

**OPERATIONAL RISK EVENTS IN BANKS AND PRACTICES FOR
COLLECTING INTERNAL LOSS DATA**

A Research Report

presented to the

Graduate School of Business Leadership

University of South Africa

In partial fulfilment of the

requirements for the

MASTER'S DEGREE IN BUSINESS LEADERSHIP,

UNIVERSITY OF SOUTH AFRICA

by

D E BOSTANDER

Student number 3112-057-1

30 November 2007

TABLE OF CONTENTS

1.	CHAPTER ONE: ORIENTATION	1
1.1	INTRODUCTION.....	1
1.2	RESEARCH OBJECTIVES.....	2
1.3	RESEARCH PROBLEM	4
1.4	SUB-PROBLEMS	5
1.5	GLOSSARY OF TERMS	6
1.6	DELIMITATIONS	10
1.7	IMPORTANCE OF STUDY	12
1.8	BENEFITS OF STUDY	14
1.9	CONTRIBUTION OF STUDY TO EXISTING BODY OF KNOWLEDGE	15
1.10	OUTLINE OF RESEARCH REPORT	16
2.	CHAPTER TWO: FOUNDATION OF STUDY	18
2.1	INTRODUCTION.....	18
2.2	HISTORY OF REGULATORY CAPITAL	18
2.3	BANKING REGULATION IN SOUTH AFRICA.....	20
2.4	RISKS FACED BY BANKS.....	22
2.5	SOUTH AFRICAN BANKING SYSTEM	25
3.	CHAPTER THREE: LITERATURE REVIEW.....	27
3.1	DEFINING OPERATIONAL RISK.....	27
3.2	CLASSIFICATION OF OPERATIONAL RISK LOSSES BY THE BASEL COMMITTEE ON BANKING SUPERVISION	29
3.3	EXPECTED AND UNEXPECTED OPERATIONAL RISK LOSSES.....	32
3.4	OPERATIONAL RISK ASSESSMENT	34
3.5	EFFECT OF OPERATIONAL RISK LOSSES ON BANKS.....	37
3.6	BENEFITS OF OPERATIONAL RISK MANAGEMENT	39
3.7	MEASURING OPERATIONAL RISK FOR CAPITAL PURPOSES	41
3.8	INTERNAL LOSS DATA.....	46
3.9	AMBIGUITY OF PRACTICES FOR COLLECTING INTERNAL LOSS DATA	48
3.10	READINESS OF THE BANKING SECTOR	51
3.11	SHIFT IN CULTURE.....	52
3.12	SUMMARY	54
4.	CHAPTER 4: RESEARCH METHODOLOGY	56
4.1	INTRODUCTION.....	56
4.2	GENERAL RESEARCH METHODOLOGY	57
4.3	POPULATION AND SAMPLE	58
4.4	MEASURING INSTRUMENT	59

4.5	DATA COLLECTION	59
4.6	DATA ANALYSIS METHODS	60
4.7	LIMITATIONS	60
5.	CHAPTER 5: RESEARCH RESULTS.....	61
5.1	BIOGRAPHIC PROFILE OF RESPONDENTS.....	62
5.2	DESCRIPTIVE STATISTICS OF LIKEY SEVERE EVENTS	66
5.3	LIKELY FREQUENCY OF OPERATIONAL RISK EVENTS	76
5.4	LOSS DATA COLLECTION PRACTICES.....	85
6.	CHAPTER 6: DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS.....	93
6.1	DISCUSSION OF RESULTS: LIKEY SEVERE OPERATIONAL RISK LOSSES IN SOUTH AFRICAN BANKS.....	94
6.2	CONCLUSION AND RECOMMENDATION: LIKEY SEVERE OPERATIONAL RISK LOSSES IN SOUTH AFRICAN BANKS.....	97
6.3	DISCUSSION OF RESULTS, CONCLUSIONS AND RECOMMENDATIONS: RANGE OF PRACTICES IN COLLECTING INTERNAL LOSS DATA FOR OPERATIONAL RISK.....	98
7.	LIST OF REFERENCES	104
8.	APPENDICES	111
8.1	APPENDIX A – SUPERVISORY REVIEW PROCESS OF THE BANK SUPERVISION DEPARTMENT.....	111
8.2	APPENDIX B - QUESTIONNAIRE.....	112
8.3	ARTICLE FOR PUBLICATION.....	120

LIST OF FIGURES

- Figure 1: South African banking sector
- Figure 2: Likelihood/impact chart
- Figure 3: Regulatory approaches for operational risk
- Figure 4: Histogram – respondent distribution
- Figure 5: Frequency distribution: banking experience
- Figure 6: Operational risk experience of respondents
- Figure 7: Mean distribution – likely severity of loss event types
- Figure 8: Mean distribution – likely severe events in business lines
- Figure 9: Mean distribution – likely frequency of loss event types
- Figure 10: Mean distribution – likely frequency of events in business lines
- Figure 11: Inclusion of near misses in loss database
- Figure 12: Recording of opportunity cost in loss database
- Figure 13: Recording of overtime cost in loss database
- Figure 14: Date of recording of operational risk losses
- Figure 15: Assignment of internal losses to business units
- Figure 16: Recording of insurance recoveries
- Figure 17: Recording of other recoveries
- Figure 18: Damage to fixed assets
- Figure 19: Assignment of market risk losses due to operational risk events
- Figure 20: Assignment of loan-related operational risk losses
- Figure 21: Loss data collection threshold
- Figure 22: Mapping matrixes
- Figure 23: Mapping of data on consolidated or legal entity basis
- Figure 24: Mapping of gross income

LIST OF TABLES

Table 1:	Assets of four largest banks as at 31 March 2007
Table 2:	Market share of core advances
Table 3:	Biographic profile of respondents
Table 4:	Descriptive statistics: likely severe operational risk losses – loss event types
Table 5:	Distribution of ratings: likely severity of ‘internal fraud’
Table 6:	Distribution of ratings: likely severity of ‘external fraud’
Table 7:	Distribution of ratings: likely severity of ‘employment practices and workplace safety’
Table 8:	Distribution of ratings: likely severity of ‘client, products and business practices’
Table 9:	Distribution of ratings: likely severity of ‘damage to physical assets’
Table 10:	Distribution of ratings: likely severity of ‘business disruptions and system failures’
Table 11:	Distribution of ratings: likely severity of ‘execution, delivery and process management’
Table 12:	Descriptive statistics: likely severe operational risk losses - business lines
Table 13:	Distribution of ratings: likely severity – corporate finance
Table 14:	Distribution of ratings: likely severity – trading and sales
Table 15:	Distribution of ratings: likely severity – retail banking
Table 16:	Distribution of ratings: likely severity – commercial banking
Table 17:	Descriptive statistics: likely frequency of operational risk losses – loss event types
Table 18:	Distribution of ratings: likely frequent events – internal fraud
Table 19:	Distribution of ratings: likely frequent events – external fraud
Table 20:	Distribution of ratings: likely frequent events – employment practices and workplace safety
Table 21:	Distribution of ratings: likely frequent events – clients, products and business practices

- Table 22: Distribution of ratings: likely frequent events – damage to physical assets
- Table 23: Distribution of ratings: likely frequent events – business disruptions and system failures
- Table 24: Distribution of ratings: likely frequent events – execution, delivery and process management
- Table 25: Descriptive statistics: likely frequency of operational risk losses – business lines
- Table 26: Distribution of ratings: likely frequent events – corporate finance
- Table 27: Distribution of ratings: likely frequent events – trading and sales
- Table 28: Distribution of ratings: likely frequent events – retail banking
- Table 29: Distribution of ratings: likely frequent events – commercial banking
- Table 30: Distribution of ratings: likely frequent events – payment and settlement

1. CHAPTER ONE: ORIENTATION

1.1 INTRODUCTION

Banks play an important role in the economy. They act as the main intermediaries between depositors that have excess funds available and those individuals that require credit from banks. To ensure that depositor funds are safe, banking regulators require that banks keep adequate levels of capital and reserves as a buffer against any losses that may arise within the banking institution.

In 1988 the first rules for banks to hold minimum capital against credit risk were issued by the Basel Committee on Banking Supervision (BCBS). These rules were commonly known as Basel I capital rules. Subsequent to 1988, the BCBS made amendments to the Basel I rules in 1996 to cater for the minimum capital requirements for market risk.

However, a number of operational risk losses over the past two decades had resulted in several bank failures, both internationally and in South Africa. This led to an increased focus on operational risk by financial regulators and banks.

1.2 RESEARCH OBJECTIVES

- a) The purpose of determining in which areas in South African banks the most severe operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines) was to:
- determine the high-risk areas that the Bank Supervision Department (BSD) of the South African Reserve Bank (responsible for the supervision of banks in South Africa), should focus on in their supervisory duties relating to operational risk,
 - provide guidelines to the boards of directors and senior management of banks regarding what areas of operational risk to focus their attention on to reduce losses resulting from operational risk events. The findings of the study will also indicate to banks which areas need strengthening in internal controls to reduce operational risk events, and.
 - indicate to senior management of banks in which business areas these operational risk losses are likely to occur.
- b) The research objectives relating to the practices for capturing internal loss data for operational risk purposes outlined below were taken directly from the research conducted by the Accord Implementation Group Operational Risk, but were adapted for this study to be relevant to South Africa. Similar to those objectives indicated in the *'Observed Range of Practice in Key Elements of the Advanced Measurement Approaches'* (*Observed Range of Practices for AMA*) issued by the Basel Committee on Banking Supervision (BCBS) in October 2006, the objectives of this research were the following:
- To conduct a “benchmarking exercise” among all South African banks to determine how internal loss data are being captured for operational risk purposes (Basel Committee on Banking Supervision, 2006b: 1).
 - To provide the BSD with “a means of framing the discussion of acceptable practice in both the management and measurement of operational risk” (Basel Committee on Banking Supervision, 2006b: 2).

“The results will be a valuable resource for both banks and the BSD to use in their respective implementation of Basel II processes” (Basel Committee on Banking Supervision, 2006b: 2).

1.3 RESEARCH PROBLEM

The purpose of this study was to determine the areas in South African banks in which the most *severe operational risk losses are likely to occur*, and to assess *the range of practices in collecting internal loss data for operational risk purposes* as required by the International Convergence of Capital Instruments and Capital Measurement Standards – A Revised Framework issued in June 2006 (better known, and referred to hereafter, as Basel II).

The study also assessed the prudence of internal loss data collection practices in relation to sound operational risk management practices and recommendations were made where appropriate. The soundness of operational risk practices was approached from a qualitative perspective, by benchmarking the research findings against the Basel II text, the Basel Committee on Banking Supervision's *Sound Practices for the Management and Supervision of Operational Risk*, and related literature.

1.4 SUB-PROBLEMS

In assessing in which areas in South African banks the most severe operational risk losses are likely to occur, the following sub-problems were addressed:

- a) Determining in which areas the most *severe* operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).
- b) Determining in which areas the most *frequent* operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).

In assessing the range of practices in collecting internal loss data for operational risk, the following current issues related internal loss data collection practices were assessed:

- c) Determining the appropriate gross loss amounts used for capturing operational risk losses within the internal loss database.
- d) Determining the range of practices of banks in using gross thresholds for collecting internal loss data.
- e) Determining whether near misses are recorded in internal loss databases of banks.
- f) Determining the range of practices for when operational risk losses are recognised (recognition dates) and captured in internal loss databases of banks.

1.5 GLOSSARY OF TERMS

Accord Implementation Group Operational Risk (AIGOR)

“A permanent working group of the Group of 10 countries (G-10), including Australia, Brazil, India and South Africa, focusing on operational risk-implementation issues regarding Basel II” (South African Reserve Bank, 2007a).

Advanced Measurement Approach

Refer to section 3.7 on page 43

Basel Committee on Banking Supervision (BCBS)

The brief description of the BCBS below was from taken the website of the BCBS (Basel Committee on Banking Supervision, 2007).

“The BCBS was established by the central-bank governors of the G-10 countries (G-10) at the end of 1974 in the aftermath of serious disturbances in international currency and banking markets (notably the failure of Bankhaus Herstatt in West Germany).

Countries are represented by their central banks and also by the authorities with formal responsibility for the prudential supervision of banking business where this is not the central bank. The BCBS provides a forum for regular co-operation between its member countries on banking supervisory matters”.

Bank Supervision Department (BSD)

The BSD is a department within the South African Reserve Bank. The purpose of the BSD is to achieve a sound, efficient banking system in the interest of the depositors of banks and the economy as a whole (South African Reserve Bank, 2007b).

Basic Indicator Approach

Refer to section 3.7 on page 42

Economic capital

Economic capital acts as a buffer against losses arising from a bank's business operations. Economic capital is bank specific and refers to a bank's internal assessment of risk and capital usage, while regulatory capital is based on standard principles for all banks (Mueller & Siberon, 2004).

Internal loss data

Internal loss data are particular to a specific institution. Internal loss data are obtained from a bank's actual historical losses and near misses of operational risk events.

Loss event database

A loss event database captures operational loss events across business and risk types (Young, 2006).

Market capitalisation

The listed market price of an individual share multiplied by the total number of shares in issuance.

Near misses

Near misses are operational risk events that almost occurred, but were prevented by some form of intervention.

Operational risk

“The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” (Basel Committee on Banking Supervision, 2006a: 144). This definition includes legal risk, but excludes strategic and reputational risk (Basel Committee on Banking Supervision, 2006a: 144).

Reputational risk

Reputational risk refers to any negative perceptions that the public, depositors, other banks, market participants and investors may have of a bank’s liquidity position and its business operations. As the concept of a bank is built on trust, any negative perceptions could lead to large withdrawals of deposits or payment of additional premium for attracting deposits from the public compared to better-perceived banks.

Run on a bank

‘A run’ on a bank refers to the large withdrawals of deposits by both institutional and retail depositors, mainly due to a breakdown in confidence and trust from depositors who do not regard their deposits as safe in that specific institution.

Standardised Approach

Refer to section 3.7 on page 42

1.6 DELIMITATIONS

The researcher focused on practices for capturing internal loss data for operational risk purposes within registered banks in South Africa and did not focus on internal loss data for other risk areas such as credit risk. Internal loss data and internal loss data collection practices are particular to a specific institution and are based on and obtained from a bank's actual historical losses and near misses of operational risk events. The research did not include the use of external data and its collection practices for identifying, measuring and monitoring operational risk.

This research focused on all banks registered with the BSD to conduct the business of a bank (involved in deposit-taking-activities). The research did not only focus on the banks making use of the advanced measurement approach (AMA) to calculate their operational risk capital. The researcher acknowledge that banks that have decided to adopt the standardised approach (TSA) or even the basic indicator approach (BIA) in January 2008, would already have started to collect internal loss data to either migrate to the AMA at a later stage, or to use the internal loss database to identify and manage operational risk losses.

The researcher recognised the work already performed by the AIGOR in a similar study to determine the range of practices for capturing internal loss data for operational risk purposes across jurisdictions of the Basel Committee on Banking Supervision (BCBS) member countries. A paper issued by the BCBS in October 2006 titled Observed Range of Practices for AMA has been consulted. The aforementioned study by the AIGOR excluded South African banks and the results from this research were not reflected in the study performed by the AIGOR.

This study did not engage in what constitutes best practices but did provide the range of practices currently been applied within the banking sector. The

researcher also assessed whether certain practices, irrespective of whether the majority of respondents apply them, constitute acceptable operational risk management.

1.7 IMPORTANCE OF STUDY

a) Operational risk management: The new science

Operational risk will for the first time attract a capital charge, and will form part of the capital calculations of banks in South Africa from 1 January 2008. Operational risk is not new to banks and other financial institutions, but operational risk management, and specifically the measurement thereof, is a new science.

b) Stability of the South African banking system

Unsound practices for measuring and managing operational risks could ultimately lead to lower levels of regulatory capital in the banking system and could pose a threat to the stability and soundness of the banking system. The banking system of South Africa is the pulse of the economy, and its contribution to the gross domestic product of South Africa is significant.

As at 31 March 2007, more than one hundred and twenty nine thousand people were employed within the South African banking system (South African Reserve Bank, 2007c). The failure of one large bank could have systemic implications and could result in many employees becoming unemployed.

This study includes a survey to banks to determine in which areas in South African banks the most severe operational risk losses are likely to occur. This will clearly indicate to the BSD what the main concerns of operational risk managers in banks are, and where to concentrate its supervisory efforts for operational risk. The BSD could thereafter, if it wishes, request banks to indicate which internal controls and mitigating procedures they have in place to prevent the loss events from recurring.

This study focuses on determining what acceptable practices within South African banks are for capturing internal losses for operational risk. The broad guidance provided by the BCBS on the collection and capturing of internal loss data for operational risk purposes could also lead to banks using methods for collecting internal loss data that would reduce the capital charge for operational risk instead of using more prudent methods to ensure sound operational risk management.

c) Importance to the South African economy

Unsound operational risk practices have led to the insolvency of many large financial institutions like Barings Bank in the United Kingdom. A banking crisis caused by operational risk will result in the loss of confidence in the South African economy by investors and could lead to a 'flight of money' and a downgrade in the country's investment rating assigned by rating agencies.

d) Peer group comparison among South African banks

The Basel II framework allows a significant amount of flexibility to banks to use their own discretion, specifically on how internal loss data should be collected for operational risk purposes. Certain banks in South Africa will approach the BSD for approval to use the AMA for operational risk purposes. These banks would be required to develop internal loss databases for the purposes of measuring and managing operational risk. The flexibility provided to banks could lead to divergent practices that *would make peer group comparison among banks an extremely difficult task.*

1.8 BENEFITS OF STUDY

a) Most likely severe operational risk losses in South African banks

As the results of the research include the most likely severe operational risk losses within banks, the outcome of the study could be presented to individual banks' boards of directors as part of the BSD's annual presentations. The boards of directors could then take note of the findings of the research and put appropriate measures in place to develop sound operational risk management practices.

b) Practices for internal loss data collection

As little is currently known about the practices South African banks use to collect internal loss data for operational risk purposes, the results of the research will be shared with the BSD to provide appropriate guidance to banks for collecting and capturing internal loss data for operational risk purposes.

As this would be based on the collective view of all registered banks in South Africa, specific guidance in the form of a Banks Act Circular *could* be sent to banks providing guidance on what constitutes acceptable practices. The guidance provided by the BSD will also ensure consistent capturing of internal loss data across the entire banking industry in South Africa.

The results could also be used by the BSD to assess individual AMA and TSA applications from banks for operational risk regulatory capital purposes.

