

**Current practices and guidelines for classifying
credit risk boundary events:
A South African approach**

JOLENE STEENKAMP

12783161

Dissertation submitted in partial fulfilment of the requirements for the degree *Master of Commerce* at
the Potchefstroom Campus of the North-West University

Supervisor: Dr. A. Heymans

Co-Supervisor: Prof. P. Styger

November 2011

ACKNOWLEDGEMENTS

My Heavenly Father has shown me an abundance of grace and unmerited favour. He has granted me the ability to write this study, and He has blessed me with family, friends and colleagues who have provided me with their unlimited support.

Herewith my sincerest appreciation to the following persons for their support and assistance in various ways throughout this study:

- Prof Paul Styger, for his initial valued advice, guidance and assistance in starting off this research.
- My supervisor, Dr Andre Heymans, for his technical inputs, assistance and guidance. I value your patience and assistance throughout this time immensely.
- My colleagues, Hans Bouckaert, Gareth Viljoen and Flippie Snyman, for their highly respected technical guidance, and for their valuable constructive criticism and fresh ideas.
- Marisa Swart, for the language editing of this dissertation.
- Ultimately, to my family and especially my fiancée, Corné, for their support and love.

Jolene Steenkamp

Johannesburg, November 2011

ABSTRACT

The financial crisis turmoil has exposed notable weakness in the risk management processes of the financial services industry. It has also led to a critical look at the scope of the various risk types as well as the classification of loss events. More importantly, the effects that incorrect risk classification might have on capital requirements are now also examined and taken into account.

Boundary events between credit risk and operational risk continue to be a significant source of concern for regulators and the industry in general. The Basel Committee on Banking Supervision (BCBS) requires that boundary events should be treated as credit risk for the purposes of calculating minimum regulatory capital under the Basel II Framework. Such losses will, therefore, not be subject to any operational risk capital charges. However, for the purposes of internal operational risk management, banks are required to identify all material operational risk losses. Boundary events should be flagged separately within a bank's internal operational risk database. The Basel II Framework does not provide any further guidelines as to what constitutes boundary events and, therefore, consistent guiding principles that banks can follow for accurately classifying and subsequently flagging such events do not exist. The potential exists that actual boundary events might be classified as purely credit risk, and correctly be included in the credit risk capital charge, but not be flagged separately within the bank's internal operational risk database. Alternatively, boundary events might be classified as operational risk and, therefore, be subject to the operational risk capital charge, instead of the credit risk capital charge. The former instance might give rise to an operational risk manager not being completely informed of the operational risks that the business is facing. The emphasis should always be on the management of risks and for this reason it is important that a financial institution indicates and flags all boundary events in their operational risk systems. To remedy this lack of guidance on the boundary event issue, guidelines are provided that banks can utilise within their risk classification processes. The approach utilised is to consider mechanisms and tools for classification, guidance from the Operational Risk Data Exchange (ORX) and the BCBS, as well as the International Accounting Standards Board (IASB).

By compiling and submitting questionnaires to five South African banks, an investigation is conducted in order to obtain a view of the current mechanisms, tools and approaches that South African Advanced Measurement Approach (AMA) banks currently utilise within their classification processes. The effectiveness of boundary event classification is assessed by analysing the percentage of losses classified as boundary. In addition, the degree of uniformity or disparity in the classification of typical boundary event scenarios is considered. This analysis is performed by providing respondents with a total of 16 typical boundary event risk descriptions, and requesting the respondents to classify each of the losses in the scenarios as credit risk, operational risk or boundary event type.

Keywords: boundary events, operational risk, credit risk, risk classification

OPSOMMING

Die onlangse kredietkrisis gedurende 2007 en 2008 het merkbare swakhede in die huidige risikobestuursprosesse van die finansiële diensbedryf uitgelig. Dit het ook daartoe gelei dat kenners heroorweging moes skenk aan die verskillende risikotipes, sowel as aan die klassifisering van die verskillende verliese- en risikotipes. Daar word nou ook gekyk na die moontlike uitwerking wat onakkurate klassifikasie van risiko's en verliese op die kapitaalvereistes wat aan banke gestel word, mag hê.

Grensgevalle tussen kredietrisiko en operasionele risiko is steeds 'n groot bron van kommer, nie net vir reguleerders nie, maar ook vir die finansiële bedryf oor die algemeen. Die Basel Komitee oor Bank Toesighouding vereis dat die grensgevalle tussen kredietrisiko en operasionele risiko geklassifiseer moet word as kredietrisiko vir die doeleindes van minimum regulatoriese kapitaalberekeninge onder die Basel II-raamwerk. Hierdie verliese sal dus nie onderhewig wees aan die berekening van kapitaal onder operasionele risiko nie. Vir die doeleindes van interne risikobestuur, word daar egter steeds van finansiële instansies verwag om hierdie operasionele risikoverwante gevalle te identifiseer en binne hul interne operasionele risikodatabasisse aan te teken. Die Basel II-raamwerk verskaf geen verdere riglyne vir die klassifikasie van grensgevalle nie. Verder bestaan daar ook nie genoegsame riglyne wat banke kan navolg om hierdie tipes risiko's en verliese akkuraat te klassifiseer nie. Dus bestaan die potensiaal dat die werklike grensgevalle tussen kredietrisiko en operasionele risiko geklassifiseer kan word as 'n suiwer kredietrisiko geval, en korrek ingesluit word in die kredietrisiko-kapitaalberekeninge, maar nie afsonderlik geïdentifiseer word binne die bank se interne operasionele risikodatabasis nie. Die alternatief is ook dat grensgevalle geklassifiseer kan word as operasioneel van aard, en daarom onderhewig gestel word aan die operasionele risikokapitaalberekening, in plaas van aan die kredietrisiko-kapitaalberekening. Eersgenoemde geval kan aanleiding daartoe gee dat 'n operasionele risikobestuurder nie oor genoegsame inligting beskik om op hoogte te bly van die operasionele risiko's waaraan die bank in werklikheid blootgestel word nie. Die klem moet altyd wees op die bestuur van risiko's, en juis om hierdie rede is dit van uiterste belang dat 'n finansiële instansie die grensgevalle tussen kredietrisiko en operasionele risiko akkuraat klassifiseer, en ook hierdie gevalle binne hul operasionele risiko-areas identifiseer.

Om hierdie gebrek aan riglyne rondom die grensgevalprobleem reg te stel, word riglyne voorgestel wat banke tydens hul klassifikasieprosesse kan gebruik. Die benadering wat gevolg word, is om oorweging te skenk aan die verskillende meganismes wat finansiële instansies vir klassifikasie kan gebruik, die riglyne wat voorgestel word deur die "Operational Risk Data Exchange", die Basel-komitee van Banktoesighouding, asook die Internasionale Rekeningkundige Standaarde.

'n Ondersoek en analise is gedoen deur die gebruik van vraelyste wat aan vyf banke in Suid-Afrika uitgestuur is. Hierdeur word ondersoek ingestel na watter meganismes tans deur banke gebruik word as hulp in die klassifikasieprosesse. Daar word ook slegs gefokus op banke wat die “Advanced Measurement Approach” gebruik vir operational risiko kapitaalberekeninge. Die mate van effektiwiteit waartoe banke vandag grensgevalle tussen kredietrisiko en operasionele risiko klassifiseer, word ook ondersoek en geanaliseer. Dit word gedoen deur die ontleding van die persentasie van verliese wat geklassifiseer word as 'n grensgeval. Daarbenewens word ook gekyk na die mate van eenvormigheid of die mate van verskil wat binne die huidige klassifisering van tipiese risikogevalle bestaan. Hierdie analise word uitgevoer deurdat die respondent voorsien word van sestig tipiese grensgeval-risikobeskrywings. Die respondent word dan versoek om elk van die verliese in die beskrywings as krediet-, operasioneel- of grensgevaltipe te klassifiseer.

