to protect in event of sectoral deterioration, contingency planning and business strategy, market awareness

Source: FSA (1999:22)

APPENDIX 5

LIST OF BANKS USED IN THE STUDY

1. Barclays bank, Ghana
2. ADB
3. Amalgamated bank, Ghana
4. Cal bank
5. Ecobank, Ghana
6. Fidelity bank, Ghana
7. Ghana Commercial Bank
8. HFC bank, Ghana
9. Intercontinental bank, Ghana
10. International Commercial bank
11. Merchant bank, Ghana
12. National Investment Bank, Ghana
13. Prudential bank, Ghana
14. Stanbic bank , Ghana
15. Standard chartered Bank, Ghana
16. The Trust bank, Ghana
17. Unibank, Ghana
18. United bank for Africa, Ghana
19. Zenith bank, Ghana
20. SG-SSB limited, Ghana