The results will highlight what constitutes sound operational risk management practices for capturing internal loss data. The study will also provide greater insight when doing peer group comparison for operational risk purposes, both

into data collection practices and the likely occurrence of severe operational risk events.

1.9 CONTRIBUTION OF STUDY TO EXISTING BODY OF KNOWLEDGE

Operational risk is not new to banks, as they have always been exposed to operational risk. However, the science of operational risk management and the quantification thereof, specifically for regulatory and economic capital purposes, are new to banks. Not many studies on operational risk have been conducted in South Africa.

The study performed by the AIGOR on the range of practices for the collection of operational risk data excluded South African banks. To the researcher's knowledge, this will be the first research of its kind to be conducted in South Africa and will provide guidance to the financial services regulators and banks on what the most likely severe operational risk losses are, what the range of practices is within South African banks for collecting internal loss data, and what constitutes sound operational risk management practices. Sound operational risk practices will be approached from a *qualitative* perspective, by benchmarking the research findings against the Basel II text, the Basel Committee on Banking Supervision's *Sound Practices for the Management and Supervision of Operational Risk*, and related literature.

This study will highlight to all the banking sector participants the most likely severe operational risk losses that could occur within banks so that appropriate action can be instituted by financial services regulators and senior management of banks to address issues specific to their banks.

1.10 OUTLINE OF RESEARCH REPORT

The research report is outlined in the following manner:

Chapter 2

Chapter 2 forms the foundation of the research study. It gives the reader a brief history of the origin of regulatory capital, a description of the regulatory structures for banking supervision in South Africa, an outline of the types of risks that banks are exposed to, as well as the current structure of the South African banking system.

Chapter 3

In this chapter a thorough literature review is conducted on relevant literature. The literature review, including references to certain surveys and studies, focuses on the main concepts of operational risk within banks relevant to the research problem. The literature review also includes several references to the Basel II text and other relevant publications and papers issued by the BCBS.

Chapter 4

Included in this chapter is the research design or 'research plan'. It includes a discussion of the general research methodology, the population and sample size, the measuring instrument to be used, data collection techniques, data analysis methods and the delimitations of the empirical study.

Chapter 5

The researcher outlines the results of the study conducted. This chapter also includes an analysis of the research results.

Chapter 6

The researcher discusses the results of the research in this chapter and concludes with recommendations to the banking sector and the BSD.

Africa = R100 000 regulatory capital requirement

Peter's Coffee Shop - R1 million loan x 100% standard risk weighting x 10% regulatory capital requirement for South Africa = R100 000 regulatory capital requirement

Although Anglo American represents lower credit risk than Peter's Coffee Shop, under Basel I capital rules both loans would be risk weighted at a credit conversion factor of 100% and would result in the same capital requirement. The Basel I rules thus did not make provision for risk differentiation and treated all private non-bank borrowers the same.

The BCBS recognised that banks' own internal capital assessments, based on both transactions as indicated above, resulted in two different internal economic capital requirements for both transactions. The BCBS also acknowledged that there was a vast difference in banks' total internal economic capital, as calculated by their economic capital models, and the total amount of capital they held for regulatory purposes. "The BCBS consulted extensively with banks and industry groups in an attempt to develop significantly more risk-sensitive capital requirements that are conceptually sound" (Basel Committee on Banking Supervision, 2007: 3).

2.3 BANKING REGULATION IN SOUTH AFRICA

The Minister of Finance is responsible for banking regulation and the drafting of financial services legislation in South Africa. The Banks Act (Act No. 94 of 1990) (Banks Act) is the first tier of banking legislation in South Africa and sets out the requirements for lawful deposit-taking activities.

The Banks Act makes provision for the appointment of a Registrar of Banks (Registrar), whose primary responsibility is the supervision of banks in South Africa. The Minister of Finance appoints the Registrar into office. The Registrar thus has a functional reporting line to the Minister of Finance (Kruger, 2007). The Bank Supervision Department (also known as the Office of the Registrar of Banks) is situated and housed within the South African Reserve Bank, with the Registrar having an administrative reporting line to the Governor of the South African Reserve Bank (Kruger, 2007).

The Regulations relating to Banks (the Regulations) make up the second tier of banking legislation. The Regulations consist of specific rules to banks on issues such as governance practices, risk management practices, reporting responsibilities and business practices.

The BSD supervisory practices include the following (Kruger, 2007):

- The quantitative analysis of financial and risk information submitted by the banks. This includes the feedback of quantitative information submitted by banks in the form of graph presentations. Feedback on quantitative information is also provided to banks' boards of directors.
- Qualitative review of banks' operations. This includes prudential meetings with bank management, the external and internal auditors, and meetings with banks' audit committees. It also entails the screening of bank

management to ensure that only 'fit and proper' people be custodians of depositor funds.

- Targeted inspections at banks' premises, specifically with regard to problem areas.

See Appendix A for the supervisory review process of the BSD.

The above-mentioned supervisory practices will, however, not always deter bank failures from happening. The primary mission of the BSD is to ensure "a sound and efficient banking system" (the researcher's own emphasis) (South African Reserve Bank, 2007b). Bank management is tasked with the responsibility to ensure that individual banks are sound and going concerns.

2.4 RISKS FACED BY BANKS

In this section of the research report the researcher will outline the various types of risks that banks are exposed to.

Banks are exposed to a number of risks. Below are the most common types of risks that banking institutions are exposed to:

Credit risk

Credit risk arises when the bank advances money to either individuals or the private and public sectors. By advancing these loans a bank is uncertain of whether those entities will repay the bank in full when the date of repayment arises.

Market risk

Market risk arises due to fluctuations in market prices of a financial instrument, based on the changes in the exchange rates, interest rates, commodity prices and other market factors.

Operational risk

This was dealt with in Chapter 1 of this research report.

Liquidity risk

A bank is exposed to liquidity risk when it is unable to meet its contractual obligations. Liquidity risk arises due to a mismatch between the contractual maturity of a bank's liabilities and the contractual maturity of its assets.

Interest rate risk

“Interest-rate risk is the sensitivity of capital and income to changes in interest rates” (Van Greuning & Bratonovic, 2003: 249).

Counterparty risk

Counterparty risk refers to the cost of replacing a contract relating to a financial instrument with a similar one, due to the failure of a counterparty to honour its commitment to the contract obligations.

Capital risk

Capital risk is the risk that a bank would not have sufficient capital to absorb losses and to continue with its business operations. The risk also entails the possibility of a bank being non-compliant with minimum regulatory capital requirements.

Currency risk

“Currency risk results from changes in exchange rates and originates in mismatches between the values of assets and liabilities denominated in different currencies” (Van Greuning & Bratonovic, 2003: 261).

As part of their Enterprise-wide Risk Management Framework, Nedbank also includes the following risks as part of their risk universe (Nedbank, 2006):

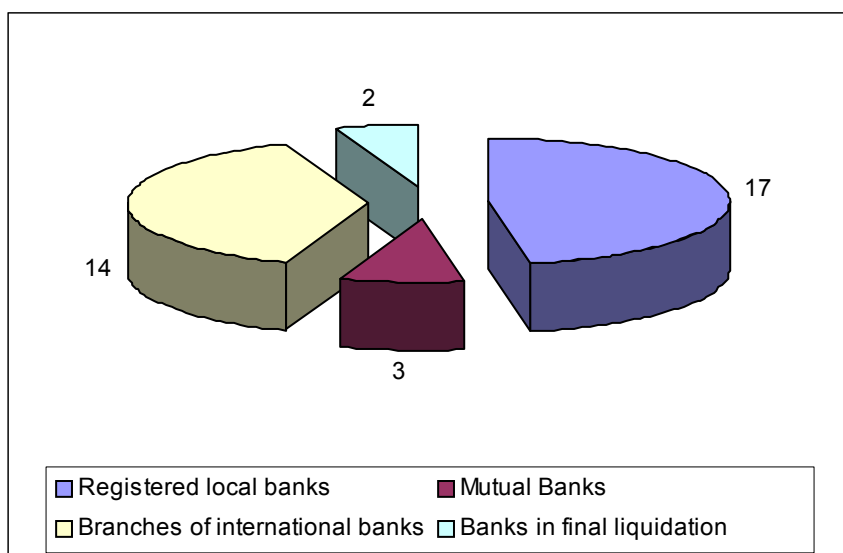
- Accounting and taxation risk
- Insurance and Assurance risk
- New business risk
- Investment risk
- Information technology risk

- Compliance risk
- Strategic risk
- Reputational risk
- Social and environmental risk
- People risk

2.5 SOUTH AFRICAN BANKING SYSTEM

The South African banking sector comprises of 36 banks. Seventeen of those banks are locally registered banks in terms of the Banks Act. Branches of international banks such as JP Morgan Chase Bank (Johannesburg Branch), HSBC Bank plc (Johannesburg Branch) make up 14 of the 36 banks. There are only 3 mutual banks operating in the country. Regal Treasury Private Bank Limited and Islamic Bank Limited are in the final processes of liquidation (South African Reserve Bank, 2006). See *Figure 1* below for a graphic depiction of the banking sector:

Figure 1: South African banking sector



Source: Adapted from South African Reserve Bank, 2006

The total banking assets of the South Africa at the end of March 2007 amounted to R2,2 trillion (South African Reserve Bank, 2007c). The assets of the five large banks (Absa Bank Limited, Nedbank Limited, The Standard Bank of South Africa Limited, FirstRand Bank Limited and Investec Bank Limited) contribute approximately 90 percent of total banking assets (South African Reserve Bank, 2007c).

See *Table 1* for the asset sizes of the four largest South African banks (excluding Investec Bank Limited):

Table 1: Assets of four largest banks as at 31 March 2007

	Standard Bank R'000	ABSA R'000	FirstRand R'000	Nedbank R'000	Total R'000
Total assets	549,817,758	476,246,402	404,491,939	390,660,067	2,176,478,566

Source: Adapted from South African Reserve Bank, 2007c

Table 2 below reflects the individual market share in core advances of the four largest banks (excluding Investec Bank Limited):

Table 2: Market share of core advances at 31 March 2007

	ABSA %	FirstRand %	Nedbank %	Standard %
Instalment sales	24	33	10	22
Mortgage loans	32	17	20	25
Credit cards	25	23	12	36
Overdrafts and other loans	20	19	24	19

Source: Adapted from South African Reserve Bank, 2007c

From the above it is clear that the four large banks have a significant share of the total banking assets and market share of core advances. This form of concentration risk poses systemic risk to the South African banking system. Therefore it is important to ensure the soundness of all banks in the banking system, in particular the four largest banks.

3. CHAPTER THREE: LITERATURE REVIEW

The literature review, including references to certain surveys and studies, will focus on the main concepts of operational risk within banks and the research problem as stated in Chapter 1. The literature review also includes several references to the Basel II text and other relevant publications and papers issued by the BCBS.

3.1 DEFINING OPERATIONAL RISK

Banks have always been exposed to operational risk. However, it was difficult to *exactly* define the concept of operational risk. Operational risk was initially defined in the negative as “any form of risk that is not market or credit risk” (Financial Stability Institute, 2007).

In order to illustrate the ambiguity surrounding the definition of operational risk even as recently as the year 2000, Crouhy, Galai & Mark (2001: 475) indicated that “operational risk is not well defined” and referred to it as a “fuzzy concept”. A further example is that of Evans (2004) who indicates that the concepts of business risk and operational risk are the same. The researcher wants to disagree with this statement.

Because operational risk could not be properly defined, banks were unable to identify, measure and manage a risk that had no formal definition. In retrospect, the negative definition of operational risk (“any form of risk that is not market or credit risk”), left risk managers with a dilemma as, strictly speaking, this definition could have included any other financial or non-financial risks. More importantly, banks were not compelled by regulatory authorities to hold capital against operational risk and therefore did not provide any incentive for banks to properly define and manage the operational risk within their specific institutions.

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 on Banking Supervision, 2006a: 144).

In Basel II, the BCBS for the first time defined operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee on Banking Supervision, 2006a: 144). This definition includes legal risk, but excludes strategic and reputational risk (Basel Committee on Banking Supervision, 2006a: 144). Samad-Khan, Rheinbay & Le Blevet (2006: 4) indicated that banks should not confuse operations risk with operational risk, as "as operations management is primarily a back-office management task in banks involving the processing and systems function, whilst operational risk manifests itself in all the activities of banks" (the researcher's own emphasis).

The definition of operational risk by the BCBS provides a structured and ordered approach to banks to identify, measure and manage operational risk. According to De Fontnouvelle et al. (2006) many banks had taken the definition of operational risk as stated in the Basel II text as their own internal definition.

3.2 CLASSIFICATION OF OPERATIONAL RISK LOSSES BY THE BASEL COMMITTEE ON BANKING SUPERVISION

This section of the literature review is relevant to the following sub-problem as stated in Chapter 1 of the research report:

- Determining in which areas in South African banks the most severe operational risk losses are likely to occur.

The BCBS, in its publication of the Basel II text, provides clear guidance on the classification of operational risk loss event types to be captured in the internal loss database, and to be used for calculating regulatory capital for operational risk in banks adopting the AMA. Operational risk losses are classified in the Basel II text according to seven event types and eight business lines. Banks are required by the Basel II rules to map all operational risk losses according to the seven loss event types outlined below (Basel Committee on Banking Supervision, 2006a: 305 – 307):

1) “Internal fraud

Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party.

2) External fraud

Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.

3) Employment practices and workplace safety

Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.

4) Clients, products and business practices

Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.

5) Damage to physical assets

Losses arising from loss or damage to physical assets from natural disaster or other events. Examples of other events include human losses from external sources such as terrorism and vandalism.

6) Business disruption and system failures

Losses arising from disruption of business or system failures. Examples of these losses includes losses due to hardware, software, telecommunications, utility outage/disruptions, etc.

7) Execution, delivery and process management

Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.”

Bruce (2006) refers to several surveys conducted in financial institutions, indicating the most severe operational risk events. The majority of the surveys indicate that most of the operational risk losses in financial institutions result from *external fraud, followed by execution, delivery and payment processes*.

In addition to the seven operational risk event types required by Basel II, banks are also required in terms of Basel II to classify all operational risk events

according to the following eight business lines (Basel Committee on Banking Supervision, 2006a: 305):

- 1) Corporate finance
- 2) Trading and sales
- 3) Retail banking
- 4) Commercial banking
- 5) Payment and settlement
- 6) Agency services
- 7) Asset management
- 8) Retail brokerage

The surveys referred to by Bruce (2006) also indicate that operational risk losses mostly occur within a financial institution's *payments and settlements processes*. The reason for classifying operational risk events in terms of the seven event types and eight business lines is for banks to determine exactly where operational risk losses occur so they could put controls in place to prevent losses from recurring.

3.3 EXPECTED AND UNEXPECTED OPERATIONAL RISK LOSSES

The concepts of expected and unexpected losses are very important to banks adopting AMA for the quantification of operational risk regulatory capital. Operational risk events could be classified as those expected more frequently-occurring losses, as well as those unexpected losses that do not occur so often. Samad-Khan, Rheinbay & Le Blevec (2006) describe expected losses as those operational risk losses in monetary terms that a bank expects to lose on average in a given year. Unexpected losses are those operational risk losses in monetary terms that are in excess of the expected average losses in a given year.

Losses such as credit card fraud, information technology (IT) system failures and downtime of systems occur frequently and are almost considered to be part of doing business. Putting appropriate continuity plans in place or strengthening internal controls of the bank could control these losses.

Unexpected operational risk losses are those that are not expected by a bank and could result in billions of rands of losses. It is those single, unique, non-repetitive events. Examples of such unexpected operational risk losses include trading losses due to unauthorised trades by an employee, a lawsuit by an employee due to discrimination claims, the loss of physical assets such as buildings, devastation due to a natural disaster and errors in the transfer of large payments. However, Samad-Khan, Moncelet & Pinch (2007) indicate that one has to guard against classifying all small losses in the expected loss category and large operational risk losses in the unexpected loss category, as this might not always be the case. Some operational risk experts are of the view that unexpected losses are not preventable, even by the financial services companies with the best operational risk practices (Bielski, 2003). The attacks on the World Trade Center in New York in 2001 are a good example of how management could not have prevented an aircraft with terrorists on board destroying company property.

Unless a bank adopting the AMA can convince regulators that it captures and manages expected losses as part of the bank's internal processes, a bank will have to reserve regulatory capital for both expected and unexpected losses (Basel Committee on Banking Supervision, 2006a). This provides a significant incentive for banks to adequately manage and control expected operational risk losses.

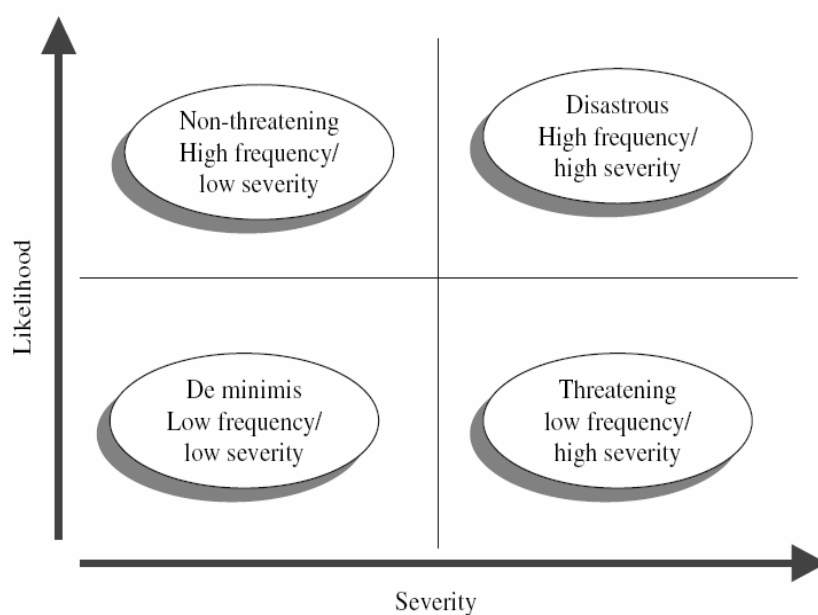
3.4 OPERATIONAL RISK ASSESSMENT

According to Scandizzo (2005) risk mapping is the starting point of operational risk assessment. It identifies the cause of operational risk events and indicates in which area of business the operational risk event occurred.

The likelihood/impact chart is the most widely used method for operational risk assessment (Scandizzo, 2005). It is also commonly referred to as the Committee for Sponsoring Organisations of the Treadway Commission (COSO) framework.

Figure 2 depicts the likelihood/impact chart.