Sleutelwoorde: grensgevalle; operasionele risiko; kredietrisiko, risiko-klassifikasie

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	i
ABSTRACT.....	ii
OPSOMMING	iii
LIST OF FIGURES	viii
LIST OF TABLES	xii
Chapter 1: Introduction and Problem Statement.....	1
1.1. Background	1
1.2. Problem statement.....	3
1.3. Objectives	4
1.4. Research methodology.....	4
1.5. Dissertation outline	4
Chapter 2: The Basel II Approach to Credit Risk.....	6
2.1. Introduction.....	6
2.2. A definition of capital	6
2.2.1. Unique definition of capital to banks.....	6
2.2.2. The reason why banks hold capital	8
2.2.3. Economic capital versus regulatory capital.....	9
2.2.4. The development of capital standards for banks.....	10
2.3. The Basel Committee.....	12
2.3.1. The goals and strategies of the BCBS.....	13
2.3.2. The concept of regulatory capital.....	13
2.4. The capital adequacy principle	14
2.5. The New Basel Capital Accord.....	14
2.6. The definition of credit risk	20
2.7. The expected and unexpected losses of credit risk	21
2.8. Basel II credit risk measurement approaches.....	22
2.9. Conclusion	29
Chapter 3: The Basel II Approach to Operational Risk	31
3.1. Introduction.....	31
3.2. Operational risk – An evolution of definitions	32
3.3. Operational risk capital – Expected and unexpected losses.....	34
3.4. Basel II Operational Risk Measurement Approaches	35
3.4.1. BIA.....	35
3.4.2. Standardised Approach	36

3.4.3.	Advanced Measurement Approaches.....	38
3.5.	AMA Capital Calculation under Basel II.....	42
3.5.1.	Phase I: Building a basis for AMA	42
3.6.1.	Phase II: Capital modelling.....	47
3.7.	Conclusion	54
Chapter 4:	Credit Risk and Operational Risk – Boundary Events.....	56
4.1.	Introduction.....	56
4.2.	Boundary events – The current relevance of the issue.....	57
4.3.	Boundary events.....	58
4.3.1.	Operational risk and credit risk as separate risk types	58
4.3.2.	Credit risk and operational risk – The boundary issue.....	60
4.3.3.	The view of the BCBS	61
4.4.	Distinguishing between credit risk events, operational risk events and boundary events	63
4.4.1.	ORX view on boundary events	63
4.4.2.	Classification Framework and Taxonomy	65
4.4.3.	Causes	73
4.4.4.	Controls and mitigation techniques.....	81
4.4.5.	Education	82
4.4.6.	The “Bow-Tie” model of operational risk	82
4.4.7.	A decision tree for boundary-event classification.....	84
4.5.	A generic incident management lifecycle.....	88
4.6.	Conclusion	88
Chapter 5:	Methodology and Analysis of Results	91
5.1.	Introduction.....	91
5.2.	Identification of the banks to participate in the study	91
5.3.	Identification of the information that is required from the banks	92
5.4.	Design of the questionnaires	93
5.5.	Programming of the questionnaires in VBA.....	94
5.6.	Holding meetings with the stakeholders of the participating banks.....	96
5.7.	Distribution of questionnaires.....	96
5.8.	Receipt of questionnaires and writing up of results	96
5.9.	Results – The General Questionnaire.....	96
5.9.1.	The use of tools to aid the classification process of loss events	97
5.9.2.	Accuracy of classification and capital treatment of boundary event losses	99
5.9.3.	Contributing factors to accuracy of boundary event loss classifications	101
5.9.4.	Operational risk data	105

5.10.	Results – the Boundary Event Scenarios Questionnaire	111
5.10.1.	Demographics	111
5.10.2.	Boundary event scenarios	115
5.11.	Summary of results	144
5.12.	Conclusion	146
Chapter 6:	Conclusion and Recommendations	148
6.1.	Introduction.....	148
6.2.	Aim of research project.....	148
6.3.	Study review – Credit risk	148
6.4.	Study review – Operational risk.....	149
6.5.	Study review – Boundary events	149
6.6.	Study review – The approaches that banks currently utilise for classification	150
6.7.	Study review – The effectiveness of boundary event classification	151
6.8.	Study review – Uniformity/disparity in the classification of boundary events	151
6.9.	Conclusion	152
6.10.	Recommendations for financial institutions.....	153
6.11.	Regulatory recommendations	155
6.12.	Recommendations for further research	156
Bibliography		157
Appendix 1		163
Appendix 2		164
Appendix 3		168
Appendix 4		174
Appendix 5		183

LIST OF FIGURES

Chapter 2

The Basel II Approach to Credit Risk

Figure #	Name	Page
Figure 2.1	The framework of the Basel II Capital Accord	16
Figure 2.2	Pillar I of Basel II	17
Figure 2.3	The four principles of the supervisory review process	19
Figure 2.4	Market discipline according to Basel's Pillar III	20

Chapter 3

The Basel II Approach to Operational Risk

Figure #	Name	Page
Figure 3.1	The basis for AMA	43
Figure 3.2	Operational risk assessment structure	45
Figure 3.3	Scorecard approach for risk assessments	47
Figure 3.4	Modelling for operational risk	48
Figure 3.5	Combination of frequency and severity distribution for the LDA	52
Figure 3.6	Total loss distribution calculation	53
Figure 3.7	An aggregated annual loss distribution	54

Chapter 4

Credit Risk and Operational Risk – Boundary Events

Figure #	Name	Page
Figure 4.1	Operational risk materialising directly or indirectly through credit risk/ market risk	59
Figure 4.2	Relationship between hazard, event and loss	74
Figure 4.3	Risk classification	76
Figure 4.4	The Bow Tie of operational risk, incorporating controls	83
Figure 4.5	A decision tree for boundary event classification	86

Chapter 5

Methodology and Analysis of Results

Figure #	Name	Page
Figure 5.1	Example of the loss description front-end in the Boundary Event Scenarios Questionnaire	95
Figure 5.2	The measurement approach currently followed by the participating banks	97
Figure 5.3	The utilisation of documented and approved guidelines for loss classification	98
Figure 5.4	Utilisation of decision tree for guidance in terms of loss classification	98
Figure 5.5	Utilisation of causal categories for guidance in terms of loss classification	99
Figure 5.6	Accuracy of boundary event classifications	100
Figure 5.7	Accuracy of boundary event capital treatment	101

Figure #	Name	Page
Figure 5.8	Belief that guidelines do/do not contribute to the success of classifications	1052
Figure 5.9	Belief that decision trees do/do not contribute to the success of classifications	102
Figure 5.10	Belief that taxonomy of events does/does not contribute to the success of classifications	103
Figure 5.11	Belief that knowledgeable, experienced and trained staff contribute to the success of classifications	104
Figure 5.12	Belief that causal categories contribute to success/failure of classifications	104
Figure 5.13	Distribution of frequency of loss by business line by event type – 2009Q1-4	106
Figure 5.14	Loss-reporting thresholds of banks – Retail Banking versus Commercial Banking	107
Figure 5.15	Boundary event losses as percentage of total losses	108
Figure 5.16	Boundary event loss frequencies as percentage of total loss frequencies	109
Figure 5.17	Qualifications of respondents	111
Figure 5.18	Operational risk knowledge of respondents	112
Figure 5.19	Credit risk knowledge of respondents	113
Figure 5.20	Banking employment and experience of respondents	113
Figure 5.21	Operational risk experience of respondents	114
Figure 5.22	Credit risk experience of respondents	114
Figure 5.23	Scenario one - classification responses	116

Figure #	Name	Page
Figure 5.24	Scenario two - classification responses	118
Figure 5.25	Scenario three - classification responses	120
Figure 5.26	Scenario five - classification responses	123
Figure 5.27	Scenario six - classification responses	125
Figure 5.28	Scenario seven - classification responses	127
Figure 5.29	Scenario eight - classification responses	128
Figure 5.30	Scenario nine - classification responses	131
Figure 5.31	Scenario ten - classification responses	133
Figure 5.32	Scenario 11 - classification responses	134
Figure 5.33	Scenario 12 - classification responses	136
Figure 5.34	Scenario 13 - classification responses	138
Figure 5.35	Scenario 15 - classification responses	140
Figure 5.36	Scenario 16 - classification responses	142
Figure 5.37	Overall view of boundary event scenario responses	143
Figure 5.38	Classification base applied for classification	144

LIST OF TABLES

Chapter 2

The Basel II Approach to Credit Risk

Figure #	Name	Page
Table 2.1	The rationale for a new accord – a comparison between the 1988 Basel I Accord and the Basel II Capital Accord	15

Chapter 3

The Basel II Approach to Operational Risk

Figure #	Name	Page
Table 3.1	Loss-event type classification	38

Chapter 4

Credit Risk and Operational Risk – Boundary Events

Figure #	Name	Page
Table 4.1	Structural differences between credit risk, market risk and operational risk	60
Table 4.2	Example of operational risks per business area	66
Table 4.3	The detailed loss-event classification of the BCBS	67
Table 4.4	Comparison of the ORX loss-event classification and the Basel II loss-event classification	71
Table 4.5	Expansion of classification framework to include credit risks	72
Table 4.6	Key people risks	77
Table 4.7	Key systems risks	78

Figure #	Name	Page
Table 4.8	Key external risks	80
Table 4.9	A risk and cause taxonomy	80
Table 4.10	Boundary event decision-tree steps	87

Chapter 5

Methodology and Analysis of Results

Figure #	Name	Page
Table 5.1	Decision-tree steps for scenario one	117
Table 5.2	Decision-tree steps for scenario two	119
Table 5.3	Decision-tree steps for scenario three	121
Table 5.4	Decision-tree steps for scenario four	122
Table 5.5	Decision-tree steps for scenario five	124
Table 5.6	Decision-tree steps for scenario six	126
Table 5.7	Decision-tree steps for scenario seven	128
Table 5.8	Decision-tree steps for scenario eight	130
Table 5.9	Decision-tree steps for scenario nine	132
Table 5.10	Decision-tree steps for scenario ten	134
Table 5.11	Decision-tree steps for scenario 11	135
Table 5.12	Decision-tree steps for scenario 12	137
Table 5.13	Decision-tree steps for scenario 13	139
Table 5.14	Decision-tree steps for scenario 14	140

Figure #	Name	Page
Table 5.15	Decision-tree steps for scenario 15	141
Table 5.16	Decision-tree steps for scenario 16	142

Chapter 1

Introduction and Problem Statement

1.1. Background

The global financial services sector experienced some difficult and distressing, especially during 2007 and 2008. From an operational risk perspective, which is the broadest and most far-reaching type of risk that a financial institution can face, 2008 was officially the worst on record (Cagan, 2009:2). Credit, market, and liquidity risk also drove the severity of these past operational risk loss events. An example hereof is the size of the US\$7 billion unauthorised trading event at Société Generale that was uncovered in January 2008. This operational risk event included fraud that was originally undertaken prior to the global credit crisis; the state of the markets, however, escalated the severity (Cagan, 2009:2).