Figure 2: Likelihood/impact chart



Source: Scandizzo, 2005

“Under this approach, businesses calculate the magnitude of their risks based on a mathematical formula, where risk is equal to the likelihood that a given event will occur multiplied by its effect (impact), should it occur, such that, $\text{Likelihood} \times \text{Impact} = \text{Risk}$ ” (Samad-Khan, 2005:2).

Based on the likelihood/impact chart, operational risk managers will classify operational risk events into one of four categories. This is regarded as a very basic method of operational risk assessment, and attracts criticism from a wide range of operational risk gurus. Scandizzo (2005) criticises it for not indicating what management actions the bank intends to institute to prevent the recurrence of the operational risk event. The method also does not provide an indication of where the operational losses occurred.

Samad-Khan (2005) criticises the COSO framework for the method of calculating operational risk. With the COSO framework, high likelihood/high severity losses represent the biggest risk to a bank. According to Samad-Khan (2005) the COSO approach is in total contrast with sound operational risk management as the most severe operational risk losses arise from low likelihood/low frequency/high impact events.

Samad-Khan's (2005) view is that high likelihood/high frequency/high severity events do not exist in operational risk. The researcher concurs with Samad-Khan (2005) as high likelihood/high frequency/high severity events suggest that losses amounting to billions of rand occur frequently, and are likely to recur without management intervention. One more criticism of this method is that it makes extensive use of risk managers' perceptions to classify operational risk losses (Samad-Khan, Rheinbay & Le Blevec, 2006).

Another method is to map operational risk losses according to standard loss categories and different business lines (Scandizzo, 2005). The researcher's view is that the intention of the BCBS to require banks to classify all operational risk events into seven loss event types and eight business lines was to form a minimum standard for operational risk assessments. This method gives management an exact idea of what the cause of operational risk events are, and in what area it occurred (Scandizzo, 2005). As a result, action plans can be instituted to prevent the recurrence thereof.

A more progressive method of operational risk assessment is the use of statistical analysis, based on historical operational risk data, to assess operational risk within the organisation. Operational risks are assessed based on the frequency of past events and not on the likelihood of the event occurring (the researcher's own emphasis) (Samad-Khan, Rheinbay & Le Blevec, 2006). There are, however, some operational risk experts that criticise the method of using statistical analysis to measure operational risk. However they are in the minority.

Levy et al. (2005) are some of those experts who indicated that historical data are best suited for the measurement of market and credit risk and emphasise that the use of statistical analysis does not necessarily fit the purposes of operational risk management. Levy et al. (2005) indicate that historical data not necessarily predict future operational risks events. The researcher disagrees with the comments made by Levy et al. (2005) as the tracking of historical loss data for operational risk had been used successfully in many large banks in the world and is considered best practice for the management and measurement of operational risk.

3.5 EFFECT OF OPERATIONAL RISK LOSSES ON BANKS

The effect of operational risk failures could have severe effects on banks and could even jeopardise the long-term sustainability of the institution involved. A well-known international example is that of Barings Bank in the United Kingdom, where the unlawful practices of trader Nick Leeson resulted in the collapse of one of the oldest banks in that country.

Kraujalis et al. (2006: 10) refer to the following institutions affected by large operational risk losses as originally identified by Kancerevyčius in 2004:

- 1994 – Kidder Peabody: USD1.69 billion
- 1995 – Salomon: USD0.13 billion
- 1995 – Barings: USD2.20 billion
- 1995 – Daiwa: USD1.10 billion
- 1997 – Natwest Markets: USD0.13 billion
- 1998 – Sumitomo: USD2.60 billion

South African banks were not immune to the rise in operational risk events. Examples include several cases of internal fraud committed by senior executive officers, the most famous of them being crimes committed by the then chief executive officer of Regal Bank Limited.

Operational risk events, whether small or large, could have an adverse effect on a bank's financial performance. Foot (2002) reminds us of the effects of operational risk losses across an entire banking operation having not just implications for the business unit in which it occurs, but could have potential devastating implications for the entire bank.

Operational risk events lead to losses for banks and erode their reserves and the net asset values (capital). Losses have to be written off through the income statements which make banks less attractive to potential investors and existing

shareholders. More significant, though, are those large losses that are publicised by the financial media. These large operational risk events could have reputational consequences and could lead to 'a run' on a bank. One can just imagine how depositors would react if they read in a newspaper that the chief executive officer of a bank embezzled hundreds of millions of rands, or that a staff member of a bank had erroneously transferred billions of rands to an entity in another country from where it will be difficult to recover the money transferred.

Garver (2006a) refers to a study conducted by the University of Pennsylvania's Wharton School where it was found that the impact of operational risk failures can greatly reduce a bank's market capitalisation up to an average of 5.3 times the amount of the operational risk loss. In a separate study conducted by Dunnet et al. (2005), it was reported that the reduction in market capitalisation could be up to 12 times that of the operational risk loss.

The larger and more complex a bank becomes, the larger the possibility of increasing operational risk events. The legacy of mergers and acquisitions over the years resulted in banks having totally different IT systems. The various combined business units are not integrated and have disconnected IT systems. In other words these IT systems do not 'talk' to each other. Thus, the disconnect between the different IT systems in banks and the absence of an enterprise-wide database result in an increase in operational risk events, mainly due to the manual reconciliation processes involved.

Many banks have already started reporting on operational risk losses to their various risk committees. The aforementioned reporting process ensures that sufficient controls and risk management practices are put in place to mitigate or prevent these operational risk losses.

It is evident from the above examples that operational risk could have negative consequences on a bank's earnings and for its reputation.

3.6 BENEFITS OF OPERATIONAL RISK MANAGEMENT

There is, however, a business case for the management of operational risk. According to Bielski (2003: 1), Wachovia considers the management of operational risk “a source of competitive advantage, whether the BCBS requires it or not” (the researcher’s own emphasis). Samad-Khan (2005) also emphasises that operational risk management should be far more than merely being in compliance with Basel II.

Banks with sound operational risk practices can enter into business transactions that other banks are not prepared to entered into (Levy, 2006). Sound operational risk management could assist banks in pricing for operational risks and thereby enhance profitability.

However, in order to gain the optimum benefits from operational risk management the bank has to put processes in place to ensure the successful implementation of an operational risk framework.

Lam (2001:1) outlines nine requirements for successful operational risk management:

- A bank has to adopt and formalise a definition for operational risk. The trick is to keep it simple and not have a sophisticated definition. The researcher noticed how many banks, especially South African banks, had adopted the Basel II definition of operational risk. Once the definition is established, a bank should move on and not get stuck on formulating the most complicated definition.
- Appoint a person that would be responsible and accountable for the operational risk function. In South Africa, the large banks all have a chief operational risk officer. In smaller banks the function resides mainly within the chief risk officer or even the chief financial officer.

-
- Draw up a list of the risks most salient to the bank. One would expect all banks to at least in their list include those risks the researcher had outlined in Chapter 1 of this report.
 - A bank has to be aware of all causes of operational risk losses and events in the bank. Capture all operational risk events and losses in a central database.
 - Introduce an operational risk reporting structure. The reporting structure should include reporting within specific business units, reporting to the chief operational risk officer, and reporting to the board of directors.
 - After the operational risk losses have been identified and reported, processes should be put in place to ensure that these operational risk events and causes are prevented and managed appropriately.
 - The silos between line management and risk management should be broken down.
 - If feasible, instead of retaining the risk, it can be transferred to an insurance company.
 - Do not lose focus by conducting change management programmes and working on changing the culture within the organisation.

3.7 MEASURING OPERATIONAL RISK FOR CAPITAL PURPOSES

Samad-Khan (2005) indicates that the effective management of operational risk requires the measurement of operational risk (the researcher's own emphasis).

The results of a study conducted by De Fontnouvelle et al. (2006) suggest that the capital requirements for operational risk will in the future exceed the minimum regulatory capital for credit and market risk. The researcher's view is that the aforementioned statement is *not* entirely true and that the regulatory capital requirements for banks will differ based on each bank's core business activities. Although the operational risk capital requirement might exceed the capital requirements of market risk, credit risk remains the main risk area in banks.

Young (2006: 70) provides the following "essential reasons" for the measurement of operational risk:

- "To identify the potential operational risk exposures of the organisation
- To serve as a platform for the calculation of the cost of operational risk (losses)
- To serve as a basis for cost-effective decisions by management
- To ensure that cost of risk does not exceed the benefits stemming from the actual management thereof"

The regulatory capital requirement for credit, market and operational risk operational is based on three pillars. The first pillar consists of the minimum capital requirements, the second the supervisory review process of the banking regulators, and the third market discipline (Basel Committee on Banking Supervision, 2006a). As this research will only focus on operational risk under the requirements of Pillar 1, a brief description of the requirements in terms of Basel II is highlighted below.

Basel II requires banks to calculate the minimum capital requirements under Pillar 1 based on three approaches, starting from the least sophisticated approach to more sophisticated approaches. These are discussed below.

a) Basic Indicator Approach (BIA)

This approach is the least complex of the three approaches outlined in the Basel II requirements and requires the least work for banks. The BIA is mainly targeted at smaller, less sophisticated banks. The BIA is only a method to calculate regulatory capital for operational risk and cannot be used to measure operational risk. Large internationally active banks are not allowed to use this method for calculating their minimum capital requirements in terms of Basel II. A bank's minimum capital requirements are calculated by multiplying a bank's positive average annual gross income over the past 3 years by an alpha factor of 15% (Basel Committee on Banking Supervision, 2006a).

According to Hughes (2005), the rationale for basing a bank's capital requirement on the level of gross income is that operational risk increases as the number of transactions in banks increases (the researcher's own emphasis).

b) Standardised approach (TSA)

This approach is somewhat more sophisticated than the BIA in that it requires a bank to split its annual gross income into eight prescribed business lines as outlined in Section 3.2 of this report.

According to Cruz (2002: 275) "the rationale behind this approach lies in the recognition that operational risks arising in different businesses have differentiating profiles, and one business unit may have a higher risk profile than another". The positive gross income of each business line is multiplied by a different beta factor, reflecting the general riskiness of that specific business line.

Although more sophisticated than the BIA, this approach does not accurately measure operational risk. It is only one method allowed by the BCBS to calculate regulatory capital for operational risk.

The BCBS also made provision for banks to adopt the Alternative Standardised Approach (ASA) for the calculation of operational risk regulatory capital based on the discretion of individual regulators. The differences between the TSA and the ASA is outline below (Financial Stability Institute, 2007):

- The regulatory capital requirement under the ASA for retail and commercial banking business lines is calculated using loans and advances as the base for the calculation, instead of gross income as in the case of TSA.
- The calculation of regulatory capital for the remaining six-business lines will be based on gross income.

c) Advanced Measurement Approach (AMA)

This is the most advanced of the three approaches to calculate operational risk regulatory capital. This method of calculating regulatory capital for operational risk is based on best practices over the last decade in large internationally active bank such as JP Morgan Chase Bank. Power (2005) and Flores et al. (2006) describe how this approach is bank-specific and reflect the historical operational risk losses of that specific institution.

“Under the Basel II AMA approach, a bank has considerable flexibility in developing and using its own methodology for calculating its risk-based capital requirement for operational risk” (Financial Stability Institute, 2007b: 17). The AMA allows a bank to calculate its minimum capital requirement under Pillar 1 based on internal operational risk loss history of a bank.

A bank adopting AMA should be able to measure unexpected losses over a one-year period using a confidence level of 99.9 percent (Basel Committee on Banking Supervision, 2006a).

Banks adopting the AMA would need to track their internal operational risk loss history for the quantification of their operational risk capital charge. Cruz (2002) confirms the aforementioned statement and describes the necessity of collecting historical data internally in order to accurately measure regulatory capital for this approach.

- Loss Distribution Approach (LDA)

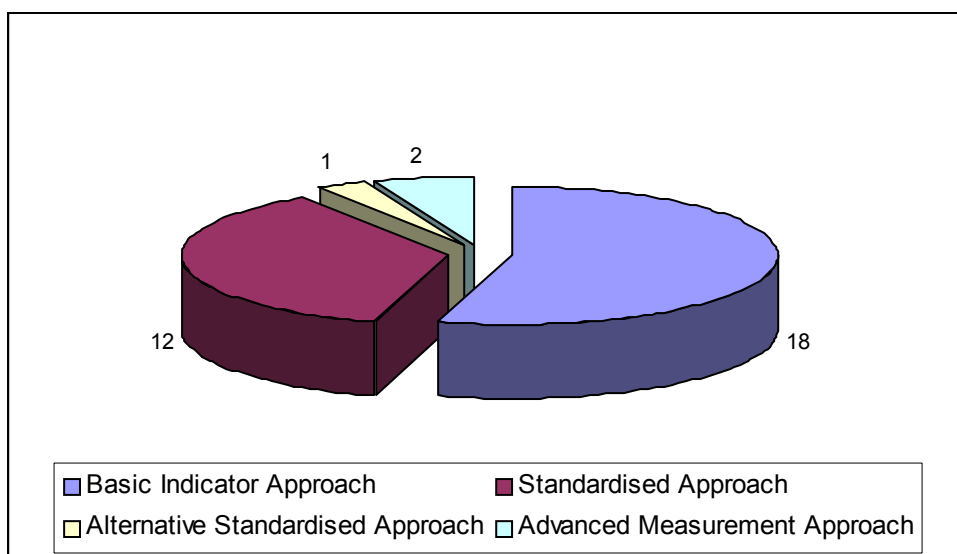
The Advanced Measurement Approach set out by the Basel Committee is based on the LDA. Frachot, Georges & Roncalli (2001: 2) described AMA as a “simplified” format of the LDA. Large internationally active banks had used the LDA for several decades to measure operational risk.

The LDA is based on statistical data as in the case of the AMA and makes sole use of internal loss data history to calculate an economic capital charge per business unit. “Under this approach, the bank estimates, for each business line/risk type cell, the probability distributions of the severity (single event impact) and of the one-year event frequency using its internal data. With these two distributions, the bank then computes the probability distribution of the aggregate operational loss. The total required capital is the sum of the Value-at-Risk of each business line and event type combination” (Frachot, Georges & Roncalli, 2001: 2).

The LDA is criticised for only using internal loss data to measure operational risk, as internal data should be complemented by external data to effectively measure operational risk (Financial Stability Institute, 2007c).

All the approaches prescribed by the BCBS above for calculating regulatory capital for operational risk will be available to South African banks. Banks approached the South African Reserve Bank and indicated their intended approaches. *Figure 3* below sets out the distribution of approaches for South African banks' calculation of operational risk regulatory capital. The 3 mutual banks are not required to adopt Basel II in 2008.

Figure 3: Regulatory approaches for operational risk



Source: Adapted from South African Reserve Bank, 2006

3.8 INTERNAL LOSS DATA

Operational risk loss data consist of internal loss data and data obtained from external sources (external data). Internal loss data are bank-specific and obtained from the different business units and support functions within a bank. External data include data obtained from public sources and could also include data provided by the insurance industry (Samad-Khan, Moncelet & Pinch, 2007). This research report as well as the section below will only focus on internal data.

According to Samad-Khan (2005) calculating historical internal loss data is the best method to use in the identification of operational risk. Haas and Kaiser (2005: 217) indicate that “the most important means of collecting relevant information for operational risk measurement is the collection of data”. Operational risk events need to be captured as soon as possible to ensure that all vital information is recorded. The staff directly involved in the operational risk event should preferably capture the event.

According to Macklin et al. (2003), JP Morgan Chase Bank captures all operational risk events in its Risk Event Database. The Risk Event Database is a central system that allows all JP Morgan Chase Bank subsidiaries around the world to capture operational risk events specific to the subsidiary’s operations. The operational risk events could then be tracked and preventative strategies put in place to prevent these risks from recurring.

Internal loss databases could also be updated with operational risk losses or near misses through the close scrutiny of audit reports (both internal and external audit reports), risk management reports, compliance reports and reports from financial services regulators (e.g. BSD reports and letters).

Van den Brink (2002: 58) indicates that for internal loss data to be relevant, at least the following information regarding the operational risk event should be reported:

- The loss amount.
- The product involved.
- The occurrence date.
- The cause of the loss.
- The process steps in which the loss occurred.
- The loss category.

3.9 AMBIGUITY OF PRACTICES FOR COLLECTING INTERNAL LOSS DATA

This section of the literature review specifically covers sub-problems relating to the range of practice for capturing internal loss data, as stated in Chapter 1.

As part of a number of guidelines provided by Young (2006: 66) for the operational risk measurement process, the following are the most important for the purpose of this report:

- Objectivity – The measurement of operational risk should be executed through the use of standard, objective criteria.
- Consistency – Operational risk data should be used in a consistent way in order to ensure that different risk profiles of similar business areas can be compared.
- Relevance – The data used to identify operational risk should be relevant to the business in order to allow management to make accurate decisions based on the risk measurements.
- Transparency – All the essential operational risk data should be reported and assessed in a way that makes risk management transparent to senior managers.
- Enterprise wide – Operational risk measurement should be designed in such a way that the results can be aggregated across the entire organisation.
- Completeness – All material operational risks should be identified and captured. This includes near misses”.

The Basel II text does *not* provide specific guidance on how banks should collect and capture internal loss data. Guidelines provided by the BCBS are very broad and the discretion on the methods to be used is largely left to banks.

a) Paragraph 673 of Basel II indicates that for a bank’s internal loss collection process to qualify for regulatory purposes it should adhere to the following:

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 on Banking Supervision, 2006a: 144).

- 1) “Collect information about the date of the event” (Basel Committee on Banking Supervision, 2006a: 153). No specific guidance is provided on what the date of the events should be in certain cases.

Haunbenstock (2005) concurs with the views of the AIGOR in that no clear guidance is provided on the date when operational risk events should be captured.

- 2) “Capture the gross loss amount in case of an event” (Basel Committee on Banking Supervision, 2006a: 153). The text does not indicate what the aforementioned gross amount should be. No specific guidance is provided on whether it would be sound operational risk management practice to use book values, market values or replacement cost.

Futjii (2005) illustrates the dilemma operational risk managers are faced with by using the example of how the loss of an office building that collapsed during an earthquake should be captured in the internal loss database. Should the amount of the loss of the office building be reflected as the book value of the building, the market value of the building at the time of the earthquake, or the cost necessary to reconstruct the building?

- 3) “Have an appropriate *de minimis* gross threshold for loss data collection” (Basel Committee on Banking Supervision, 2006a: 144). The Basel II text provides an example of 10 000 euros. It indicates, “while the appropriate threshold may vary between banks, it should be broadly (the researcher’s own emphasis) consistent between peer banks” (Basel Committee on Banking Supervision, 2006a: 153). Haunbenstock (2005) corroborated with the aforementioned that the thresholds for capturing loss events should be bank-specific. The researcher’s task is to determine what thresholds are in use in different banks in order to make an appropriate peer group comparison.

- 4) The Basel II rules do not provide any guidance on whether internal data should include near misses. Near misses are operational risk events that almost occurred, but were prevented by some form of intervention. Fujii (2005) explains his view on the inclusion of near misses in internal loss databases and state that the inclusion of near misses could only enhance internal loss data to better predict the future.

This researcher's view is that near misses and opportunity cost should be recorded to provide for sufficient levels of regulatory capital against operational risk losses. Marshall (2001: 191) confirms the researcher's view by indicating, "loss records should ideally include near misses as well as actual incidents that may cause losses, as these provide important information".

3.10 READINESS OF THE BANKING SECTOR

Bethell-Jones (2001) and Garver (2006b) describe how the capital management practices for operational risk are still immature if compared to capital management practices for credit and market risk. They blame the lack of progress mostly on the lack of accurate data for operational risk.

According to Kraujalis et al. (2006) banks fail to give sufficient attention to operational risk. It is better for banks to concentrate on those risk areas that management and the board are comfortable with. Young (2006) has the same view and comments specifically on the lack of progress in this area by South African banks.

Could the lack of progress be ascribed a lack of top management commitment to an effective operational risk programme? Some bankers indicate that operational risk within the new Basel Capital Accord was only a late addition by the BCBS when it revised the Capital Accord (Bielski, 2003). Macklin et al. (2003) reported that the success of the operational risk programme at JP Morgan Chase Bank could be attributed to the support of top management of that bank.

Regulators are also to blame as they have not exerted enough pressure on banks, specifically the smaller ones, to develop their operational risk practices. The smaller banks do not have the resources to employ an operational risk officer, let alone instituting a fully-fledged operational risk function.

The large internationally active banks such as JP Morgan Chase Bank and Wachovia support the operational risk requirements in the new Capital Accord (Bielski, 2003). Macklin et al. (2003: 2) report how JP Morgan Chase Bank had adopted the management of operational risk as a “primary risk discipline”. Many of the smaller banks can argue that the operational risk requirements within the new Capital Accord are based on the current practices in these large

internationally active banks, and these banks will not have to make significant adjustments to their current practices and systems.

Principle 8 of the Sound Practices for the Management and Supervision of Operational Risk indicates that “banking supervisors should require that all banks, regardless of size (the researcher’s own emphasis), have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management” (Basel Committee on Banking Supervision, 2003a: 13).

3.11 SHIFT IN CULTURE

The definition of operational risk could be summarised as the risk resulting from people, systems and external events. As the ‘people factor’ is one of the main contributors to operational risk, the culture of the organisation plays a significant role in the behaviour of people (Holmquist, 2007).

Banks are currently focusing most of their efforts on complying with the minimum requirements of Basel II. Those banks that are looking beyond Basel II compliance, focuses their energies on getting value from the introduction of sound operational risk measurement and management practices.

Sabatini (2007) warns that operational risk managers who are only playing the ‘compliance card’ will not get the full attention of business managers. Business managers will only give their full attention when operational risk managers explain the effect of sound operational risk management on their operations’ bottom line (Sabatini, 2007).

Many of these banks do not realise that these practices means absolutely nothing if you do not change the behaviour of the people working in the

organisation. Levy et al. (2005) reported that, in consulting for McKinsey they found that many of the people issues are being put last.

According to Levy et al. (2005) authority and rank in the bank should not only be determined by an employee's contribution to the bank's income. A change in a bank's remuneration structure is necessary to change a culture of risk management. Staff should not only be remunerated for the volumes of business that they bring to the organisation. An adjustment to the bonus structure of the bank should be made based on individuals' contribution to the overall risk profile of the organisation.

Many banks had introduced risk-adjusted performance measurement (RAPM) systems to also remunerate employees for their contribution to the overall risk profile of the organisation.

Macklin et al. (2003) also recommend that the culture of a bank should be changed from a culture of preventing mistakes, to a culture of risk management within a specific risk tolerance level. Risk should not only be seen as something adverse but should be seen as an opportunity for profit if correctly measured and managed.

Hanssen (2005: 2) provides characteristics of a "good operational risk culture":

- Accountabilities are known
- Problems are handled with a sense of urgency
- Proactive identification of operational risks
- Employees are encouraged to raise their hand and seek help
- Investment in operational management reward

3.12 SUMMARY

The Basel II requirements for operational risk will be effective in South Africa from 1 January 2008 and it will be prudent of those South African banks, especially those planning to adopt AMA, to start collecting internal loss data in respect of operational risk events. Losses that have already occurred as a result of operational risk events need to be captured in an internal loss database.

Although the new Capital Accord wants to motivate banks to develop their operational risk methods and eventually move to the more sophisticated approaches, the reality is that many banks will just hold the minimum capital required for operational risk without improving their operational risk practices (Bielski, 2003).

Banks and regulators need to understand that operational risk management is not about arriving at a capital amount (the researcher's own emphasis) to be held for operational risk (Samad-Khan et al., 2006). It is also about the identification and management of operational risk. The researcher's view, confirmed by Anders & Van den Brink (2004), is that both the BIA and the TSA do not abscond banks from having an internal loss database for operational risk purposes to identify and track operational risk losses.

This researcher again refers to Principle 8 of the Sound Practices for the Management and Supervision of Operational Risk. This indicates that "banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management (Basel Committee on Banking Supervision, 2003a: 13). Samad-Khan et al. (2007) confirm the above-mentioned statement and indicate that regardless of what approach banks follow to calculate regulatory capital for operational risk, all

banks should still develop processes for the identification and management of operational risk.

From the above it is clear that there is a need for banks to have an operational risk management framework to manage their operational risks. Banks should not only be driven by regulatory compliance but should realise that there is also a business case for operational risk management. Lam (2001) indicated that we all agree that it is not easy to measure operational risk, but that a bank could gain so much from managing operational risk.

Garver (2006a) refers to the American Banker's first quarter, 2006 Executive Forum online survey for leaders of financial companies, where nearly 400 respondents described how the enhancement of operational risk practices provided added advantages for banks. It is hoped that South African banks, specifically the smaller ones, recognise the business case of identifying, measuring and managing operational risk.

4. CHAPTER 4: RESEARCH METHODOLOGY

This chapter includes an introductory paragraph (emphasising the research problem), the general research methodology, the population and sample size, the measuring instrument to be used, data collection techniques, data analysis methods and the delimitations of this study.

4.1 INTRODUCTION

The purpose of this study was to determine in which areas in South African banks the most severe operational risk losses are likely to occur and to assess the range of practices in collecting internal loss data for operational risk purposes as required by the International Convergence of Capital Instruments and Capital Measurement Standards – A Revised Framework issued in June 2006 (better known, and referred to hereafter, as Basel II).

The study also assesses the prudence of these practices in relation to sound operational risk management practices and applicable recommendations were made where appropriate. The soundness of operational risk practices was approached from a *qualitative* perspective, by benchmarking the research findings against the Basel II text, the Basel Committee on Banking Supervision's Sound Practices for the Management and Supervision of Operational Risk, and related literature from the literature review.

Sub-problems

- Determining in which areas the most *severe* operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).

-
- Determining in which areas the most *frequent* operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).

In assessing the range of practices in collecting internal loss data for operational risk, the following current issues related internal loss data collection practices were assessed:

- Determining the appropriate gross loss amounts for capturing operational risk losses within the internal loss database.
- Determining the range of practices of banks in using gross thresholds for collecting internal loss data.
- Determining whether near misses are recorded in internal loss databases of banks.
- Determining the range practices for *when* (the recognition dates) operational risk losses are recognised and captured in internal loss databases of banks.

4.2 GENERAL RESEARCH METHODOLOGY

The purpose of this study was to determine in which areas in South African banks the most severe operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines) and to assess the range of practices in collecting internal loss data for operational risk purposes as required by the Basel II capital rules.

The investigation of the aforementioned research problem is explorative and quantitative of nature, as the researcher made extensive use of survey research in the form of a questionnaire to all registered banks. According to Leedy & Ormrod (2005: 183) “quantitative survey research involves acquiring information about one or more groups – perhaps about their characteristics, opinions, attitudes, or previous experience – by asking questions and tabulating their

answers. The ultimate goal is to learn about a large population by surveying a sample of that population". The researcher makes extensive use of descriptive statistics.

The assessment of whether the operational risk practices of South African banks are sound was approached from a *qualitative* perspective, by benchmarking the research findings against the Basel II text, the researcher's experience in risk management in banks, the Basel Committee on Banking Supervision's Sound Practices for the Management and Supervision of Operational Risk, and related literature from the literature review.

4.3 POPULATION AND SAMPLE

The researcher is fully aware of the BSD's requirement that all five large banks (Absa Bank Limited, Nedbank Limited, The Standard Bank of South Africa Limited, FirstRand Bank Limited and Investec Bank Limited), irrespective of whether they are targeting the AMA for operational risk on 1 January 2008, develop internal loss databases for the tracking, measuring and monitoring of operational risk.

However, the research intended to include *all* the registered banks in South Africa and thereby representing the total population. The researcher again refers to Principle 8 of the Sound Practices for the Management and Supervision of Operational Risk where it is stated that "banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management" (Basel Committee on Banking Supervision, 2003a: 13).

4.4 MEASURING INSTRUMENT

A questionnaire was sent to all banks registered in South Africa. The questionnaire consisted of closed questions. “The researcher poses a series of questions to willing participants; summarises their responses with percentages, frequency counts, or more sophisticated statistical indexes; and draws inference about a particular population” (Leedy & Ormrod, 2005: 183).

The questionnaire was based on the requirements contained in the Basel II text on operational risk, the Observed Range of Practices for AMA published by the BCBS in October 2006, and issues arising from the review of literature on operational risk.

4.5 DATA COLLECTION

A questionnaire in electronic format was sent to banks via electronic mail after obtaining authorisation from the BSD. The questionnaires were sent to and completed by the official within the individual banks responsible for the centralised operational risk function (usually the Chief Operational Risk Officer).

The questionnaire was in the form of a checklist. “A checklist is a list of behaviours, characteristics, or other entities that a researcher is investigating” (Leedy & Ormrod, 2005: 185). The response deadline for the questionnaires was two weeks from the time the questionnaires were sent to the banks. A follow-up electronic mail as well as several telephone calls was made after the two-week deadline in order to ensure a sufficient response rate.

As there are strong competitive pressures between the banks within the banking system, individual bank information will be considered as confidential.

A literature review that included the following disciplines was conducted:

- Risk management
- Banking regulation
- Operational risk management
- Economic capital

4.6 DATA ANALYSIS METHODS

“Quantitative researchers tend to rely heavily on deductive reasoning, beginning with certain premises and then drawing logical conclusions from them” (Leedy & Ormrod, 2005: 96). Descriptive statistics (e.g. mean, median, range, etc.) was used to analyse the data obtained from the questionnaires. The statistical data analysis functions within Microsoft Excel were used to analyse and interpret the results.

The objective of the research as set out in Chapter 1 of the research report was taken into account in the interpretation of the data. In order to ensure the appropriate interpretation of statistical results, a certain BSD staff member (an actuary) was asked to validate the interpretation of the data.

4.7 LIMITATIONS

Banks were reluctant to divulge actual loss data collected for operational risk purposes. The researcher therefore had to draft a new questionnaire posing questions not based on obtaining the actual internal loss data but on operational risk managers' experience of what they consider to be areas of likely severe operational risk losses in South African banks.

5. CHAPTER 5: RESEARCH RESULTS

Chapter 5 outlines the research results of a study conducted to determine in which areas in South African banks the most severe operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines). The study also assessed the range of practices in collecting internal loss data for operational risk purposes as required by Basel II.

A questionnaire consisting of closed questions was sent to all banks registered in South Africa. The questionnaire was based on the Basel II text on operational risk, the Observed Range of Practices for AMA published by the BCBS in October 2006, and issues arising from the review of literature on operational risk.

5.1 BIOGRAPHIC PROFILE OF RESPONDENTS

The questionnaire was sent out to staff in charge of the operational risk function of all registered banks in South Africa. The study excluded the 3 mutual banks. Mutual banks are not required to adopt Basel II on 1 January 2008. The questionnaire was thus sent out to all 33 banks (total population).

Eleven of the 33 operational risk officers responded to the questionnaire. This equalled to a 33,3% response rate. The profiles of the respondents are outlined below in *Table 3*:

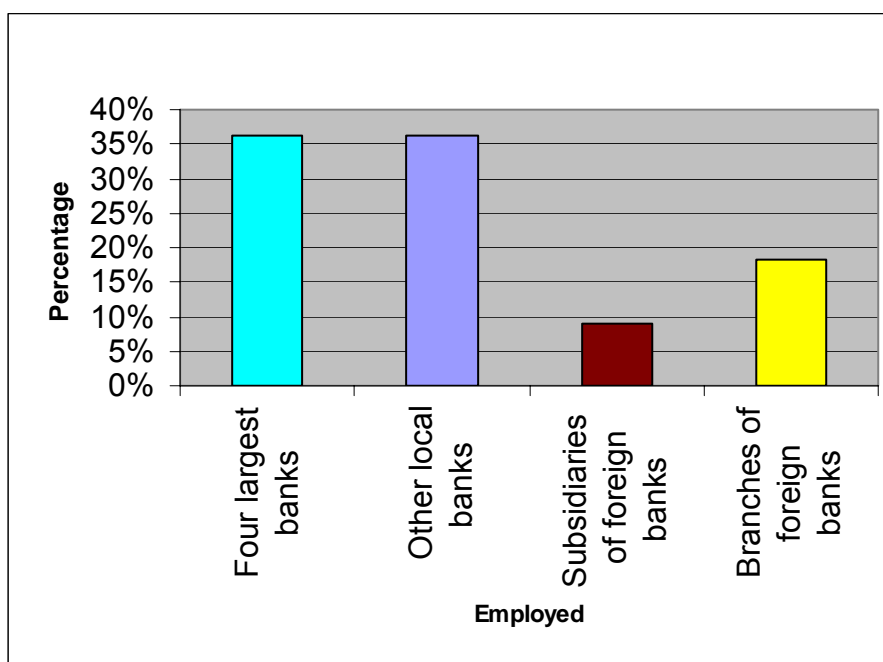
Table 3: Biographic profile of respondents

	<i>Frequency</i>	<i>Relative frequency (%)</i>	<i>Cumulative frequency</i>	<i>Cumulative frequency (%)</i>
<i>Employment</i>				
Four largest banks	4	36%	4	36%
Other local banks	4	36%	8	73%
Subsidiaries of foreign banks	1	9%	9	82%
Branches of foreign banks	2	18%	11	100%
<i>Banking experience</i>				
1 - 5 years	1	9%	1	9%
6 - 10 years	5	45%	6	55%
11 - 15 years	4	36%	10	91%
> 15 years	1	9%	11	100%
<i>Operational risk experience</i>				
1 - 3 years	2	18%	2	18%
4 - 6 years	7	64%	9	82%
7 - 9 years	1	9%	10	91%
> 9 years	1	9%	11	100%

5.1.1 Employment

It is important to note that responses from all types of banks were received ranging from the four largest banks, other local banks, subsidiaries of foreign banks and branches of foreign banks. Also important is that all four of the largest banks responded to the questionnaire. The responses were, however, dominated by the four largest banks in South Africa and other local banks each representing 36%, respectively, of respondents. A graphical illustration of where respondents were employed is depicted in *Figure 4* below:

Figure 4: Histogram – respondent distribution

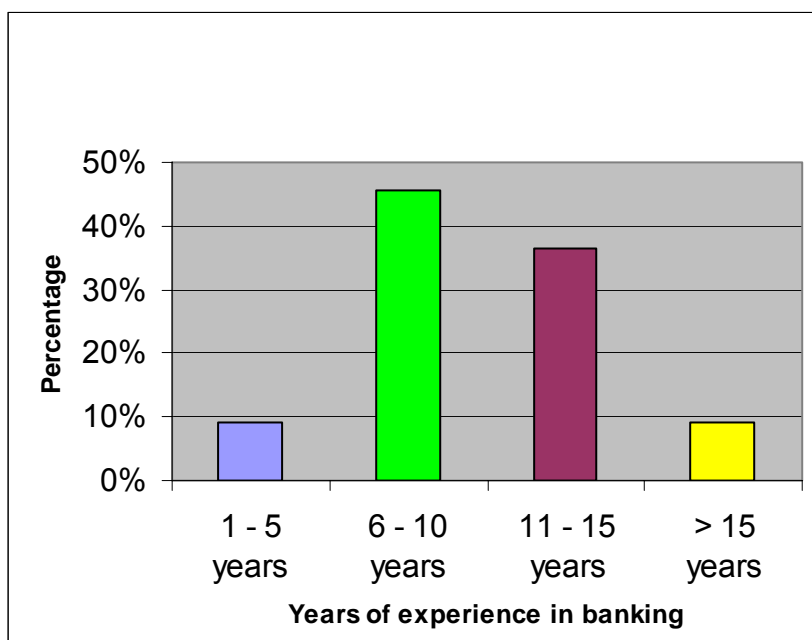


5.1.2 Banking experience

The larger group of respondents (45%) had banking experience in the category (6 -10 years). The second largest number of respondents (36%) had banking experience of between 11 and 15 years.

See *Figure 5* depicting the distribution of respondents in terms of number of years employed in the banking sector.

Figure 5: Frequency distribution: banking experience

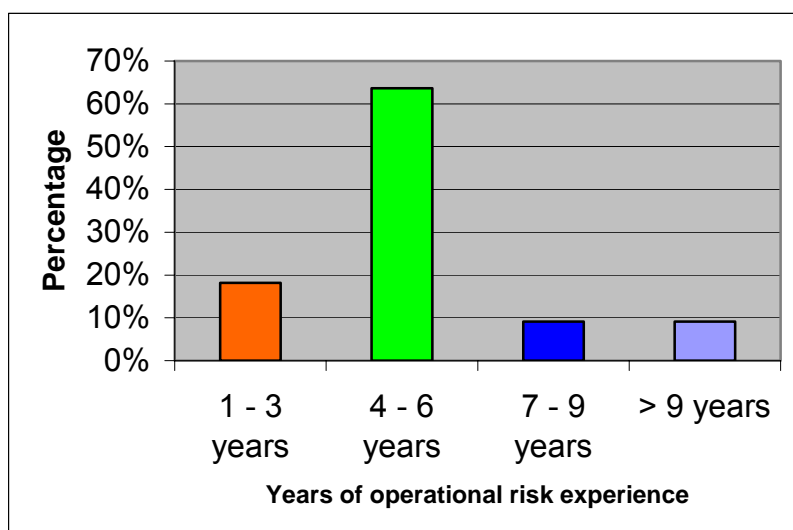


5.1.3 Operational risk experience

A majority of respondents (64%) had operational risk experience in the category (4 - 6 years). Operational risk functions within banks are relatively new seeing that prior to the introduction of Basel II not many banks had dedicated operational risk officers and operational risk functions. Operational risk was managed on a reactive basis rather than proactively.