The credit crisis has exposed some significant weaknesses in risk management processes across the financial services industry (KPMG, 2009:2). However, of more importance here is the fact that it also led to a critical look at the scope of the various risk types and the classification of loss events, and in turn the effects that incorrect risk classification might have on capital requirements (KPMG, 2009:2). The credit crisis generally brings into question many banks' overall risk governance. In most cases the inadequacy of overall risk governance is evident in the absence of a clear framework, policies or the necessary capabilities to achieve clear goals regarding the different types of risks faced across the organisation. Another shortcoming is the inability to accurately classify these risks (KPMG, 2009:10).

It is thus vital that all employees are completely informed of the various risk types. Senior management should set the overall strategic direction and embed risk management philosophy across the business. This will enhance the accurate classification, measurement and management of the various risk types. Clear guidance reflected in policies and procedures should be provided while clear expectations of compliance with these policies and procedures should be set (KPMG, 2009:10). In summary, there is a need not only for truly integrated risk management policies and procedures, but also for proper risk classification guidelines in particular. Proper risk classification will also enable more accurate minimum capital requirement calculations than that required for the various risk types.

The dilemma that most banks face today is the fact that operational risk is sometimes commonly mistaken for credit risk, and specifically operational risk events are regularly mistakenly identified as credit risk events. This study will, therefore, focus principally on credit risk loss events and operational risk loss events and specifically, operational risk losses that are related to credit risk.¹ Credit risk dominates retail bank activity, and is defined by the Bank for International Settlements

¹ Please note that operational risks relating to market risk are excluded from this study.

(BIS) as the potential that a counterparty will fail to meet its obligations in accordance with agreed terms (BIS, 2000:1). However, operational risk also plays a vital role. It is important to note that operational risk events might be the actual cause of credit risk events; that is, leading to a counterparty failing to meet its obligations. Operational risk for any financial institution – and within any business line – arises from the influence and interaction of internal and external factors and events on the people, processes and technology utilised in business processes within that institution (Gallati, 2003:290). Therefore, the influence and interaction of these internal and external factors within any line of credit operations within a bank, might give rise to loss events. The question therefore arises: are these loss events classified as credit risk loss events, or operational risk loss events?

After a number of banking crises, including the collapse of Barings bank in 1995, operational risk began to demand greater attention during the mid-1990s. In addition, since 1999, the BIS expressed the intention to introduce a new regulatory capital requirement for operational risk over and above market and credit risk (Saita, 2007:115). As institutions are generally distinctive in the way they combine people, processes and technology, it has always been complicated and for some impossible to create a single generic definition of what constitutes operational risk (Gallati, 2003:290). There is, however, a common core operational risk definition as proposed by the BIS: “operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” (BIS, 2006a:144). It should be recognised that this definition is not intended to include defaults that are otherwise covered in the scope of credit risks (Gallati, 2003:289). Operational risk is also frequently defined as any risk that is not categorised as market or credit risk, and is viewed as the risk of loss arising from a range of human or technical errors. Some institutions take the view that risks such as settlement, collateral and netting risks are not necessarily classifiable as operational risk, as they may contain elements of more than one type of risk (Gallati, 2003:289). The definition of operational risk distinguishes between direct and indirect impacts from operational risk causes. The impact might be observable and manifested in a credit risk event, resulting in a loss or a profit (Gallati, 2003:291). As far as the definition of an operational event is concerned, a bank could decide to adopt a stricter definition of operational risk; alternatively, appropriate definitions and guidelines should be instituted for other events or losses.

Major consequences will ultimately become evident in the credit or market risk buckets when operational risk is treated as a distinct risk type. This view is, however, misleading from a management perspective. These risks have structural differences in almost every respect – including a maximum loss amount, inspection level and portfolio – and different responses from management are thus required. Overlooking key events or misclassifying operational risks as credit risks can have considerable consequences for banks (KPMG, 2005:11). The BCBS requires that operational risk losses that are related to credit risk (hereafter referred to as *boundary events*) should be treated as credit risk for the purposes of calculating minimum regulatory capital under the Basel II Framework

(BIS, 2006a:153). Such losses will, therefore, not be subject to any operational risk capital charges. However, for the purposes of internal operational risk management, banks are required to identify all material operational risk losses. Such material operational risk-related credit risk losses should be flagged separately within a bank's internal operational risk database (BIS, 2006a:153). The Basel II Framework does not provide any further guidelines as to what constitutes boundary events and, therefore, consistent guiding principles do not exist that banks can follow for accurately classifying and subsequently flagging such events.

The potential exists that actual boundary events might be classified as purely credit risk, and correctly be included in the credit risk capital charge, but not be flagged separately within the bank's internal operational risk database. Alternatively, boundary events might be classified as operational risk and, therefore, be subject to the operational risk capital charge, instead of the credit risk capital charge. The former instance might give rise to an operational risk manager not being completely informed of the operational risks that the business is facing. The emphasis should always be on the management of risks (Sands, 2011b) and for this reason it is important that a financial institution indicates and flags all boundary events in its operational risk system.

The need is highlighted for banks to take a prudent approach to the identification and classification of operational risks within the credit risk environment. Attendant to this is an increasing need for proper guidelines in classifying credit risk and operational risk boundary events. The essence of this study is to investigate the approach that banks currently follow in terms of the classification of boundary events, and to propose guidelines to be followed for classification of boundary events. Due to the lack of sufficient literature on boundary event classifications, questionnaires are compiled and distributed to current experts and relevant parties within five participating banks in South Africa. The goal is to discover the various possible approaches that are followed in the identification and classification of boundary events.

1.2. Problem statement

Limited guidelines currently exist for banks to properly identify and classify boundary events, and it is not clear which tools and/or mechanisms are currently used by banks to assist in the classification process of boundary events. It is furthermore not clear whether there is any uniformity in how South African banks and their operational risk stakeholders classify boundary events.

1.3. Objectives

The first objective is to provide a clear definition of what constitutes credit risk losses, operational risk losses, and boundary events. Furthermore, suitable guidelines are to be set out for banks to classify boundary events and to establish:²

- an understanding of the approach, tools and mechanisms that banks currently utilise for classifying boundary events,
- an idea as to how effectively banks classify boundary events and flag operational risks that are existent in credit risk losses, and
- an overview of the uniformity or disparity that currently exists with regards to how operational risk experts approach the classification of typical boundary event losses.

1.4. Research methodology

This study comprises a literature study and empirical research. The literature study covers credit risk, operational risk and boundary events, and is followed by the empirical research – including the research and analysis techniques, data constitution, data analysis and interpretation.

For the first section of this study, the focus is on providing the background on credit risk and operational risk, and then on providing a clear understanding of boundary events. A method is also proposed for classifying boundary events. Subsequently, questionnaires are to be distributed to relevant parties and current experts within five South African banks. The aim is to discover various possible approaches currently followed in the South African industry. Relevant qualitative analyses will establish the basis for obtaining an understanding of the approaches that are followed by the various participating banks and operational risk experts. The analysis will also be performed in conjunction with the proposed guidelines for classification.

1.5. Dissertation outline

Chapter 2 provides a literature review regarding the concept of capital, and specifically regulatory capital. The history and background of the BCBS is provided. An appropriate definition of credit risk is provided. Thereafter, an overview of the Basel II regulatory requirements for credit risk is set out, whereby a review is conducted on Basel II credit risk and the minimum capital requirements of this risk type. The various Basel II approaches to credit risk are also discussed.

In Chapter 3, the reader is provided with a literature review on the evolution of operational risk definitions, after which the Basel II operational risk minimum capital requirements are set out. There are various Basel II approaches to operational risk, and the basic requirements for these approaches

² In this study, boundary events specifically refer to events relating to credit risk.

are discussed. Subsequently, a two-phase approach to the implementation of the capital requirement calculations under the AMA³ is set out.

Boundary events are discussed in Chapter 4. Various approaches and considerations are provided in order to form a proper definition of boundary events. A distinction between credit risk and operational risk is established and explained. The various mechanisms that can be utilised for loss event classification are discussed. These include, amongst other things, classification frameworks or taxonomies, causal categories and the education of staff. Subsequently a decision tree is proposed that can be utilised for the classification process of boundary events.

Chapter 5 discusses the methodology of research and the steps and approaches followed in the compilation of the questionnaires. The data gathering and analysis of results obtained from the questionnaires are discussed in detail. The chapter discusses the results obtained in the general questionnaire that is to be completed by each participating bank. From these results, it is possible to ascertain which approaches, tools and mechanisms are currently utilised by South African banks to classify boundary events. Also, an indication is obtained as to how effectively banks classify boundary events and flag operational risks that are existent in credit risk losses. The results from the boundary event scenarios questionnaire are also discussed. From these results, an overview of the uniformity or disparity that currently exists with regards to how operational risk experts approach the classification of typical boundary event losses is obtained.