See *Figure 6* below depicting the distribution of respondents in terms of their number of years experience in operational risk.

Figure 6: Operational risk experience of respondents



5.2 DESCRIPTIVE STATISTICS FOR LIKELY SEVERE OPERATIONAL RISK EVENTS

Questions 4 to 8 were based on the seven loss event types and eight business lines as specified in the Basel II text. A four-point scale was used for questions 4 to 8 of the questionnaire. A rating was required for each item of the seven loss event types and eight business lines. A rating of 1 indicated very low severity, 2 only slightly severe events, 3 a severe event and a rating of 4 indicated an extreme severe operational risk event. The researcher will first address the objectives of the research below, and thereafter other pertinent results from other questions included in the questionnaire.

5.2.1 Loss event types

Summary description statistics in respect of the likely *severe* operational risk losses in terms of the Basel II seven loss event types are depicted below:

Table 4: Descriptive statistics: likely severe operational risk losses – loss event types

	<i>Internal fraud</i>	<i>External fraud</i>	<i>EPWS</i>	<i>CPBP</i>	<i>Damage to assets</i>	<i>BDSF</i>	<i>EDPM</i>
Mean	1.6	2.6	1.5	2.4	2.1	3.2	3.0
Standard error	0.2	0.3	0.2	0.3	0.3	0.2	0.2
Median	2.0	3.0	1.0	2.0	2.0	3.0	3.0
Mode	2.0	3.0	1.0	3.0	1.0	3.0	3.0
Standard deviation	0.5	0.9	0.7	0.9	1.0	0.8	0.6
Sample variance	0.3	0.9	0.5	0.9	1.1	0.6	0.4
Kurtosis	-2.0	-0.4	1.0	-0.4	-0.9	-0.9	0.4
Skewness	-0.7	0.0	1.3	0.0	0.4	-0.3	0.0
Range	1	3	2	3	3	2	2
Minimum	1	1	1	1	1	2	2
Maximum	2	4	3	4	4	4	4
Sum	18	29	16	26	23	35	33
Count	11	11	11	11	11	11	11

* EPWS Employment and workplace safety

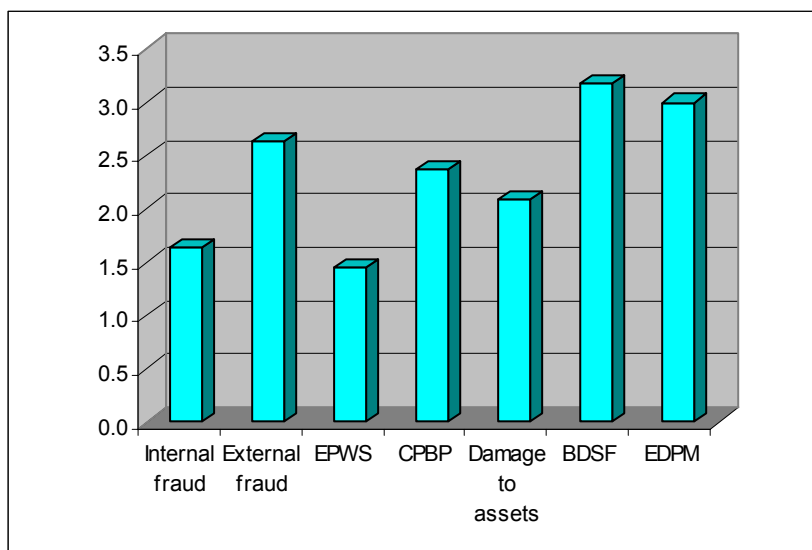
* CPBP Clients, products and business practices

* BDSF Business disruption and system failures

* EDPM Execution, delivery and process management

Figure 7 depicts the average ratings of likely severe operational risk events per Basel II loss event types.

Figure 7: Mean distribution – likely severity of loss event types



- Internal fraud

The average rating of 1.6 is very low. In fact, the rating represents the second lowest of all average ratings of likely severe operational risk loss event types. A range of 1 was reported which indicates a low variability in ratings scored. This also points to most respondents rating this category as having a *low likelihood* of a severe operational risk event.

The mode = 2. None of the respondents gave a rating of 3 or above. See *Table 5* below reflecting the distribution of ratings:

Table 5: Distribution of ratings: likely severity of 'internal fraud'

% of ratings on four-point scale				
	1	2	3	4
Internal fraud	36%	64%	0%	0%

- External fraud

External fraud ranked third in terms of the highest average rating assigned to likely fraud. An average rating of 2.6 was reported by respondents. However, a range of 3 was reported indicating a high variability in the scores from low to high ratings. The mode is reported as 3, with most ratings in the 2 and 3 rating categories.

See *Table 6* depicting the distribution of ratings:

Table 6: Distribution of ratings: likely severity of 'external fraud'

% of ratings on four-point scale				
	1	2	3	4
External fraud	9%	36%	36%	19%

- Employment practices and workplace safety

This loss event type ranked the lowest with an average score of 1.5 as a likely severe operational risk event. This category scored a range of 2. The aforementioned range indicates low variability on a four-point scale. The mode = 1. Also see *Table 7* below reflecting the distribution of ratings on a four-point scale:

Table 7: Distribution of ratings: likely severity of 'employment practices and workplace safety'

% of ratings on four-point scale				
	1	2	3	4
EPWS	64%	27%	9%	0%

- Clients, products and business practices

An average rating of 2.4 was reported on a four-point scale. This rating ranked fourth in terms of severity. A range of 3 was reported indicating that there was a high variability in the scores from low to high ratings. See *Table 8* depicting the distribution of ratings:

Table 8: Distribution of ratings: likely severity of 'client, products and business practices'

% of ratings on four-point scale				
	1	2	3	4
CPBP	18%	36%	36%	9%

- Damage to physical assets

The average rating of 2.1 is the third lowest rating. A range of 3 was reported indicating that there was a wide variability in the scores between 1 and 3. See *Table 9* depicting the distribution of ratings:

Table 9: Distribution of ratings: likely severity of 'damage to physical assets'

% of ratings on four-point scale				
	1	2	3	4
Damage to assets	36%	27%	27%	9%

- Business disruption and system failures

The highest average rating of 3.2 on a four-point scale was scored in this category. The mode = 3. The majority of respondents rated this category 3 and above. This is an indication that operational risk managers in banks considered this to be the most likely area where a severe operational risk event might occur. A range of 2 was reported which indicates a fairly low variability in ratings scored. See *Table 10* below depicting the distribution of ratings:

Table 10: Distribution of ratings: likely severity of 'business disruptions and system failures'

% of ratings on four-point scale				
	1	2	3	4
BDSF	0%	18%	45%	36%

- Execution, delivery and process management

A high average rating of 3 was scored for execution, delivery and process management on a four-point scale.

The mode = 3. See *Table 11* reflecting the distribution of ratings:

Table 11: Distribution of ratings: likely severity of 'execution, delivery and process management'

% of ratings on four-point scale				
	1	2	3	4
EDPM	0%	18%	64%	18%

5.2.2 Business lines

Summary description statistics in respect of the likely severe operational risk losses in terms of the Basel II seven business lines are depicted in *Table 12* below:

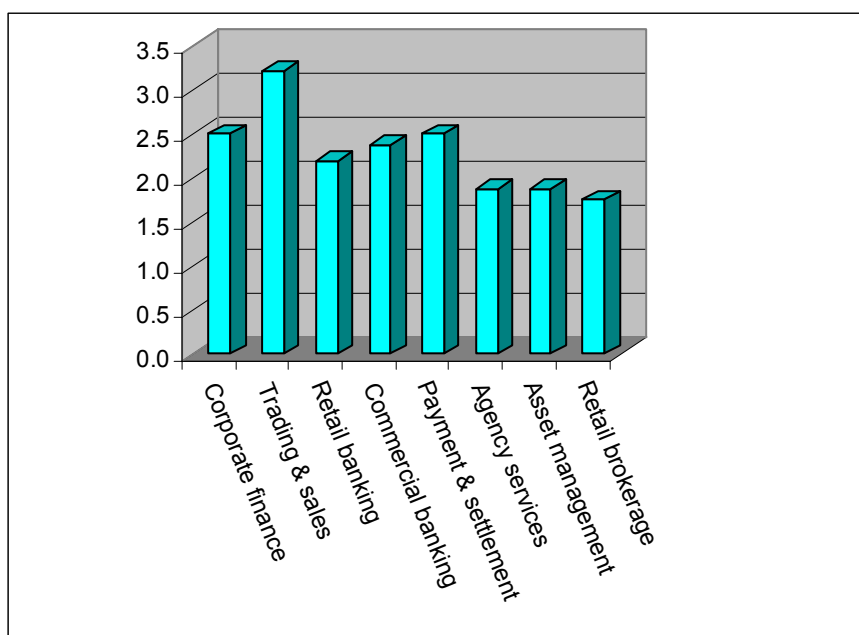
Table 12: Descriptive statistics: likely severe operational risk losses - business lines

	<i>Corporate finance</i>	<i>Trading & sales</i>	<i>Retail banking</i>	<i>Commercial banking</i>	<i>Payment & settlement</i>	<i>Agency services</i>	<i>Asset management</i>	<i>Retail brokerage</i>
Mean	2.5	3.2	2.2	2.4	2.5	1.9	1.9	1.8
Standard Error	0.5	0.2	0.2	0.4	0.2	0.4	0.3	0.4
Median	3.0	3.0	2.0	2.5	2.5	1.5	2.0	1.5
Mode	3	3	2	3	3	1	1	1
Standard Deviation	1.3	0.7	0.6	1.1	0.5	1.1	0.8	1.0
Sample Variance	1.7	0.4	0.4	1.1	0.3	1.3	0.7	1.1
Kurtosis	-1.9	0.0	0.2	-0.9	-2.8	0.3	-1.4	3.1
Skewness	-0.3	-0.3	-0.1	0.0	0.0	1.1	0.3	1.7
Range	3	2	2	3	1	3	2	3
Minimum	1	2	1	1	2	1	1	1
Maximum	4	4	3	4	3	4	3	4
Sum	20	29	22	19	20	15	15	14
Count	8	9	10	8	8	8	8	8

* Values for business lines not applicable to specific banks were not taken into consideration in the calculations

Figure 8 depicts the average ratings of likely severe operational risk event per the eight Basel II business lines.

Figure 8: Mean distribution – likely severe events in business lines



- Corporate finance

The average rating of 2.5 is very low on four-point scale. A range of 3 was reported which indicates a fairly high variability in ratings scored. See *Table 13* below depicting the variability in ratings:

Table 13: Distribution of ratings: likely severity – corporate finance

% of ratings on four-point scale				
	1	2	3	4
Corporate finance	38%	0%	38%	25%

- Trading and sales

This category scored the highest average rating of 3.2, indicating a high likelihood of a severe operational risk event. The mode = 3. The majority of respondents rated this category 3 or 4. This is an indication that operational risk managers in banks considered this to be the most likely business line where a severe operational risk event might occur. A range of 2 was reported which indicates a fairly low variability in ratings scored. See *Table 14* depicting the distribution of ratings:

Table 14: Distribution of ratings: likely severity – trading and sales

% of ratings on four-point scale				
	1	2	3	4
T&S	0%	11%	56%	33%

- Retail banking

Retail banking scored a high average of 2.2 on a four-point scale. Mode = 2. See *Table 15* below depicting the distribution of ratings:

Table 15: Distribution of ratings: likely severity – retail banking

% of ratings on four-point scale				
	1	2	3	4
Retail banking	10%	60%	30%	0%

- Commercial banking

A low average score of 2.4 was reported in this category. A range of 3 was reported, which indicates a fairly high variability in ratings scored. See *Table 16* depicting the distribution of ratings:

Table 16: Distribution of ratings: likely severity – commercial banking

% of ratings on four-point scale				
	1	2	3	4
Commercial banking	25%	25%	38%	13%

- Payment and settlement

A low average rating of 2.5 was scored in this category.

- Agency services

A low average rating of 1.9 was scored in this category.

- Asset management

A low average rating of 1.9 was scored in this category.

- Retail brokerage

A low average rating of 1.8 was scored in this category.

5.3 LIKELY FREQUENCY OF OPERATIONAL RISK EVENTS

5.3.1 Loss event types

Summary description statistics in respect of the likely *frequency* of operational risk losses in terms of the Basel II seven loss event types are depicted below:

Table 17: Descriptive statistics: likely frequency of operational risk losses – loss event types

	<i>Internal fraud</i>	<i>External fraud</i>	<i>EPWS</i>	<i>CPBP</i>	<i>Damage to assets</i>	<i>BDSF</i>	<i>EDPM</i>
Mean	2	2.9	1.4	2.2	1.4	2	2.9
Standard error	0.2	0.3	0.2	0.3	0.2	0.3	0.3
Median	2	3	1	2	1	2	3
Mode	2	4	1	2	1	2	4
Standard deviation	0.6	1.1	0.5	0.9	0.7	0.9	1.0
Sample variance	0.4	1.3	0.3	0.8	0.5	0.8	1.1
Kurtosis	0.4	-0.5	-2.0	0.8	2.6	1.6	-0.9
Skewness	0	-0.8	0.7	0.7	1.8	1.0	-0.4
Range	2	3	1	3	2	3	3
Minimum	1	1	1	1	1	1	1
Maximum	3	4	2	4	3	4	4
Sum	22	32	15	24	15	22	32
Count	11	11	11	11	11	11	11

* EPWS Employment and Workplace Safety

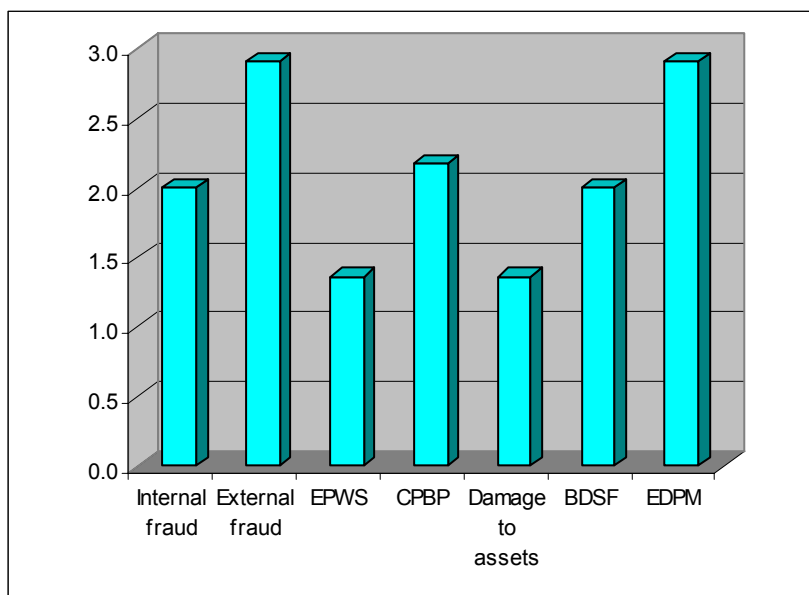
* CPBP Clients, products and business practices

* BDSF Business disruption and system failures

* EDPM Execution, delivery and process management

Figure 9 depicts the average ratings of the likely frequency of operational risk events per Basel II loss event types.

Figure 9: Mean distribution – likely frequency of loss event types



- Internal fraud

An average rating of 2 was scored. Sixty-four percent of scores were '2' ratings. See *Table 18* below depicting the distribution of ratings:

Table 18: Distribution of ratings: likely frequent events – internal fraud

% of ratings on four-point scale				
	1	2	3	4
Internal fraud	18%	64%	18%	0%

- External fraud

External fraud scored the highest average rating (2.9) in terms of the likely frequency of operational risk events. The majority of respondents rated this category 3 or 4. See *Table 19* depicting the distribution of ratings:

Table 19: Distribution of ratings: likely frequent events – external fraud

% of ratings on four-point scale				
	1	2	3	4
External fraud	18%	9%	36%	36%

- Employment practices and workplace safety

This category scored the lowest average rating (1.4) in terms of likely frequency of operational risk losses. See *Table 20* depicting the distribution of ratings:

Table 20: Distribution of ratings: likely frequent events – employment practices and workplace safety

% of ratings on four-point scale				
	1	2	3	4
EPWS	64%	36%	0%	0%

- Clients, products and business practices

An average rating of 2.2 was scored in this category on a four-point scale. See *Table 21* below depicting the distribution of ratings:

Table 21: Distribution of ratings: likely frequent events – clients, products and business practices

% of ratings on four-point scale				
	1	2	3	4
CPBP	18%	55%	18%	9%

- Damage to physical assets

A low average rating of 1.4 was scored in this category in terms of likely frequency of operational risk events. See *Table 22* depicting the distribution of ratings:

Table 22: Distribution of ratings: likely frequent events – damage to physical assets

% of ratings on four-point scale				
	1	2	3	4
Damage to assets	73%	18%	9%	0%

- **Business disruption and system failures**

This category scored a low rating of 2 on a four-point scale. See Table 23 depicting the distribution of ratings:

Table 23: Distribution of ratings: likely frequent events – business disruptions and system failures

% of ratings on four-point scale				
	1	2	3	4
BDSF	27%	55%	9%	9%

- **Execution, delivery and process management**

This category scored the highest average rating of 2.9. Ratings were spread across the 2, 3 and 4 rating categories. See Table 24 depicting the distribution of ratings:

Table 24: Distribution of ratings: likely frequent events – execution, delivery and process management

% of ratings on four-point scale				
	1	2	3	4
EDPM	9%	27%	27%	36%

5.3.2 Business lines

Summary description statistics in respect of the likely frequency of operational risk losses in terms of the Basel II eight business lines are depicted in *Table 25* below:

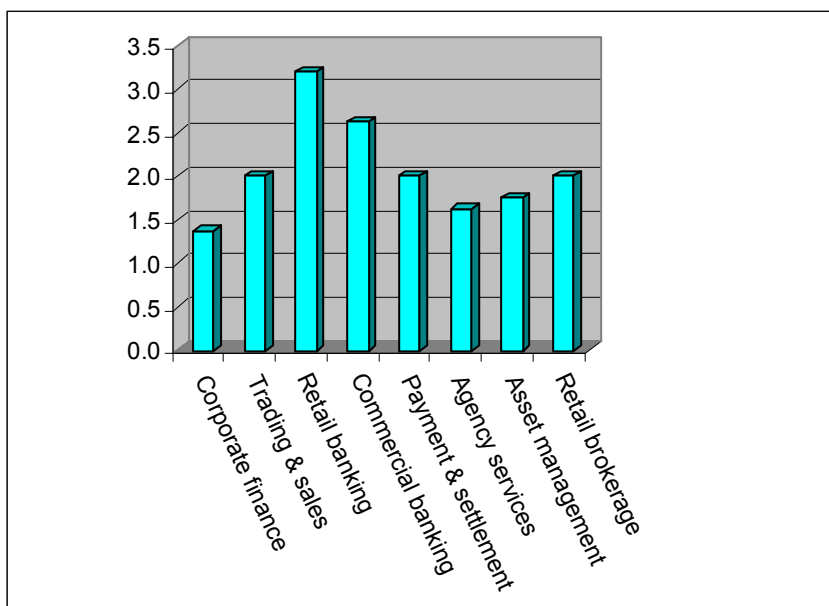
Table 25: Descriptive statistics: likely frequency of operational risk losses – business lines

	<i>Corporate finance</i>	<i>Trading & sales</i>	<i>Retail banking</i>	<i>Commercial banking</i>	<i>Payment & settlement</i>	<i>Agency services</i>	<i>Asset management</i>	<i>Retail brokerage</i>
Mean	1.4	2.0	3.2	2.6	2.0	1.6	1.8	2.0
Standard error	0.3	0.2	0.3	0.3	0.4	0.4	0.3	0.5
Median	1	2	3.5	2.5	2	1	1.5	1
Mode	1	2	4	2	2	1	1	1
Standard deviation	0.7	0.7	1.0	0.7	1.1	1.2	0.9	1.4
Sample variance	0.6	0.5	1.1	0.6	1.1	1.4	0.8	2.0
Kurtosis	3.2	-0.3	0.9	-0.2	0.4	1.4	-1.5	-1.6
Skewness	2.0	0.0	-1.2	0.8	0.9	1.7	0.6	0.8
Range	2	2	3	2	3	3	2	3
Minimum	1	1	1	2	1	1	1	1
Maximum	3	3	4	4	4	4	3	4
Sum	11	18	32	21	16	13	14	16
Count	8	9	10	8	8	8	8	8

* Values for business lines not applicable to specific banks were not taken into consideration in the calculations

Figure 10 depicts the average ratings of the likely frequency of operational risk events per Basel II business lines.

Figure 10: Mean distribution: likely frequency of events in business lines



- Corporate finance

A low average rating of 1.4 was scored in this category. See *Table 26* below depicting the variability in ratings:

Table 26: Distribution of ratings: likely frequent events – corporate finance

	% of ratings on four-point scale			
	1	2	3	4
Corporate finance	75%	13%	13%	0%

- Trading and sales

An average rating of 2 indicates an average likelihood in terms of the frequency of operational risk events in this category. The mode = 2. See *Table 27* depicting the distribution of ratings:

Table 27: Distribution of ratings: likely frequent events – trading and sales

% of ratings on four-point scale				
	1	2	3	4
T&S	22%	56%	22%	0%

- Retail banking

Retail banking scored the highest average score of 3.2 on a four-point scale. The mode = 4. See *Table 28* depicting the distribution of ratings:

Table 28: Distribution of ratings: likely frequent events – retail banking

% of ratings on four-point scale				
	1	2	3	4
Retail banking	10%	20%	30%	50%

- Commercial banking

A low average score of 2.6 was reported in this category. The mode = 2. See *Table 29* depicting the distribution of ratings:

Table 29: Distribution of ratings: likely frequent events – commercial banking

% of ratings on four-point scale				
	1	2	3	4
Commercial banking	0%	50%	38%	13%

- Payment and settlement

A low average rating of 2 was scored in this category. See the *Table 30* depicting the distribution of ratings:

Table 30: Distribution of ratings: likely frequent events – payment and settlement

% of ratings on four-point scale				
	1	2	3	4
P & S	38%	38%	13%	13%

- Agency services

A low average rating of 1.6 was scored in this category.

- Asset management

A low average rating of 1.8 was scored in this category.

- Retail brokerage

A low average rating of 2 was scored in this category.

5.4 LOSS DATA COLLECTION PRACTICES

This section contains the research findings (research results) on practices in capturing internal loss data for operational risk purposes.

Questions 9 to 23 of the questionnaire focused on the assessment of the range of practices in collecting internal loss data for operational risk purposes as required by Basel II. The aforementioned questions were based on a questionnaire internally circulated among the members of the AIGOR.

All results from responses on questions to assess the range of practices in collecting internal loss data for operational risk purposes are depicted in the figures below.