Chapter 6 concludes this study by referring to the aims of this study. This is followed by a summary of this study while conclusions are further drawn from the results obtained in this study.

Recommendations that financial institutions can follow to assist in their risk management loss classification processes are provided. Finally, recommendations are provided for further research.

³ This is an approach used under operational risk.

Chapter 2

The Basel II Approach to Credit Risk

2.1. Introduction

Many different ratios and rules exist for the governance of banks, but capital adequacy is the single most important financial ratio for supervisors to examine the soundness of a particular bank (Matten, 2000:82). Capital should be available to absorb future, unidentified losses (Matten, 2000:16). Considering the eminence of the Basel Accord and its subsequent proposal, it is essential to realise the importance of capital in a financial institution (Matten, 1999:6). The identification, management and measurement of credit risk in a bank play a distinct role in the measurement of capital adequacy for a financial institution. The aim of this chapter is to consider first of all, the role and importance of capital in a financial institution, and subsequently, the Basel II approach to credit risk. This is important, as the purpose of this study is to consider the various approaches followed for the classification of operational risk losses related to credit risk.

Two approaches are prescribed for measuring credit risk. These two approaches are TSA, and the IRB approach, which consists of the foundation and the advanced approach. These approaches are discussed in more detail in this chapter.

2.2. A definition of capital

Koch and MacDonald (2003:471) define capital as: *“the cumulative value of assets minus the cumulative value of liabilities and represents ownership interest in a firm”*. The management of capital for corporate institutions and enterprises is a topic that has been amply covered during the past decades. However, the concept of capital for banking – from a regulatory perspective – differs significantly from accounting capital (Koch & MacDonald, 2003:471). The reason for this difference lies purely in the nature of capital: its sole and primary purpose is to absorb financial risks, instead of providing funding for the assets of the business (Matten, 2000:29).

2.2.1. Unique definition of capital to banks

Specific problems for banks arise (with regard to capital, capital allocation and the management thereof) in the unique form of their balance sheets, due to some common reasons. The source of a retail bank's finances – being mainly customer deposits – cannot be viewed as external funding to the institution, as it is part of the business itself. Secondly, this issue is exacerbated by the fact that banks are required by regulation to maintain levels of equity that is not necessarily strictly required for the financing of their operations. Finally, banks may be either asset-driven, or liability-driven. A bank is asset-driven when the majority of its business lies in the creation of assets, such as loans, while

leaving a portion of the balance sheet for which the bank has to seek refinancing. In the case of a bank being liability-driven, the bank has to consider where to invest surplus funds (Matten, 2000:2).

In classic corporate financial theory, capital exists mainly to carry out the following two particular activities or goals. The first is transference of ownership, where the institution transfers ownership of its assets, cash flow or profits to the shareholders through the selling of shares to third parties. The second is to fund the business (Matten, 2000:14). The transference of ownership and business funding are very closely incorporated in a non-financial institution. This is because the company views capital as a way in which funds are raised, while the shareholder requires a return on the funds from individual projects. However, for financial institutions the liability side of the balance sheet forms part of the activities of the bank, instead of existing purely to fund the activities of the bank (Matten, 2000:15).

Thus a textbook approach to capital management cannot be applied directly to banks. In order to ensure safe and sound operations that enhance the stability of the financial system, individual banking organisations need robust risk management and strong capital positions (Bernanke, 2006). As such, capital is a significant support for the safety and soundness of a banking system. One could point to numerous examples in history in which countries' banking and financial systems suffered because of inadequate capital during times of financial stress (Bies, 2005). To this end, the absorption of financial risk is essential and forms a vital part of a bank's business and it is not merely an incidental activity (Matten, 2000:29).

The fact that capital plays such a fundamental and integral role in a financial institution is amply illustrated through the attention and focus given to it by the various interested parties. Regulators and banking supervisors have deemed capital so important that the single global standard for establishing the strength of banking, is based around capital (Matten, 2000:29). However, it is not only the regulators who realise the importance of capital; most bank customers, counterparties, investors and rating agencies would agree that capital provides a valuable backstop against risk-taking (Bies, 2005).

Although the role players all agree on the importance of capital, their definitions of what capital is, differ. These different perspectives include the treasurer's view, the regulator's view, the risk manager's view and the shareholder's view (Matten, 2000:30).

The treasurer concerns himself with various forms of paid-in capital, for example equity, hybrid instruments, or subordinated debt. He typically aims to reduce the overall cost of capital by asking what capital is available, what instruments exist within the institution to raise capital, how the available base can be managed to meet requirements and how the raised funds can be invested (Matten, 2000:30).

The view of the regulator is slightly narrower in that it includes all forms of eligible paid-in capital. For example, subordinated debt – which only has a few years before it is due for repayment – will be

included only partially, while certain hybrid instruments might not be included at all. The regulator is therefore concerned about the level of capital to protect the deposits and creditors against losses (Matten, 2000:30).

The risk manager is concerned about the risk of losses. This function is independent of the entity carrying the cost of that loss. The risk manager is therefore more interested in, and involved with the estimation of the risk profile of the bank's positions, the size of potential losses, and ultimately the probability of the losses (Matten, 2000:30).

The shareholder is merely concerned with his/her investment, which includes the equity, retained earnings, or share premium accounts, which typically belongs to the shareholder. The shareholder is more concerned with the returns that are earned on invested funds, and the considerations as to whether proper returns are generated to compensate for the riskiness of activities undertaken (Matten, 2000:30).

Efficient capital management is not only fundamental, but a necessary precondition for the optimisation of shareholder value for financial institutions. Capital exists in a financial institution not to provide finance, but to absorb the risks undertaken. Based on this principle, it can be concluded that capital allocation is thus not ancillary to the business processes; it should, in fact, be part of them (Matten, 2000:1).

2.2.2. The reason why banks hold capital

The heart of a bank's business is the lending of deposits to its customers. The bank earns interest from these loans, which is in turn utilised to pay for the deposits. While customers' deposits and interest are safe, the bank will always be facing at least one of several risks, one of which will always include the risk of losing money on the loans given to customers (Chaudhary *et al.*, 2005).

A bank's assets – which are made up mainly of its loans and investments – are risky, uncertain, and always prone to losses. Its liabilities (which are made up of its deposits) are certain. That is why bank failures are caused largely by the losses incurred on its assets. Such losses might occur in the form of (Chaudhary *et al.*, 2005):

- default by borrowers, known as credit default risk;
- losses on its investments in different securities, which constitutes market risk; and
- fraud, systems and process failures, also known as operational risks.

The general accounting equation as it is commonly known, states that $\text{Assets} = \text{Liabilities} + \text{Owners' Equity}$. In other words, for a financial institution, the assets should be equal to the external liabilities plus capital. A loss in a bank's assets must be balanced by a capital reduction, as the liabilities – which are the bank's depositors – are to be respected at all times. Therefore, the bank should under all circumstances have sufficient capital for the absorption of losses because of credit, market and

operational risks. The reason why banks fail can thus be ascribed to such losses that cause their capital to be lost (Chaudhary *et al.*, 2005).

Capital has become the primary tool for reaching goals such as the absorption of large and unexpected losses, depositor protection and the insurance of on-going viability of the financial system (Matten, 2000:81). The theoretical reason that a bank holds capital is in order to provide protection against unexpected losses (Bessis, 2002:31). The amount of capital held should not only cover a bank's "normal" or expected losses, but also the unexpected and improbable losses. At the same time, the institution should be able to operate at the same level of capacity (Matten, 1999:6).

The role of capital, in any company, whether a deposit-taking institution or a corporation, is to provide creditor protection and to provide a buffer against future, unidentified losses; finally, it provides protection to depositors in the process (Matten, 2000:11). This is a simple view of the importance and role of capital in a bank, but it is important to provide an explanation for the seemingly high levels of capital that a bank holds, and is required to hold from a regulatory perspective. The bank is therefore required to review the forces behind the development of capital standards (Matten, 2000:11).

2.2.3. Economic capital versus regulatory capital

From a financial institution's point of view, the term "capital" can be divided into "economic capital" and "regulatory capital". Regulators believe that bank capital serves as protection of the deposit insurance funds in the event of the failure of the bank. Also, greater bank capital insures lower costs of arranging mergers or paying depositors in the case of a bank failing (Koch & MacDonald, 2003:481).

Banks would ultimately hold capital regardless of whether there is a regulatory requirement for them to do so. The main reason for this is that investors and depositors are more willing, and likely, to lend their money to a financial institution when they have the confidence that the institution has the ability to absorb large and unexpected losses. In addition, they should also be assured that bank owners themselves, have funds that are at stake in the successful operation of the institution (Yeh *et al.*, 2005:4).