Figure 11: Inclusion of near misses in loss database

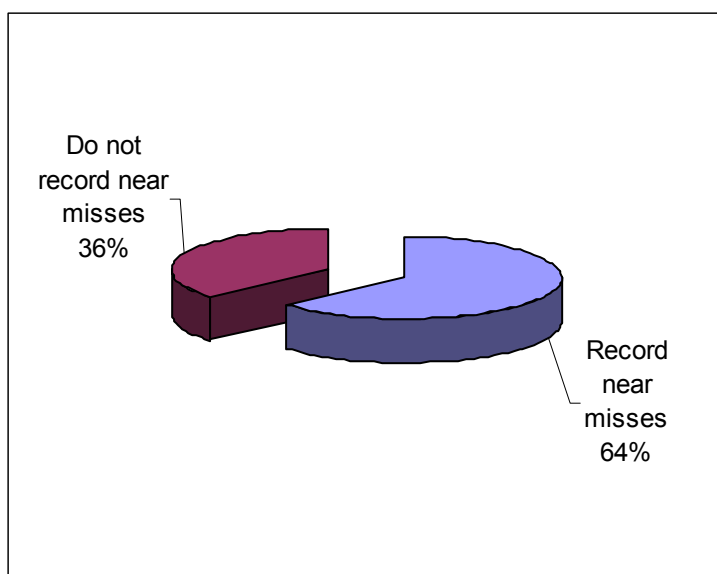


Figure 12: Recording of opportunity cost in loss database

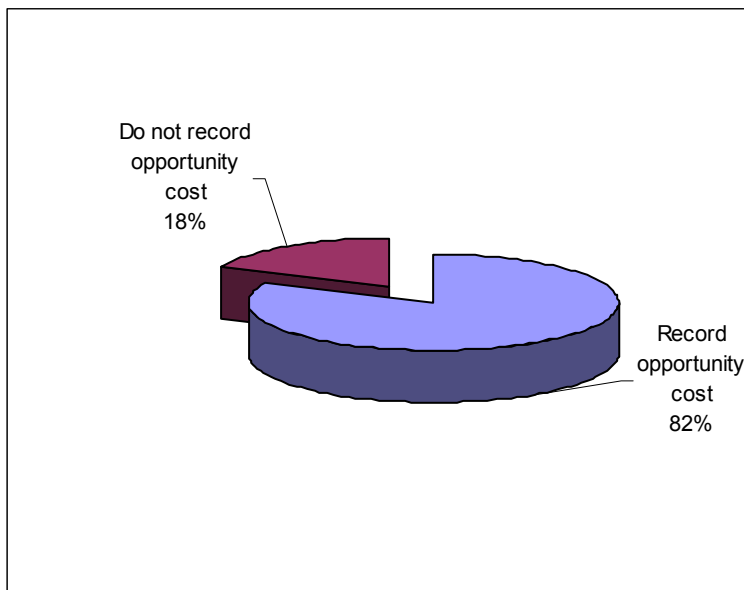


Figure 13: Recording of overtime cost in loss database

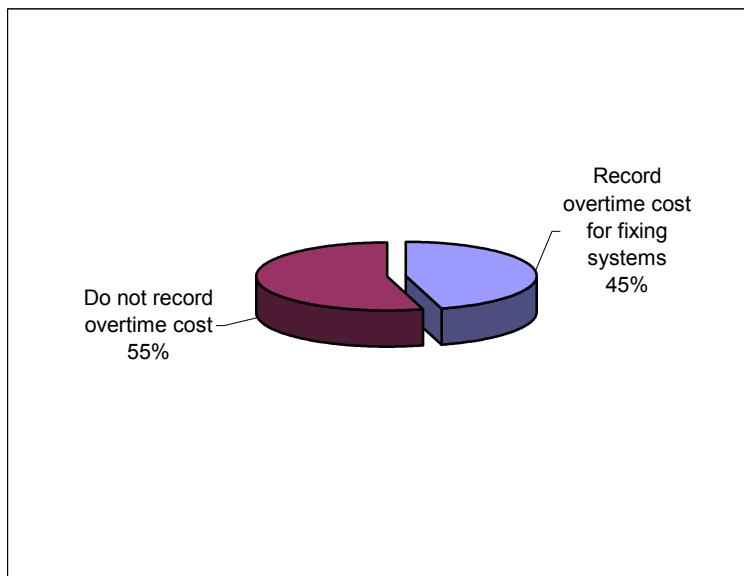


Figure 14: Date of recording of operational risk losses

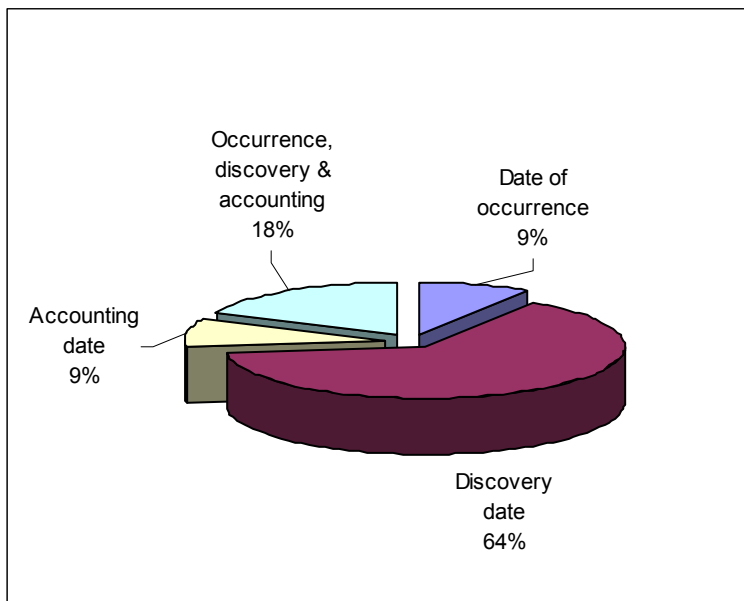


Figure 15: Assignment of internal losses to business units

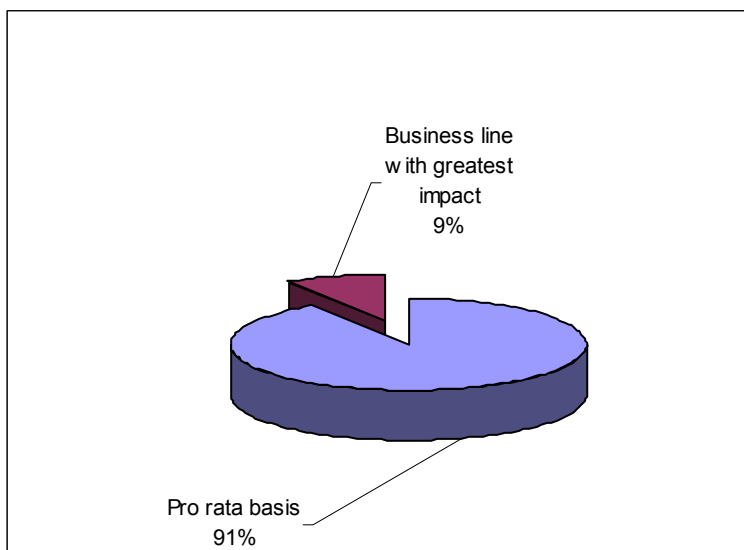


Figure 16: Recording of insurance recoveries

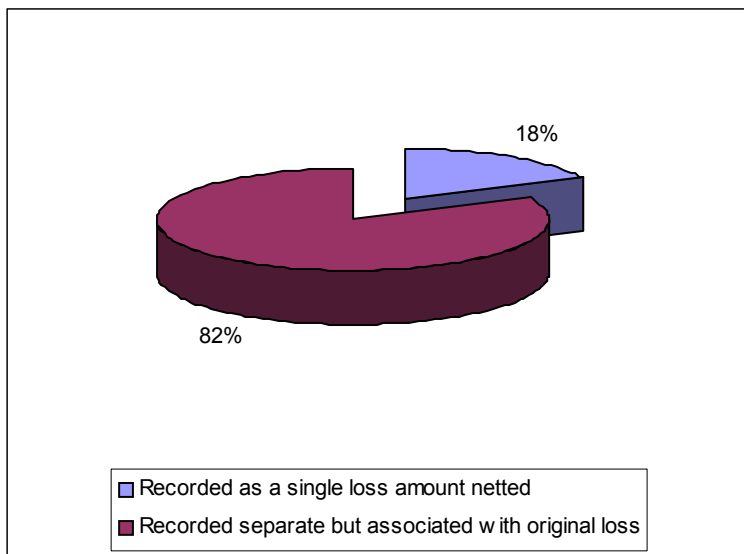


Figure 17: Recording of other recoveries

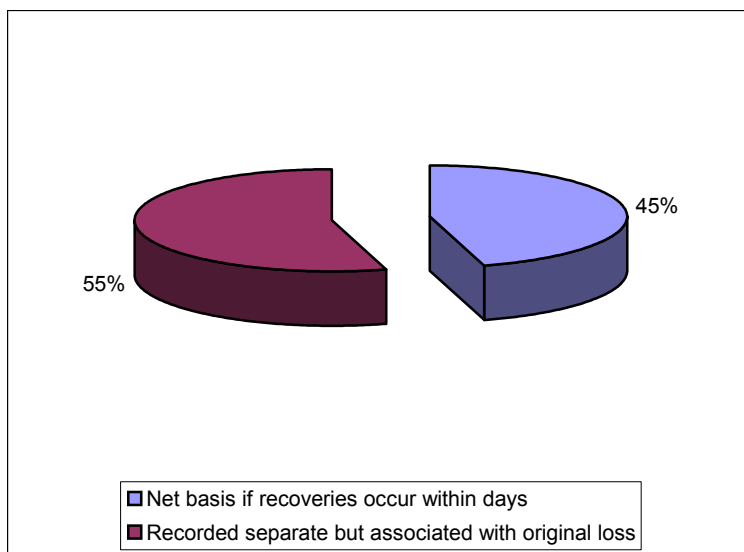


Figure 18: Damage to fixed assets

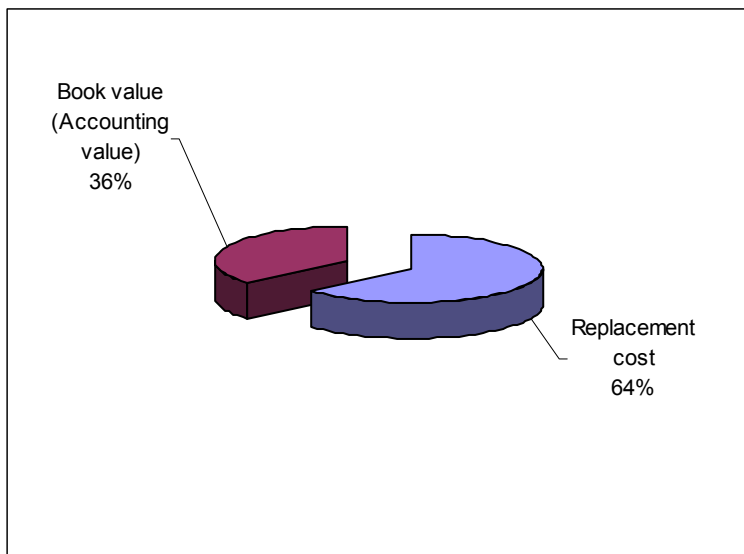


Figure 19: Assignment of market risk losses due to operational risk events

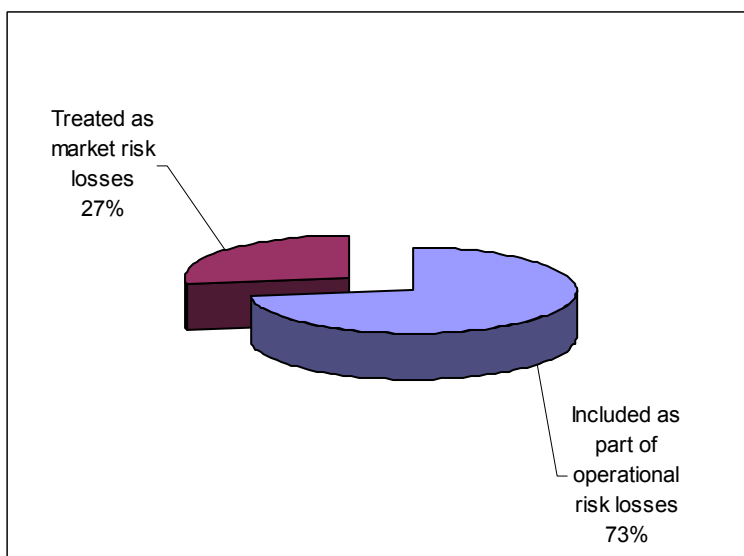


Figure 20: Assignment of loan-related operational risk losses

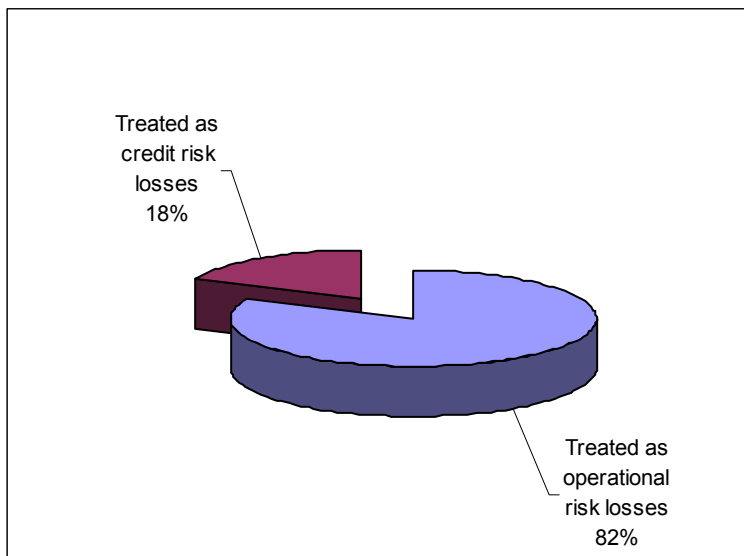


Figure 21: Loss data collection thresholds

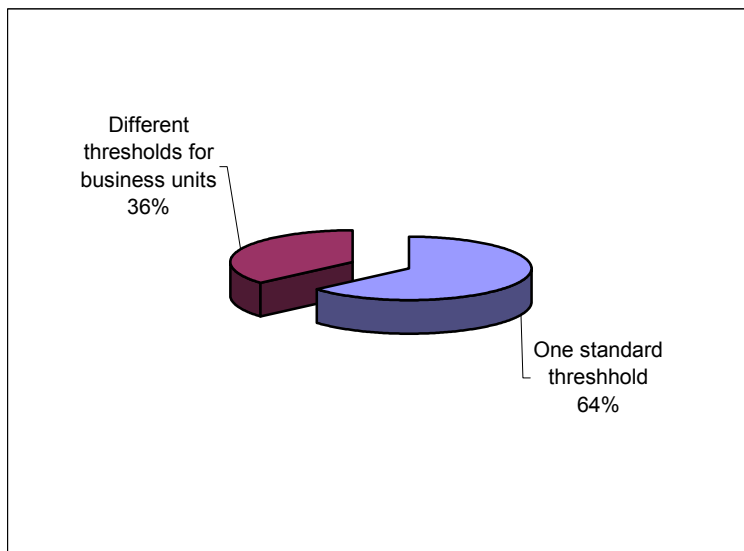


Figure 22: Mapping matrixes

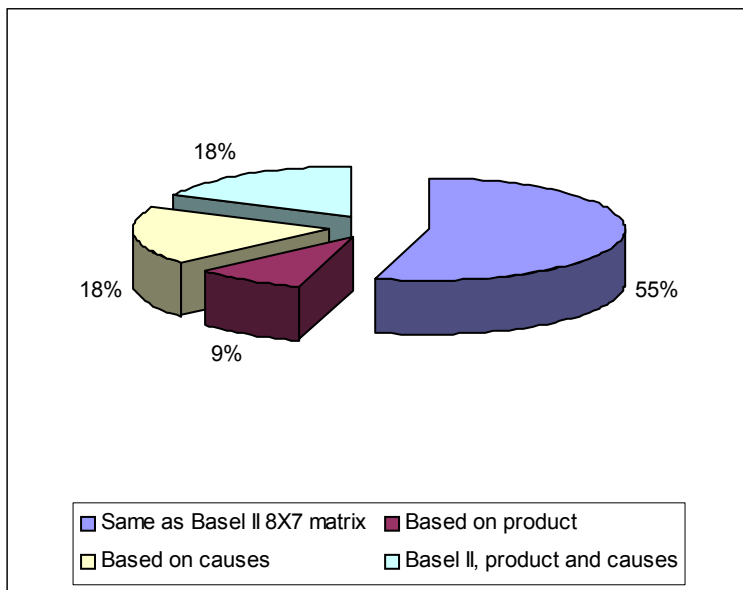


Figure 23: Mapping of data on consolidated or legal entity basis

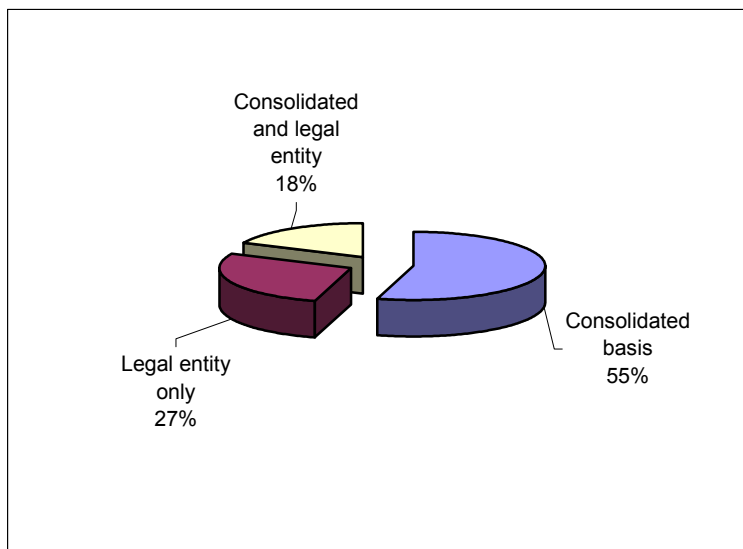
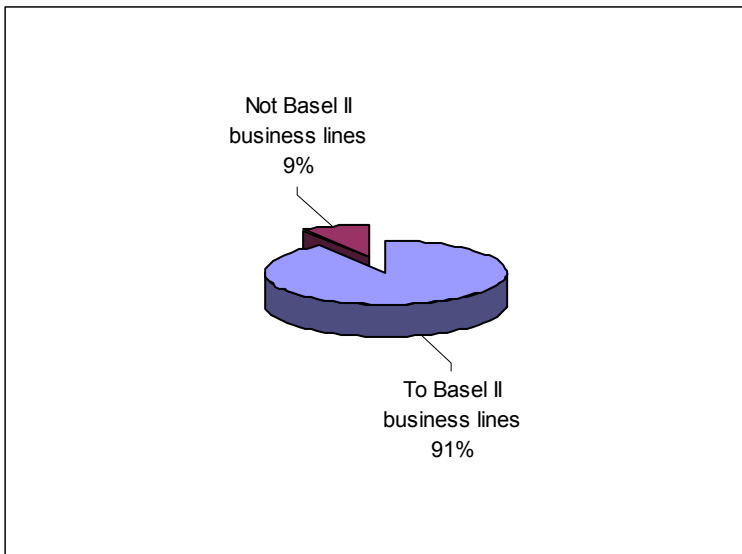


Figure 24: Mapping of gross income



6. CHAPTER 6: DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

The purpose of this chapter is to:

- discuss the findings of the research results as outlined in Chapter 5;
- compare the research findings of determining likely severe operational risk losses in South African banks with the findings of the Operational Risk Loss Data Collection Exercise conducted by the Risk Management Group of the BCBS in 2002;
- benchmark the research finding of assessing the range of practices in collecting internal loss data for operational risk purposes with the paper issued by the BCBS in 2006 titled “Observed range of practice in key elements of the Advanced Measurement Approaches (AMA)”; and
- link the research findings to the research objectives as outlined in Chapter 1.

A structured questionnaire containing 23 questions was sent to persons in charge of the operational risk functions of all banks and branches of foreign banks registered in South Africa. The three mutual banks were excluded from the study, as they are not required to implement Basel II in January 2008. The questionnaire was sent to the total population of banks that will be required to comply with Basel II as from 1 January 2008. Of the remaining 33 banks and branches of foreign banks, 11 banks, including branches of foreign banks responded to the questionnaire. This is a response rate of 33 percent.

6.1 DISCUSSION OF RESULTS: LIKELY SEVERE OPERATIONAL RISK LOSSES IN SOUTH AFRICAN BANKS

The results of the first part of the research problem and its sub-problems will be discussed below:

Determining in which areas in South African banks the most severe operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).

- a) Determining in which areas the most severe operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).

The research results revealed that respondents in South African banks believed that the loss event type '*business disruption and system failures*' are likely to result in the most severe single operational risk loss. These results are *not consistent* with the Operational Risk Loss Data Collection Exercise conducted by the Risk Management Group of the BCBS in 2002 where eighty-nine banks submitted over 47,000 operational risk loss events captured in their internal loss databases. The results revealed that '*business disruption and system failures*' represented the lowest impact (approximately 2%) in terms of severe operational risk losses captured in the internal loss databases of the 89 participating banks (Basel Committee on Banking Supervision, 2003b).

However, the above-mentioned results of this study may be attributable to the uncertainty of corporations of the consistency of power supplies by Eskom, the national electricity provider. During the past two years South African individuals and corporations had to contend with many power outages which resulted in a loss in business as well as a loss in

confidence in the electricity supplier. Telkom, the main telecommunications provider in South Africa, does not in all circumstances adequately meet customers' needs. During the past year retail banks experienced an increase in bombings of automated teller machines, which may have influenced the responses.

'Trading and sales' scored the same high average rating as *'business disruption and system failures'*. This was identified as the business line where the most severe single operational risk loss is likely to occur in South African banks. Trading and sales represents a high-risk area for most banks engaged in these activities. *'Trading and sales'* includes a bank's treasury function, market making activities and proprietary positions in fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repurchase agreements, brokerage, debt and prime brokerage" (Basel Committee on Banking Supervision, 2006a). Most of the income obtained from this business line is very volatile, and not of repetitive.

- b) Determining in which areas the most frequent operational risk losses are likely to occur (based on the Basel II seven loss event types and eight business lines).

'External fraud' (an average rating of 2.9) and *'execution, delivery and process management'* (also an average rating of 2.9) scored the highest average ratings as the loss event types where the most frequent operational risk losses are likely to occur. These results are consistent with the Operational Risk Loss Data Collection Exercise conducted by the Risk Management Group of the BCBS in 2002 where eighty-nine banks submitted over 47,000 operational risk losses captured in their internal loss databases. The results revealed that the loss event type *'external fraud'* represented the highest frequency of operational risk losses at

approximately 45% of all operational risk losses reported by participating banks (Basel Committee on Banking Supervision, 2003b). 'Execution, delivery and process management' represented the second highest frequency of operational risk losses at approximately 35% of all operational risk losses reported by participating banks (Basel Committee on Banking Supervision, 2003b).

Respondents indicated that '*retail banking*' is the business line where the most frequent single operational risk losses are likely to occur in South African banks. 'Commercial banking' also scored high in terms of the business line where the most frequent single operational risk losses are likely to occur. These results are in agreement with the Operational Risk Loss Data Collection Exercise conducted by the Risk Management Group of the BCBS in 2002 where it was indicated that 61% of operational risk losses occur within retail banking (Basel Committee on Banking Supervision, 2003b). Commercial banking was the second highest business line in terms of the frequency of operational risk losses, at approximately 23% of all operational risk losses reported by participating banks (Basel Committee on Banking Supervision, 2003b). In the business lines of retail and commercial banking the volume of transactions runs into the hundreds of thousands per day. The aforementioned findings are also consistent with the statement by Hughes (2005) who indicates that operational risk increases as the number of transactions in banks increases.

Frequently occurring single operational risk losses do not have a severe impact in monetary terms. However, if management does not put controls in place to limit the occurrence of these losses the aggregate monetary values of these losses could amount to millions of rands.

6.2 CONCLUSION AND RECOMMENDATION: LIKELY SEVERE OPERATIONAL RISK LOSSES IN SOUTH AFRICAN BANKS

It is evident that the high-risk operational risk areas in banks, in terms of the severity of single operational risk loss events are:

- losses due to 'business disruption and system failures'; and
- losses within the 'trading and sales' areas of banks.

The BSD, boards of directors and senior management of banks should focus their attention on strengthening banks' internal controls relating to these events.

Based on the discussions of the most likely frequency of operational risk events, the BSD, boards of directors and senior management of banks should focus their attention on strengthening banks' internal controls related to:

- losses due to 'external fraud'; and
- losses within the 'retail banking' business line.

The researcher believes that the objectives of the first part of the research study have been met as the aforementioned areas identified serve as a basis for the following:

- It provides guidance to banking regulators, specifically the BSD, on the high-risk areas they should focus their supervisory duties on in respect of operational risk in South African banks.
- It also serves as a guideline to the boards of directors and the senior management of banks on what areas of operational risk to focus their attention to reduce operational risk losses.
- It provides an indication to senior management of banks in which business areas these operational risk losses are likely to occur.

6.3 DISCUSSION OF RESULTS, CONCLUSIONS AND RECOMMENDATIONS: RANGE OF PRACTICES IN COLLECTING INTERNAL LOSS DATA FOR OPERATIONAL RISK

The findings outlined in Section 5.4 will serve as a basis for benchmarking internal loss data collection practices in South African banks for operational risk purposes. The results of the study will be shared with the BSD. It was, however, not the objective of the study to be prescriptive to banks in terms of the outcome of the study. The goal of the study was to determine the range of practices and then assess criteria for acceptable practice. The researcher's view is that the practices adopted by the majority of respondents represented acceptable practices for collecting loss data for operational risk.

The findings may also be used by the BSD as “a means of framing the discussion of acceptable practice in both the management and measurement of operational risk” (Basel Committee on Banking Supervision, 2006b: 2).

The findings are summarised below:

a) Near misses

It appears that the majority of banks prefer the inclusion of near misses in their internal loss databases. A large percentage (64%) of the banks that responded indicated that they record near misses in internal operational risk loss event databases. All four of the largest banks' operational risk managers indicated that they do record near misses. 'No' answers were mainly from smaller local banks and some branches of foreign banks.

“Given the general scarcity of operational risk loss data, however, near miss data could be useful in both risk management and measurement” (Basel Committee on Banking Supervision, 2006b: 16). The researcher therefore

concludes that the inclusion of near misses in internal loss databases is an acceptable practice for loss data collection.

b) Opportunity cost

Eighty-two percent of banks that responded indicated that they record opportunity cost in internal operational risk loss event databases. Only one large bank and one smaller South African bank indicated that they do not record the opportunity cost of an operational risk event.

The researcher's view is that the inclusion of opportunity cost in internal loss data is an acceptable practice that should be encouraged.

c) Date of recording operational risk losses

Most banks (91%) record at least the discovery date of internal operational risk losses. Banks that solely capture the accounting dates and the dates of the occurrence of the losses were in the minority (9%). All four large banks indicated that they record at least the discovery dates.

The researcher concluded by indicating that banks should at least capture the date of the discovery of an operational risk event as this represents acceptable practice among the majority of banks.

d) Method of assigning losses that occurred in multiple business units

A major portion of the banks (91%) indicated that they do assign losses that may impact on multiple business activities, on a pro rata basis, to the multiple business activities.

e) Recording of recoveries (insurance and other recoveries)

Eighty-two percent of banks reported that insurance recoveries after operational risk events are recorded in the internal loss database as separate entries but associated with the original loss event. Fifty-five percent of banks

indicated that recoveries are recorded separately but associated with the original loss. If recoveries only occur after a certain date they also record the recoveries separately, but associated with the original loss.

This practice is considered to be the more conservative approach, as it does not offset the gross loss amount and the insurance recoveries.

f) Recording damage to fixed assets

Replacement cost is seen as the most appropriate way to capture gross loss amounts for damage to fixed assets. Sixty-four percent of respondents indicated that they use replacement cost to capture gross loss amounts for operational risk purposes. The four larger banks indicated that they use replacement cost for the gross loss amounts. Interesting to note is that the branches of foreign banks that replied indicated that use book values (accounting values) as gross loss amounts.

The researcher's view is that in the case of fixed assets accounting values are mostly based on historical cost, which may materially understate gross loss amounts. The understatement of such a gross loss amount ultimately will lead to the understatement of regulatory capital for operational risk. It is thus evident that the replacement cost of damage to fixed assets represents acceptable practice and is the more conservative approach determining gross loss amounts.

g) Recording of overtime cost

The majority of banks (55%) indicated that they do not record overtime cost for fixing systems in their internal loss databases. This finding is inconsistent with results from a similar study conducted by the AIGOR where many of the banks indicated that they do record overtime cost for fixing systems as part of their gross loss amounts (Basel Committee on Banking Supervision, 2006b: 2). Three of the four larger banks indicated that they do record

overtime cost for fixing systems in the internal loss database. Other smaller banks, one large bank and one branch of a major foreign bank indicated that they do not record overtime cost for fixing systems.

Although the majority of respondents indicated that they do not record overtime cost for fixing systems, the researcher is of the view that this cost should be recorded as it represents the cost of bring a system to its original working capacity. The researcher's view is that the same principles should be applied as those used for the section above on using replacement cost for recording damage to fixed assets.

This is one area banks could be encouraged to consider changing their practices.

h) Market risk losses due to rogue trading

Seventy-three percent of banks indicated that market risk losses caused by traders that violate their loss and risk limits are included as part of operational risk loss events. All four larger banks indicated that they treat these losses as operational risk losses.

The 23 percent of banks that indicated that they do not record market risk losses due to rogue trading in their internal loss databases are in breach of Basel II rules. The Basel II rules explicitly indicate that market risk losses due to operational risk events should be treated as market risk losses (Basel Committee on Banking Supervision, 2006a).

i) Loan-related losses caused by operational risk events

Eighty-two percent of banks indicated that although not used in the calculation of operational risk capital, they do record loan-related losses that are caused by inadequate or failed processes, technology or human performance as operational risk losses in their internal loss databases.

Although very difficult to determine the true nature of loan-related losses (whether credit related or operational risk related), banks that identify the causes of these losses to be operational risk related, should record these losses in their operational risk internal loss databases.

j) Loss data collection thresholds

Sixty-four percent of respondents use one standard threshold for all business units to capture internal operational risk losses. Three of the four larger banks indicated that they use different thresholds for different business units.

Although the majority of banks indicated that they use standard thresholds for different business units, the researcher indicated that this practice is not always acceptable to the management of different business units as the materiality in, for example, the home loans divisions would significantly differ from that in corporate finance.

The researcher's view is that the most prudent practice should be to set different thresholds that are applicable to the nature and business of the different business units.

k) Mapping matrixes

"Although there is no specific requirement to do so", seventy-three percent of respondents use mapping matrixes that correspond to the 8x7 matrix contained in the Basel II text (Basel Committee on Banking Supervision,

2006b: 19). Also of note is that 91% of the banks that responded indicated that they do map operational risk gross income to the Basel II business lines.

The researcher concluded that since operational risk management practices are still in an infancy stage, most banks adopted the 8x7 matrix as it provided them with a basis to work from until they can develop much more sophisticated methods.

l) Mapping data (legal entity or consolidated basis)

The majority of banks (55% + 18% = 73%) with subsidiaries do map operational risk data on a consolidated and legal entity basis. It is clear from the responses that the banks that indicated that they only map loss data on a legal entity basis are either branches of foreign banks (no subsidiaries) or smaller local banks.

It is, however, only prudent to also assess operational risk losses on a legal entity basis as to determine the exact origin of losses.

The researcher wants to conclude this section of the research report by indicating that the objectives of this part of the research study have successfully been met as follows:

- The study served as a “benchmarking exercise” among all South African banks on how internal loss data are being captured for operational risk purposes (Basel Committee on Banking Supervision, 2006b: 1).
- It also may provide the BSD and other financial services regulators with “a means of framing the discussion of acceptable practice in both the management and measurement of operational risk” (Basel Committee on Banking Supervision, 2006b: 2).