Economic capital represents a bank's internal estimate of the capital required to run the business that is developed by the bank itself. This estimate of economic capital may differ from the minimum regulatory capital requirement that is defined for regulatory capital, one reason being that the bank might include risks that are not formally subject to regulatory capital; different parameters or methodologies might also be used (Saita, 2007:7). Economic capital is mostly defined as the level of capital that is required to protect the bank from losses, with a certain confidence level or probability, which is related to a desired rating (Elizalde & Repullo, 2007:88). Required economic capital can

therefore be defined as the amount of capital that a bank considers necessary for running the business from its point of view, totally independent of regulatory constraints (Saita, 2007:7).

Saita (2007:7) makes a basic distinction between regulatory capital and economic capital by stating that a bank calculates regulatory capital according to the regulators' rules and methodologies; hereby, a minimum regulatory capital requirement is also defined for each bank. The regulators also stipulate which components of the bank's balance sheet can be considered to be eligible as capital, that is, available regulatory capital (Saita, 2007:7). Regulatory capital, being the predominant focus of the study, can be defined as being derived from a set of rules, such as the Bank for International Settlements (BIS) capital accords. These rules are designed to ensure the banking system holds enough capital (Crouhy *et al.*, 2001:532). There is no real consensus regarding the intrinsic value of regulation, although regulation may be considered acceptable if it enables the minimisation of market imperfections such as monopolistic situation, imperfect information or to protect the public good (De Servigny & Renault, 2004:387).

Four general goals of banking regulations – and therefore regulatory capital – can be outlined (Bessis, 2002:25). Firstly, it improves the safety of the banking industry by imposing capital requirements directly in line with the risks that banks can be facing. Second, common benchmarks are set for all players, leading to a level and competitive playing field for banks. This aim is a reflection of the fact that there will be competitive imbalances in the system, with different banks subjected to different standards when global harmonisation is not present (Matten, 2000:15). The level of capital has an impact on the return required by shareholders; a bank with a lower capital requirement is in a position to price its products “more keenly”, as its threshold return would be lower. Therefore, greater stability is brought to the system when banks are forced to hold a minimum level of capital (Matten, 2000:16). The third general goal is the promotion of sound supervisory and business practices, and finally, the imposition of the recognition of the concept behind the capital adequacy principle (Bessis, 2002:25).

2.2.4. The development of capital standards for banks

By the beginning of the 21st century banks came under immense pressure to improve their capital efficiency. This pressure mainly came from a necessary and essential increase in the level of capital that was required by regulators, as well as the deregulation of the industry. In addition, shareholders have become more demanding and insistent, and rating agencies substantially more experienced in knowing their requirements (Matten, 2000:4). This was, however, not always the case. The deregulation of the banking and financial industry occurred in three phases, described in more detail below.

The first phase. Banks were generally highly regulated and restricted by national regulators, protecting them from competitive forces until the late 1970s. This was mainly the result of the impact

of the Great Depression that plagued the US, and the role hyperinflation played in the political developments in Europe during the 1930s (Matten, 2000:11).

The 1970s marked a time when commercial banks in the United States faced several restrictions. These included restrictions on interest rates, on both the lending and deposit sides of businesses. Banks were also limited in the geographical scope of their operations (Strahan, 2003:111). The Bretton Woods agreement, which was established in 1944 and consisted of a system of exchange rate stability, ensured that banks had a fairly easy time in managing their exposures (Matten, 2000:12). However, after the Bretton Woods system failed in the early 1970s, exchange and interest rate volatility increased substantially. The first phase – arguably starting with the collapse of the Bretton Woods agreement and the initial oil price crisis in the beginning of the 1970s – exposed banks to risks they were certainly not familiar with, namely considerable rises in interest rates and currency exchange rate volatility (Matten, 2000:4). This was as a result of the gradual relaxation of exchange-control regulations. Subsequently, central banks were left with only a single useful way of implementing monetary policy: by employing their influence over the money supply to banks, and subsequently, over interest rates (Matten, 2000:12).

The second phase. During this phase the deregulation of the financial industry was a priority, with policymakers aiming to destroy what was seen as a cosy cartel. This phase was characterised by a technology revolution, which globalised a market that was previously closed. This led to a higher level of competition, which in turn led to banks placing market share above all other goals. The resulting effect was an erosion of capital levels and also credit standards (Matten, 2000:4). As a consequence, banks were faced with an increasingly volatile environment, accompanied by highly inelastic pricing control over liabilities and assets (Matten, 2000:12).

To combat these effects, the financial industry was deregulated, exposing the banks to the unprotected environment of competition. Therefore, nearing the end of the 1970s, continuous deregulation of the banking sector started to take place; this included the abandonment of asset regulation, deposit rate ceilings and also entry controls (Stolz, 2002:4).

The third phase. Subsequently, a significant banking crisis took place, namely the partial collapse of the loans and savings industry in the United States at the beginning of the 1990s. Banks became increasingly aggressive, expanding to new markets in which they had very little or even no experience (De Servigny & Renault, 2004:384). The result was that the industry became prone to excess, over-lending to Latin American governments. Consequently, in the third phase, regulators were introduced to stringent and globally consistent standards that ensure both the safety of the system, as well as a fair, level playing field (Matten, 2000:5).

2.3. The Basel Committee

As discussed above, the regulatory system evolved over time and has undergone significant changes through the years. By the 1970s supervisors agreed on the general need to compel all internationally active banks to preserve and maintain pre-defined minimum adequate levels of capital in order to achieve the following two objectives (Saita, 2007:8):

- preserving systemic stability in the context of growing deregulation and fading competitive barriers; and
- conserving a level playing field among banks from different countries, while eliminating possible competitive advantages for the banks that were previously allowed to hold less capital than their peers.

In 1974 this led to the foundation of the BCBS by the central bank Governors of the Group of Ten (G10) countries. The aim was to develop a common framework; an effort that led to the Basel I Accord being published in July 1988 (Saita, 2007:8).

Following the oil crisis of 1973, severe disturbances shook the financial markets, culminating in 1974 with the downfall of Bankhaus Herstatt in West Germany. This put into motion a chain reaction of events, leading to the collapse of a larger bank, namely Franklin National Bank in New York, and several other banks (United Nations Conference on Trade and Development, 2006:5). The Basel Committee on Banking Supervision (BCBS) was established at the end of 1974 in the aftermath of these serious disruptions in international currency and banking markets with the main purpose of improving supervisory quality, and in turn preventing a systemic collapse of the world's financial markets (United Nations Conference on Trade and Development, 2006:6). The first meeting took place in February 1975. Meetings have been held regularly, or about three to four times a year since (BIS, 2009).

The BCBS serves as a forum for regular collaboration between the member countries on general banking supervisory matters. The main objective is to improve supervisory understanding as well as the quality of worldwide banking supervision. This objective is to be reached in three principal ways, namely the exchange of information on national supervisory arrangements, the increased effectiveness of the techniques that are to be applied for the supervision of the international banking business, and the laying down of minimum supervisory standards specifically in those areas where they are desirable (BIS, 2009:1).

No formal supranational supervisory authority is held by the BCBS and its conclusions were never intended to have, and do not have, any legal force (BIS, 2009:1). The BCBS documents merely represent international guidelines that are to be translated into national regulation, occasionally leaving national supervisors some freedom to define their exact implementation details on selected

issues (Saita, 2007:8). The framework established by the BCBS was intended to apply to the internationally active banks as supervised by the G10 countries. Other countries, however, have also adopted this framework and still continue to do so. Compliance with the Basel Accord gives banks a “seal of approval” with regards to capital adequacy and also makes it easier for them to compete (Matten, 2000:97).

2.3.1. The goals and strategies of the BCBS

The BCBS has three broad goals. The first goal is to provide participating financial institutions with a forum for communication, dialogue and information exchange among supervisors. Perhaps the most visible goal to the broader community is the second goal, which includes the promotion of improvements in the general risk management practices and banking supervision framework. Thirdly and finally, the promotion of mechanisms for pragmatic implementation of the principles developed by the BCBS is deemed as important (BIS, 2006b). Central to the second goal is ensuring that banks follow sensible risk management practices. Since banks rely heavily on capital for their core business, it is no surprise that the Basel Accord has strict subscriptions regarding capital and minimum capital requirements as a principal way of managing risk. The following section will discuss regulatory capital and Basel’s view on this capital.

2.3.2. The concept of regulatory capital

The 1988 Basel I Accord defines the concept of regulatory capital in tiers. These tiers comprise core capital (Tier 1 capital) and supplementary capital (Tier 2 and Tier 3 capital) (Saita, 2007:9).

2.3.2.1. Tier 1: core capital

This element includes permanent shareholders’ equity and also disclosed reserves. Tier 1 capital is capital that is freely and permanently available for absorbing losses, while at the same time not obligating banks to cease trading. An example would typically include the ordinary share capital of the bank. The importance of Tier 1 capital lies in the fact that it safeguards not only the survival of the bank, but also the stability of the financial system (Matthews, 1996:136).

2.3.2.2. Tier 2: supplementary capital

This element includes undisclosed reserves, revaluation reserves, hybrid (debt/equity) capital instruments and subordinated term debt. Tier 2 capital generally absorbs losses mostly in the event of a wind-up of a bank. Therefore, Tier 2 capital provides a significantly lower level of protection for both depositors at the bank and other creditors. Tier 2 capital will come into effect subsequent to Tier 1 capital being lost by the bank. An example of Tier 2 capital would typically be subordinated debt, as in the event of a winding-up, subordinated debt holders are only repaid once all other creditors have already been repaid (Matthews, 1996:136).

2.3.2.3. Tier 3: short term subordinated debt

Banks may also – at the discretion of their national authority – employ a third tier of capital. Tier 3 capital consists of short-term subordinated debt, for the purpose of meeting market risk capital requirements only (BIS, 2006a:16). Tier 3 capital can be used to serve as a buffer against losses caused by market risk events in the instance that Tier 1 and Tier 2 capital are insufficient for these purposes (Matthews, 1996:136).

2.4. The capital adequacy principle

Regulations impose a quantification of potential losses originating from risks; these potential losses are the groundwork for determining the capital base of a financial institution. Importantly, the heart of risk regulations is the “capital adequacy” principle, and this principle imposes a capital base corresponding to the risks that a bank is exposed to (Bessis, 2010:9).

This principle of capital adequacy was the starting point of the materialisation of today’s modern risk management. The reason for this is because it requires bank risk managers to translate risks, which might at first sight appear as intangibles, into monetary values. Therefore, the actual quantification of various risk types and also the modelling thereof made remarkable advances under the impetus of capital regulations (Bessis, 2010:9).

The key concept around capital adequacy is that banks must hold capital at a level that reflects the risk contained in their balance sheet assets. Three different components are taken into account when referring to capital adequacy, namely capital ratio, risk-weighted assets (RWA) and the capital base (Smit, 2009:22). A bank’s risk-based capital ratio would have a numerator representing the capital available to the bank, while the denominator would be a measure of the risks faced by the bank. Last mentioned is also referred to as the RWA of the bank (Ferguson, 2003):

$$\text{Capital ratio} = \frac{\text{Capital base}}{\text{RWA}}, \quad (2.1)$$

The capital ratio can be determined by applying the definition of regulatory capital and RWA. It can therefore be said that the capital ratio is the relationship between RWA and the capital base. The capital base consists of the different tiers of capital developed by the BCBS, as discussed above. RWAs represent the bank’s assets multiplied by the proper risk weight (Saita, 2007: 11).

2.5. The New Basel Capital Accord

The shortcomings of the 1988 Basel I Accord led the BCBS to introduce and release a first consultative package on a new and more risk-sensitive accord in June 1999; a second revised version

was later released in January 2001. Table 2.1 below can be used to describe the rationale for a new accord, that is, the need for more flexibility and risk sensitivity (Bessis, 2002:41):

Table 2.1: The rationale for a new accord – a comparison between the 1988 Basel I Accord and the Basel II Capital Accord.

The 1988 Basel I Accord	The Basel II Capital Accord
Focus is placed on a single risk measure	More emphasis is placed on banks' own internal methodologies, supervisory review and market discipline
One-size-fits-all: only one option is proposed to banks	Flexibility, menu of approaches, incentives: banks have several options
Broad-brush structure (forfeits)	More credit risk sensitivity for better risk management

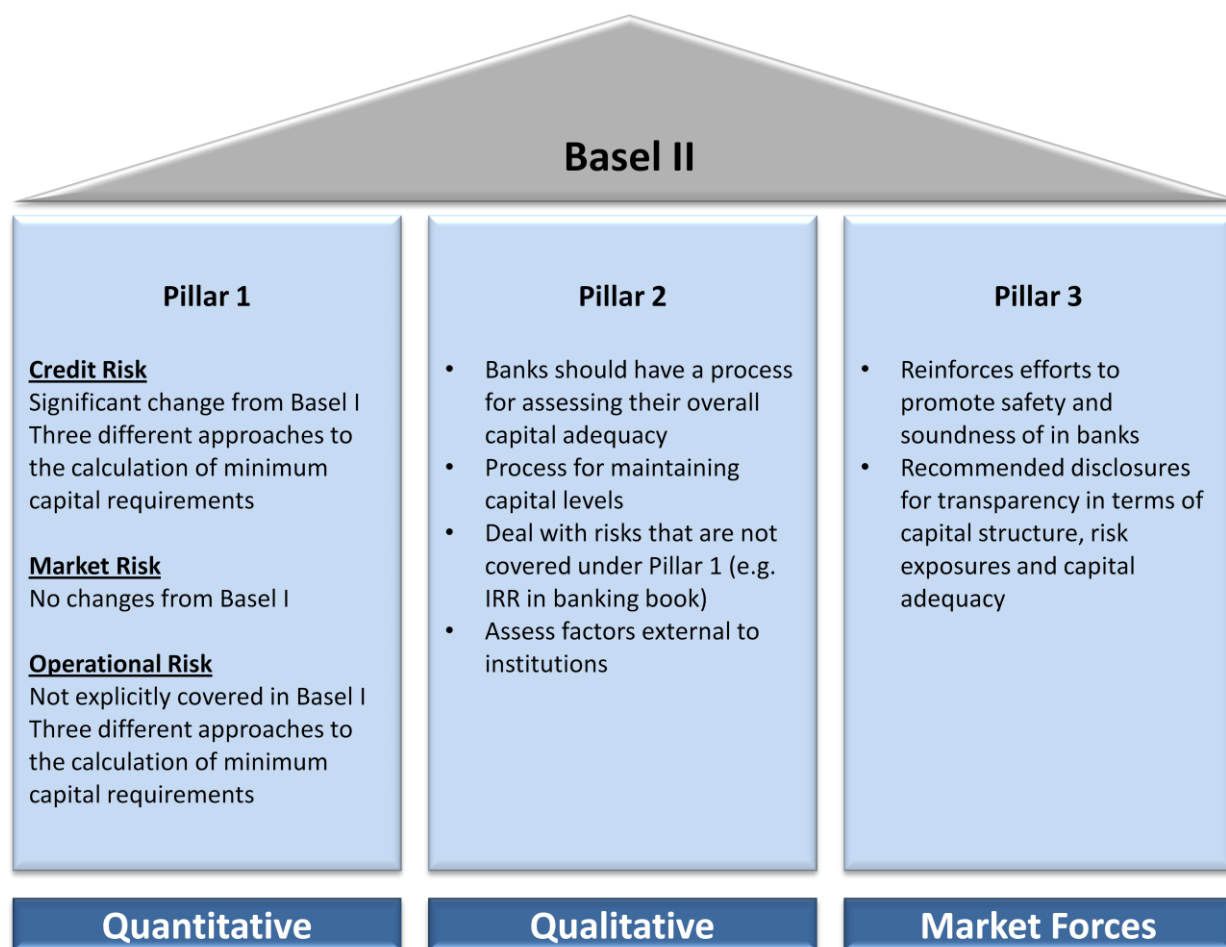
Source: Bessis (2002:41)

The Basel I Accord focused mainly on capital regulation; Basel II, however, consists of three mutually reinforcing pillars (Stolz, 2002:5). Together with this came capital requirement definitions with major enhancements to the general credit risk measures, as well as the first coverage of operational risk, disclosure, supervisory review process, and also market discipline. At the same time, some features of the 1988 Basel I Accord were enhanced (Bessis, 2010:232).

The main idea of the new proposal is that the safety and soundness of the financial system could not be obtained and maintained by merely imposing on banks some minimum capital requirements. This is what is implied by Pillar 1. It is imperative that a bank must also rely on increased attention and power for the supervisory review process – this is included in Pillar 2. Finally, Pillar 3 implies that a greater recourse to risk disclosure and therefore market discipline is important (Saita, 2007:10). Basel II therefore comprises the following three pillars (De Servigny & Renault, 2004:396):

- Pillar 1: Minimum Capital Requirements. The objective here is the determination of the amount of capital required, given the level of risk in the bank's portfolio.
- Pillar 2: Supervisory Review Process. Early action from regulators is enabled, deterring banks from using unreliable data.
- Pillar 3: Market Discipline. The banks' disclosure vis-a-vis its competitors and financial markets is devised in order to enable external monitoring, and also a better identification of its risk profile.

The general framework is illustrated in Figure 2.1.



Source: Adapted from KPMG (2003:5) and De Servigny & Renault (2004:397)

Figure 2.1: The framework of the Basel II Capital Accord.

Basel II defines capital charges not only for credit risk, but also for operational risk and contains – for the first time – an integrated approach in which credit, market and operational risks are united with the aim of calculating the overall risk exposure of a bank and to calculate the required regulatory capital that is needed to support the bank’s specific risk profile (Gallati, 2003:342).