7. LIST OF REFERENCES

Anders, U. and Van den Brink, G. 2004. 'Implementing a Basel II Scenario-Based AMA for Operational Risk'. In: Ong, M K. Ed. *The Basel Handbook: A Guide for Financial Practitioners*. London: Inclusive Media Investments Limited. 343 – 368.

Basel Committee on Banking Supervision. 2003a. *Sound Practices for the Management and Supervision of Operational Risk*. Switzerland: Bank for International Settlements

Basel Committee on Banking Supervision. 2003b. *The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected*. Switzerland: Bank for International Settlements

Basel Committee on Banking Supervision. 2006a. *International Convergence of Capital Instruments and Capital Measurement Standards: A Revised Framework, (Basel II)*. Switzerland: Bank for International Settlements.

Basel Committee on Banking Supervision. 2006b. *Observed range of practice in key elements of the Advanced Measurement Approaches (AMA)*. Switzerland: Bank for International Settlements.

Basel Committee on Banking Supervision. 2007. *History of the Basel Committee and its membership*. Switzerland: Bank for International Settlements.
Available from: <<http://www.bis.org/html>
[Accessed 20 February 2007].

Bethell-Jones, R. 2001. 'Basle Committee tries to come to terms with operational risk'. *International Financial Law Review*. London: March 2001. Volume number 20, Issue. 3; 10 pgs (ProQuest).

-
- Bielski, L. 2003. 'Basel II: A Guide to operational risk'. *ABA Banking Journal*, November 2003. New York. Volume number 95, Issue 11, p48-51; 4p (Proquest).
- Bruce, L. 2006. 'Operational Risk: Are You Prepared?'. *AFP Exchange*. Bethesda: Volume number 26, Issue. 6; 6 pgs (ProQuest)
- Crouhy, M. Galai, D. and Mark, R. 2001. *Risk Management*. New York: McGraw-Hill.
- Cruz, M G. 2002. *Modeling, Measuring and Hedging Operational Risk*. West Sussex: John Wiley & Sons Limited.
- De Fontnouvelle, P. Dejesus-Rueff, V. Jordan, J S. and Rosengren, E S. 2006. 'Capital and Risk: New Evidence on Implications of Large Operational Losses'. *Journal of Money, Credit & Banking*. Volume number 38, Issue 7, p1819-1846; 28p (EBSCO Host Research databases).
- Dunnet, R. Levy, C. and Simoes, A P. 2005. 'Managing Operational Risk in Banking'. *McKinsey Quarterly*. Issue 1, p21-24; 4p (EBSCO Host Research databases).
- Evans, A. 2004. 'Operational Risk Management'. *Risk Management*, October 2004. New York. Volume number 51, Issue. 10, p50 (ProQuest).
- Flores, F. Bonson-Ponte, E. and Escobar-Rodriguez, T. 2006. 'Operational risk information system: a challenge for the banking sector'. *Journal of Financial Regulation and Compliance*. London. Volume number 14, Issue. 4; (ProQuest).

Foot, M. 2002. 'Operational risk management for financial institutions'. *Journal of Financial Regulation and Compliance*. London, Volume number 10, Issue. 4; 4 pgs; (ProQuest).

Financial Stability Institute. 2007a. 'Operational Risk On-line Training Module'. Available from: <<http://www.fsiconnect.org> [Accessed 7 February 2007].

Financial Stability Institute. 2007b. FSI online training Modules. 'Operational Risk Management'. Available from: <<http://www.fsi.org> [Accessed 3 March 2007].

Financial Stability Institute. 2007c. FSI online training Modules. 'Basel II - Operational Risk Management - AMA'. Available from: <<http://www.fsi.org> [Accessed 20 August 2007].

Frachot, A. Georges, P. and Roncalli, T. 2001. 'Loss Distribution Approach for Operational risk'.

Futjii, K. 2005. 'Building Scenarios'. In: Davis, E. ed. *Operational Risk: Practical Approaches to Implementation*. London: Inclusive Media Investments Limited. 169 – 178.

Garver, R. 2006a. 'Calculating Operational Risk's Multiplier'. *American Banker*. Volume number 171, Issue 110, p1-3. (EBSCO Host Research databases).

-
- Garver, R. 2006b. 'Operational Risk: Who's Making Progress'. *American Banker*, Volume number 171, Issue 86, p9-16, (EBSCO Host Research databases).
- Haas, M. and Kaiser, T. 2005. 'Prerequisites for Effective Operational Risk Management and Efficient Risk-based Decision Making'. In: Davis, E. ed. *Operational Risk: Practical Approaches to Implementation*. London: Inclusive Media Investments Limited. 215 – 225.
- Hanssen, J. 2005. 'Corporate Culture and Operational Risk'. *Bank Accounting and Finance*. Volume number 18, Issue 2, p35-38. (EBSCO Host Research databases).
- Haubenstock, M. 2005. 'Constructing an Operational Event Database'. In: Ong, M, K. ed. *The Basel Handbook: A Guide for Financial Practitioners*. London: Inclusive Media Investments Limited. 429 – 466.
- Holmquist, E. 2007. 'Changing culture', *OpRisk & Compliance*. April 2007. 41-43.
- Hughes, P. 2005. 'Using Transaction data to Measure Operational Risk'. In: Davis, E. ed. *Operational Risk: Practical Approaches to Implementation*. London: Inclusive Media Investments Limited. 3 – 12.
- Kraujalis, S. Karpaviciene, E. and Cvilikas, A. 2006: 'The Specifics of Operational Risk Assessment Methodology Recommended by Basel II'. *Engineering Economics*, Volume number 48, Issue 3, p7-17. (EBSCO Host Research databases).
- Kruger, E M. 2007. 'Strategic feedback session.' [PowerPoint Presentation] 7 April 2007. South African Reserve Bank, Pretoria.

-
- Lam, J. 2001: 'Top ten requirements for operational risk management'. *Risk Management. New York*: August 2004. Volume number 48, Issue 11, p58. (Proquest).
- Leedy, P. and Ormrod J, E. 2005. *Practical Research: Planning and Design*. 8th Edition. New Jersey: Pearson Education, Inc.
- Levy, C. Samandari, H and Simoes, A P. 2005. 'Better operational-risk management for banks'. *McKinsey Quarterly*. Available from: <<http://www.mckinsey.com> [Accessed 29 April 2007].
- Macklin, B. De Tora, D. Rath, E and Rothman, P. 2003: 'A Partnership Approach to Operational Risk Management'. *Banking and Accounting Finance*, Volume number 16, Issue 6, p9-14. (EBSCO Host Research databases).
- Marshall, C. L. 2001. *Measuring and Managing Operational Risks in Financial Institutions: Tools, Techniques, and other Resources*. Singapore: John Wiley & Sons (Asia) Pte Ltd.
- Mueller, H. and Siberon J. 2004. 'Economic capital in the limelight'. *Journal of Financial Regulation and Compliance*. London: November 2004. Volume number 12, Issue. 4; 8 pgs (ProQuest).
- Nedbank Group Limited. 2006. *Nedbank Group 2006 Annual Report*. Johannesburg: Nedbank Group Limited.
- Power, M. 2005. 'The invention of operational risk'. *Review of International Political Economy*. Volume number 12, Issue 4, p577-599, (EBSCO Host Research databases).

Sabatini, J. 2007. 'The rules of engagement', *Operational Risk and Compliance Magazine*. April 2007. 16-19.

Samad-Khan, A. 2005. *Why COSO is flawed*.
Available from: <<http://www.opriskadvisory.com>
[Accessed 28 February 2007].

Samad-Khan, A. Rheinbay, A. and Le Blevec, S. 2006. 'Fundamental issues in OpRisk Management', First published in *Operational Risk and Compliance Magazine*. Incisive Financial Publishing.

Samad-Khan, A. Moncelet, B. and Pinch, T. 2007: '*Uses and Misuses of data*'.
Available from: <<http://www.opriskadvisory.com>
[Accessed 28 February 2007].

Scandizzo, S. 2005: 'Risk Mapping and Key Risk Indicators in Operational Risk Management'. *Economic Notes*, Volume number 34, Issue 2, p231-256. (EBSCO Host Research databases).

South African Reserve Bank. 2006. *Bank Supervision Department Annual Report 2006*. Pretoria: South African Reserve Bank.

South African Reserve Bank. 2007a. *BankIndaba*. January/February 2007 issue.

South African Reserve Bank. 2007b. 'Mission of the Bank Supervision Department'
Available from: <<http://www.reservebank.co.za>
[Accessed 10 March 2007].

South African Reserve Bank. 2007c. Total Banks Data

Available from: <<http://www.reservebank.co.za>
[Accessed 23 May 2007].

Wikipedia. 2007. *Definition of cheque kiting*

Available from: <http://en.wikipedia.org/wiki/Bank_fraud
[Accessed 10 March 2007].

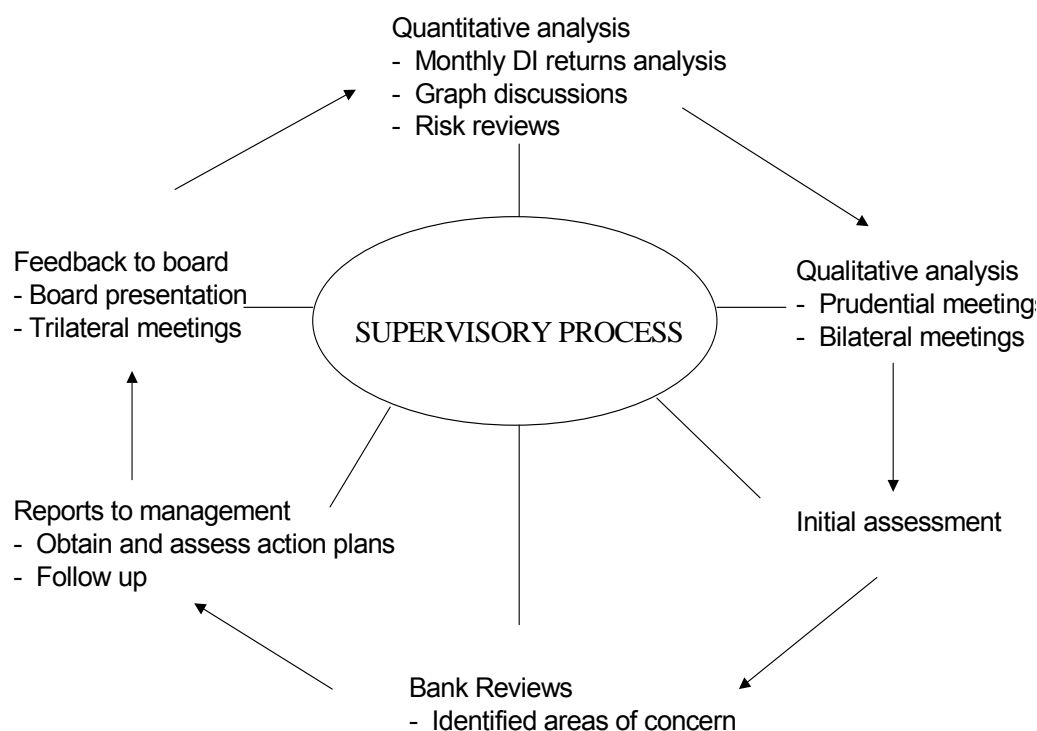
Van den Brink G, J. 2002. *Operational Risk: The new Challenge for Banks*. New York: Palgrave.

Van Greuning H. and Bratanovic, S. 2003. *Analyzing and Managing Banking Risk*. 2nd Edition. Washington: The International Bank for Reconstruction and Development/ The World Bank.

Young, J. 2006. *Operational Risk Management: The Practical application of a qualitative approach*. Pretoria: Van Schaik Publishers.

8. APPENDICES

8.1 APPENDIX A – SUPERVISORY REVIEW PROCESS OF THE BANK SUPERVISION DEPARTMENT



Source: Kruger, 2007

8.2 APPENDIX B – QUESTIONNAIRE



Research for Master's Degree in Business Leadership

I am currently busy with the research component of the Master's Degree in Business Leadership (MBL) at the University of South Africa's School of Business Leadership (SBL).

The purpose of my study is to determine in *which areas* in South African banks the most *severe* operational risk losses are *likely* to occur (based on the Basel II seven loss event types and eight business lines). The study also assesses the range of practices in collecting internal loss data for operational risk purposes as required by Basel II.

The questionnaire takes about 10 minutes to complete. I will appreciate your favourable consideration in completing the enclosed questionnaire and assisting me in my research efforts.

The completed questionnaire should be returned to myself via electronic mail at the following address: denzel.bostander@resbank.co.za by 14 August 2007.

Thank you in advance
Denzel Bostander

QUESTIONNAIRE

[Please tick appropriate boxes]

The answers to the questions 1 to 8 should be based on your experience in risk management/operational risk management of banks.

1. Indicate number of years experience in the banking sector

1	1-5	
2	6-10	
3	11-15	
4	>15	

2. Indicate number of years experience in operational risk management

1	1-3	
2	4-6	
3	7-9	
4	>9	

3. Indicate where you are currently employed

1	One of the four larger banks	
2	Other local bank	
3	Subsidiary of a foreign bank	
4	Branch of a foreign bank	

4. Indicate the importance of the following risk areas for your bank

(1 – not important at all, 2 – only slightly important, 3 – rather important, 4 – very important)

Please tick the appropriate box next to each item

	Risk faced by banks	1	2	3	4
4.1	Credit risk				
4.2	Market risk				
4.3	Liquidity risk				
4.4	Interest-rate risk				
4.5	Operational risk				
4.6	Currency risk				

5. Indicate the operational risk loss event type where the most severe single operational risk loss is likely to occur in respect of your bank

(1 – very low severity, 2 – only slightly severe, 3 - severe, 4 – extremely severe)

Please tick the appropriate box next to each item

	Loss event types	1	2	3	4
5.1	Internal fraud				
5.2	External fraud				
5.3	Employment practices and workplace safety				
5.4	Clients, products and business practices				
5.5	Damage to physical assets				
5.6	Business disruption and system failures				
5.7	Execution, delivery and process management				

Important note:

Questions 5 to 8 are based on the seven loss event types and eight business lines as specified in the *International Convergence of Capital Instruments and Capital Measurement Standards – A Revised Framework* issued in June 2006 (better known as Basel II)

6. Indicate the **business line** where the most **severe** single operational risk loss is likely to occur in respect of your bank.

(1 – very low severity, 2 – only slightly severe, 3 - Severe, 4 – extremely severe)

Please tick the appropriate box next to each item

	Business line	1	2	3	4
6.1	Corporate finance				
6.2	Trading and sales				
6.3	Retail banking				
6.4	Commercial banking				
6.5	Payment and settlement				
6.6	Agency services				
6.7	Asset management				
6.8	Retail brokerage				

7. Indicate the **loss event type** where operational risk losses occur most **frequently** in your bank.

(1 – very low frequency, 2 – only slightly frequent, 3 – rather frequent, 4 – extremely frequent)

Please tick the appropriate box next to each item

	Loss event type	1	2	3	4
7.1	Internal fraud				
7.2	External fraud				
7.3	Employment practices and workplace safety				
7.4	Clients, products and business practices				
7.5	Damage to physical assets				
7.6	Business disruption and system failures				
7.7	Execution, delivery and process management				

8. Indicate the **business line** where operational risk losses occur most frequently in respect of your bank.

(1 – very low frequency, 2 – only slightly frequent, 3 – rather frequent, 4 – extremely frequent)

Please tick the appropriate box next to each item

	Business line	1	2	3	4
8.1	Corporate finance				
8.2	Trading and sales				
8.3	Retail banking				
8.4	Commercial banking				
8.5	Payment and settlement				
8.6	Agency services				
8.7	Asset management				
8.8	Retail brokerage				

The answers to questions 9 to 23 should be specifically related to your bank. Questions 9 to 23 are only to be completed if your bank captures internal loss data.

9. Do you record **near misses** in your loss event database?

1	Yes	
2	No	

10. Do you record **opportunity cost** of operational risk events in your loss event database?

1	Yes	
2	No	

11. Do you record **overtime cost** for fixing system failures in your loss event database?

1	Yes	
2	No	

12. **When** do you record the internal operational risk loss in the internal loss database?

1	Date of occurrence	
2	Discovery date	
3	Accounting date	
4	Date of detection	

13. How does your bank **assign** the loss that may impact on multiple business activities:

1	Assigns the loss to the business for which the impact is the greatest	
2	Assigns pro-rated losses across the businesses in which it occurs	

14. **How** does your bank capture the loss that is covered by insurance and actually offset by insurance recovery afterward?

1	As a single loss amount on a netting-out basis	
2	As a separate loss amount, associated with its original loss	
3	As a separate loss amount <u>without</u> association with its original loss	

15. How does your bank capture the losses that are offset by recoveries afterward?

1	As a single loss amount on a netting-out basis if recoveries occur within a few days after the occurrence of loss events	
2	As a single loss amount on a netting-out basis if recoveries occur within a day after the occurrence of loss events	
3	As separate loss amounts	

16. How does your bank evaluate the damage to fixed assets?

1	Replacement cost	
2	Market value	
3	Book value (accounting value)	

17. How does your bank treat market losses that are caused by traders who violate loss or risk limits inadvertently?

1	Include them as operational risk losses	
2	Include them as market risk losses	

18. How does your bank treat loan-related losses that are caused by inadequate or failed processes, technology or human performance?

1	Include them as operational risk losses	
2	Include them as credit risk losses	

19. How does your bank treat losses caused by inadequate business decisions by senior management that could be considered as strategic losses?

1	Include them as operational risk losses	
2	Do not include them as operational risk losses	

20. In collecting loss data, your bank sets a threshold or thresholds that are based mainly on:

1	One standard threshold for all the business units	
2	Different loss thresholds for different business units	

21. Does your bank map the data to matrixes that:

1	Are the same as the 8x7 matrix set out in Basel II	
2	Are <i>not</i> the same as the 8x7 matrix set out in Basel II	
3	Are based on client rather than on product	
4	Are based on causes rather than events	

22. Does your bank map the data on:

1	A consolidated basis rather than on each legal entity basis	
2	On a legal entity basis	

23. Mapping of gross income

1	Banks map gross income data to the business lines that are the same as the Basel definition	
2	Banks map gross income data to the business lines that are not necessarily the same as those in the Basel definition	

Important note:

Questions 9 to 23 of this questionnaire were based on a questionnaire internally circulated amongst the members of the Accord Implementation Group Operational Risk (AIGOR).

8.3 ARTICLE FOR PUBLICATION

See next page