The three pillars of Basel II

The three pillars of Basel II were established with the aim to achieve the following four objectives. The first objective is to further soundness and safety in the financial system through the preservation of at least the same level of capital as is currently maintained in the system. Secondly, competitive equality is to be improved by ensuring that two financial institutions with the same portfolios hold similar levels of capital, irrespective of where they are located. The third objective is the establishment of a broader approach to risks, as to eliminate the shortcomings and criticisms of Basel I.⁴ This entails covering more risk types such as operational risk and interest rate risk in the banking book. The fourth and final objective is the focus on internationally active banks, while also ensuring

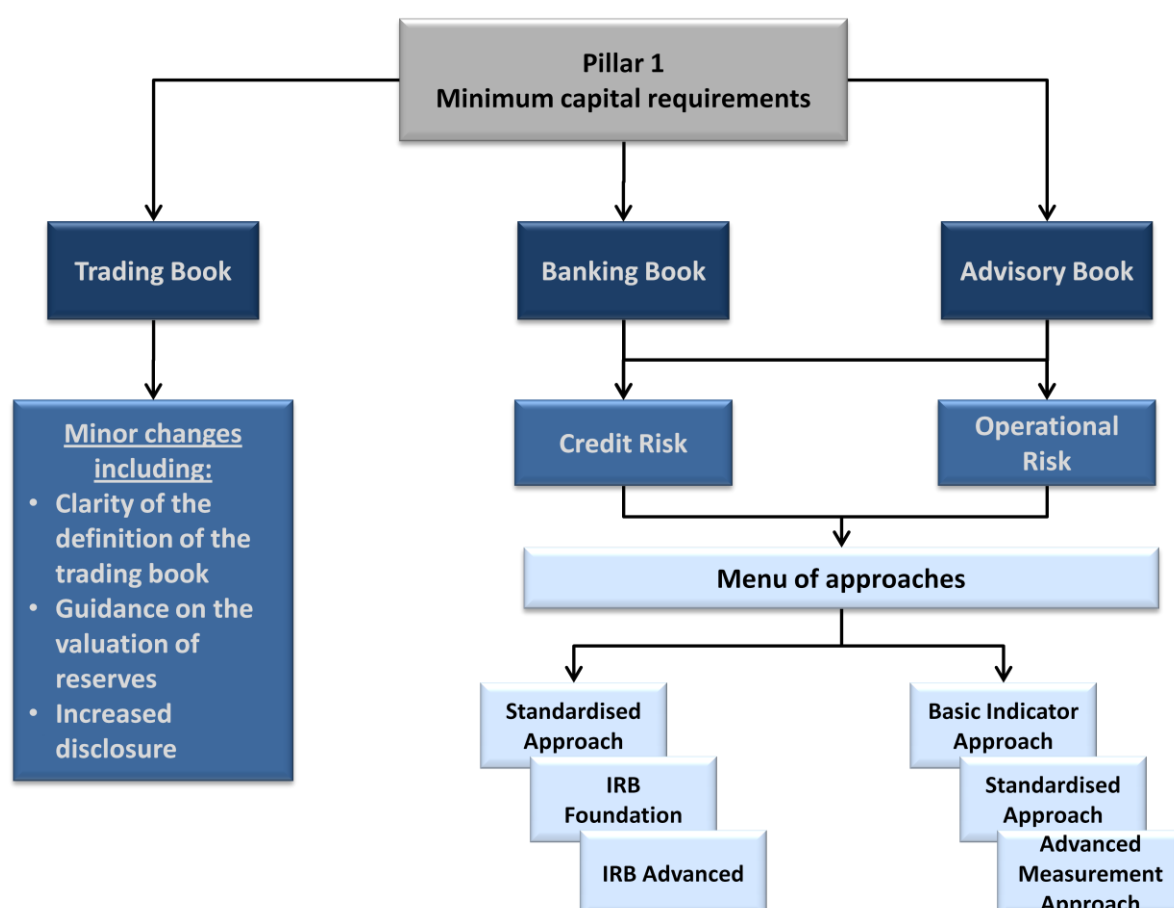
⁴ Note that any reference to Basel I or Basel II is referring to the Basel I or Basel II Capital Accord.

that the approach can be applied to banks with different levels of sophistication and complexity (Crouhy *et al.*, 2001:72).

The three mutually reinforcing pillars together should therefore add to the safety and soundness of the financial system. The BCBS emphasises the need for rigorous application of all three the pillars (Gallati, 2003:352). More detail on the three pillars is provided in the following section.

2.5.1.1. Pillar 1: overall minimum capital requirements

Pillar 1 of Basel II can generally be viewed as the main “pillar” of the regulations, as it sets out the minimum capital requirements, or capital adequacy levels, that a bank is required to hold based on its credit, operational and market risks. The major changes that were brought to the minimum capital requirements originally set out in Basel I are the general approaches to credit risk and also the inclusion of explicit capital requirements for operational risk (Bessis, 2002:42). The rules on market risk received minor modifications (Saita, 2007:11). The BCBS’ general goal is to ensure that the bank’s regulatory capital requirement is adequate to address underlying risks (Gallati, 2003:352). Figure 2.2 can be used to illustrate Pillar 1 of Basel II:



Source: Jones and Shiekh (1999:48)

Figure 2.2: Pillar 1 of Basel II.

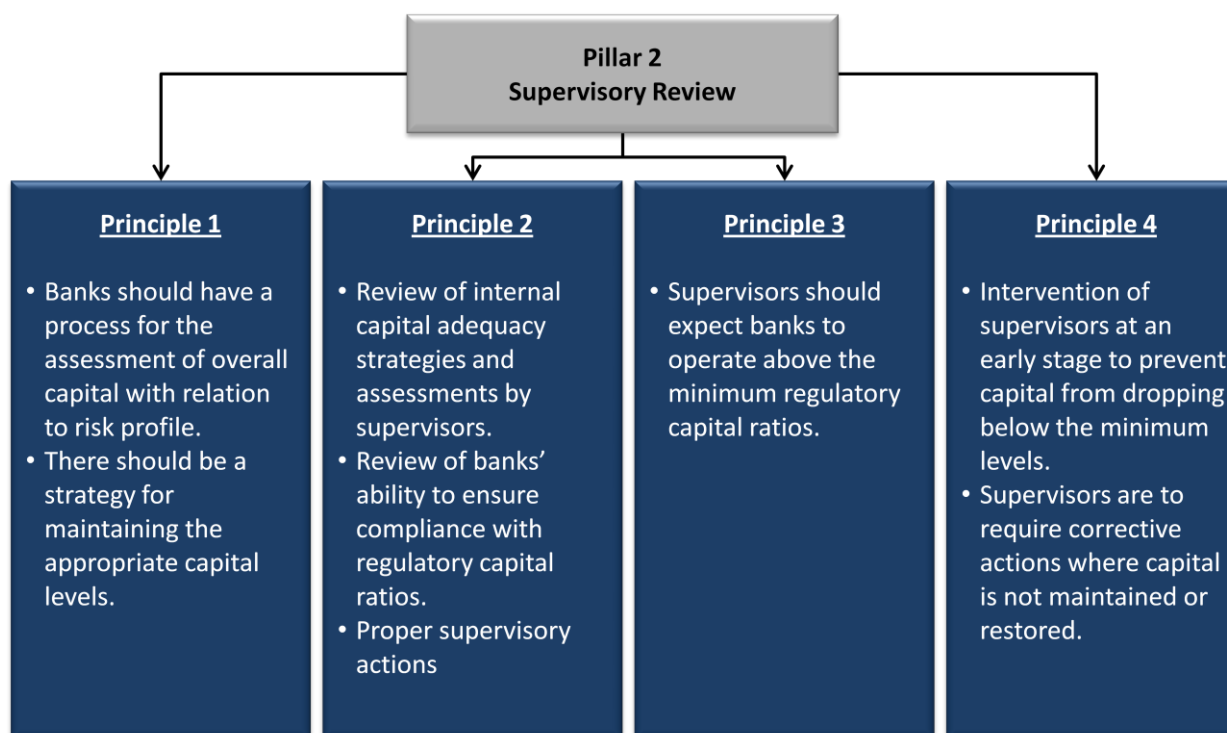
2.5.1.2. Pillar 2: supervisory review process

Although the minimum regulatory capital requirement was changed to make it more risk-sensitive, the Basel II Accord clearly states that a bank's ability to survive does not only depend on the amount of capital held to face possible risks. Elements such as the eminence of risk management systems and procedures, the reliability of its provisioning policy and its capital management and planning process are also of vital importance to a bank's ability to survive (Saita, 2007:14). The second pillar can therefore be viewed as a tool that is used to clarify the role of national supervisory authorities, thereby encouraging improvements in banks' risk management techniques, setting, where required, individual capital requirements higher than Pillar 1 minimums for such banks where risk management systems and procedures appear to be ineffective (Saita, 2007:14).

In terms of Pillar 2, the BCBS sets out three main areas that might have significance (BIS, 2006a:204):

- Risk types that are considered by Pillar 1 but are not completely captured by the Pillar 1 process, for instance credit concentration risk appearing in the credit risk portfolio.
- Issues not accounted for under Pillar 1, such as interest rate risk in the banking book arising from the mismatch between the interest rate sensitivity of assets and liabilities.
- Factors considered external to the bank that may impact the bank's risk profile, e.g. the business cycle.

Under Pillar 2, banks are allowed to have their own measures of capital requirements beyond the scope of Pillar 1 and over time, regulators will likely require banks to disclose much more risk information (KPMG, 2003:8). Additionally, in order to comply with Pillar 2, banks are required to implement a consistent risk-adjusted management framework that is comparable in its sophistication to, and also closely linked with the risk approaches chosen under the first Pillar (KPMG 2003:6). Pillar 2 is based on four key principles of supervisory review, which address two central issues, the first of which is the need for banks to assess capital adequacy relative to general risks. The second issue to be addressed is the need for supervisors to review the banks' assessments, and thereby determine whether it is required of them to request the banks to hold additional capital beyond that required under the first Pillar (KPMG, 2003:6). The four key and basic principles that were formulated by the BCBS in order to inspire supervisors' policies are summarised in Figure 2.3 (Bessis, 2002:49):



Source: Adapted from Bessis (2002:49)

Figure 2.3: The four principles of the supervisory review process.

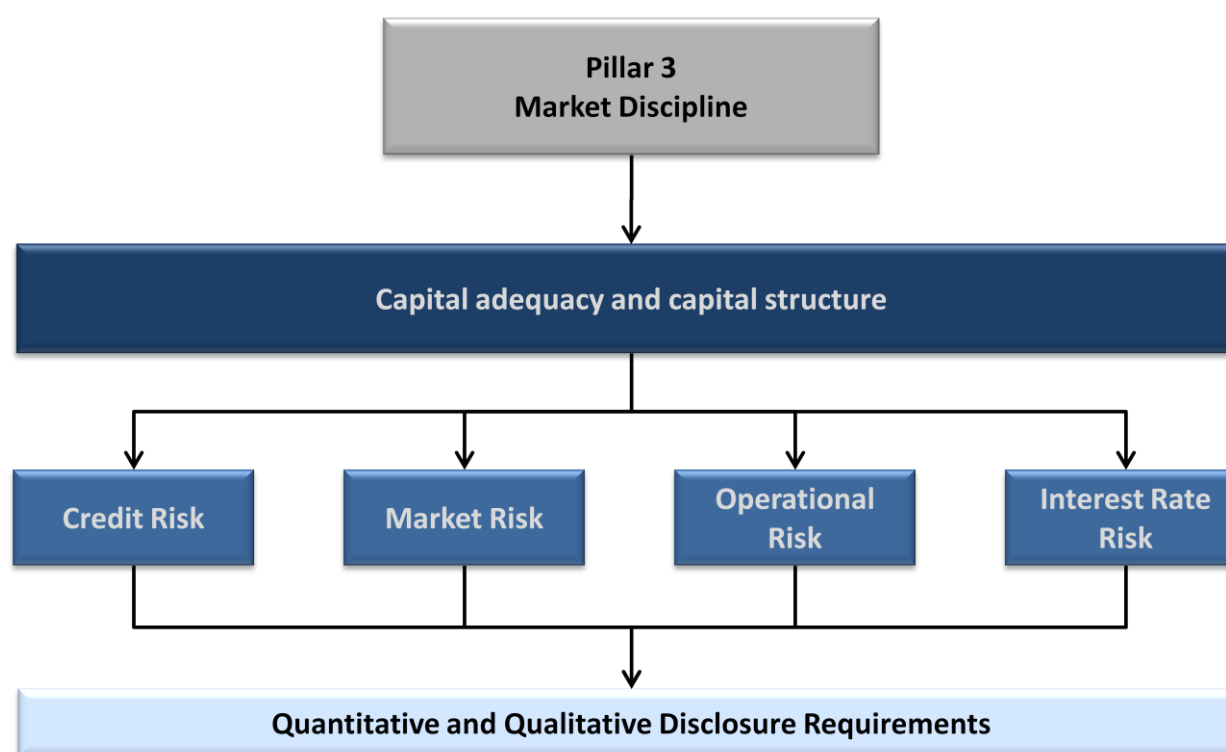
2.5.1.3. Pillar 3: market discipline

The purpose of Pillar 3 is to complement the minimum capital requirements set out in Pillar 1, and the supervisory review process of Pillar 2 (BIS, 2006a:226). The BCBS aims to foster market transparency in order for market participants to easily assess bank capital adequacy (Crouhy *et al.*, 2001:87). Disclosure requirements and recommendations are set out in several areas; this includes the way a bank calculates its capital adequacy and measures its risks. The core set of disclosure recommendations is relevant to all banks.

More thorough requirements for supervisory recognition of internal methodologies for credit risk, credit risk mitigation techniques, and asset securitisation are also included. The bank's objective and strategy for the disclosure of public information concerning its financial condition and performance should be approved by the board of directors and set out in a formal disclosure policy. In addition, increasingly detailed and comprehensive disclosure requirements will be applicable for supervisory recognition of internal methodologies for credit risk, credit risk mitigation techniques, and asset securitisation. Disclosures will include core components – comprising of qualitative and quantitative factors – and supplemental components. The banks are also required to implement a process for assessing the appropriateness and frequency of disclosure. This verification process is to be performed at least semi-annually and quarterly disclosure is required for internationally active banks (Gallati, 2003:354).

Therefore, Pillar 3 encompasses both quantitative and qualitative disclosure requirements; these requirements are for capital adequacy and capital structure, as well as credit risk, market risk, operational risk and interest rate risk in the banking book (KPMG, 2003:22). Pillar 3 is summarised in Figure 2.4 below.

Subsequent to the background provided of capital terms and the Basel Committee, the next section focuses on credit risk, and the detailed requirements of Basel in terms of credit risk.



Source: Adapted from KPMG (2003:22)

Figure 2.4: Market discipline according to Basel’s Pillar 3.

2.6. The definition of credit risk

Credit risk is the most important risk for banks and financial institutions in general. It can most simply be defined as the potential that a borrower from the bank, or counterparty, will fail to meet her obligations in accordance with agreed terms (BIS, 2000:1). The BIS also defines credit risk as the risk that a counterparty will not settle an obligation in full value, either when due or at any time thereafter (BIS, 2009:57).

The most common credit events in financial institutions include failure to meet payment obligations when they are due, repudiation, bankruptcy, obligation default and/or obligation acceleration, and material adverse debt restructuring (Sungard, 2010). On a higher level, the three most commonly utilised credit events include failure to pay, bankruptcy and restructuring (Creditflux, 2010).

2.7. The expected and unexpected losses of credit risk

Credit risk – in a narrow sense – can be defined as the risk arising from an unexpected deterioration in the credit quality of a counterparty (Saita, 2007:68). It should, however, be kept in mind that credit risk management covers not only unexpected, but also expected losses. It is therefore imperative to supply some background on expected losses and unexpected losses, before proceeding to a detailed discussion of Basel II credit risk measurement approaches.

As stated above, credit risk management covers unexpected and expected losses. The former is covered by bank capital, whereas the latter is covered by provisions. The prominence given to unexpected events can be derived from the fact that the nature of the credit business includes a certain number of defaults in a portfolio. These defaults can be expected and also estimated ex ante; therefore, strictly speaking, such defaults are not a source of risk (Saita, 2007:68). It is therefore true that expected losses are not part of risk, since they are predictable by a bank as the normal level of losses associated with the bank's day to day business and credit portfolio (Saita, 2007:68).

Matten (2000:157) is also of the opinion that expected loss is not part of risk, but is a cost of doing business. One can go further in defining expected loss as the average level of credit loss, which is to be expected from any given exposure or set of exposures over a given time period (Matten, 2000:188). For this reason, expected loss is the mean of the loss distribution and provides the foundation for economic provisioning. The expected loss measure used in Basel II as a benchmark for provisioning, applies to credit losses (Bessis, 2010:214). Expected loss is the first indicator of risk that a bank considers, and it is the level of loss that the bank is exposed to on average. The expected loss on a security i is defined as (De Servigny & Renault, 2004:237):

$$EL_i = EAD_i \times PD_i \times LGD_i \quad (2.2)$$

where:

EL = Expected Loss,

EAD = Exposure at Default,

PD = Probability of Default, and

LGD = Loss Given Default.

The expected loss of a portfolio of N assets is the sum of the expected losses on the constituents of the portfolio (De Servigny & Renault, 2004:237):

$$EL_p \equiv E(L_p) = \sum_{i=1}^N EL_i \quad (2.3)$$

In this instance, L_p equals the random loss on the portfolio. EL_p is the random expected loss on the portfolio. There exists an *ex post* difference between actual and expected loss, which is referred to as the unexpected loss. From an *ex ante* perspective, unexpected losses can be further defined as the difference between the amount of losses associated with an extreme percentile in the probability distribution of future losses, and the amount of expected losses (Saita, 2007:69). It should be noted that unexpected loss is modelled firstly at the individual loan level (Matten, 2000:158).

The unexpected loss, UL_p , is defined as the standard deviation of portfolio losses (De Servigny & Renault, 2004:237):

$$UL_p = \sqrt{E\{[L_p - E(L_p)]^2\}}. \quad (2.4)$$

From an economic point of view, expected losses are, on average, unavoidable. At the same time, banks should hold capital to face unexpected losses. This principle is clearly defined in the Basel II Accord, which will be discussed in more detail in the sections that follow. The Basel II Accord states that regulatory requirements are defined in terms of unexpected losses, provided that a bank can prove to have adequate provisioning policies (Saita, 2007:69).

2.8. Basel II credit risk measurement approaches

Basel II provides a range of “risk-sensitive options” that banks can utilise to address both credit risk and operational risk. Specifically for credit risk, this range includes the following approaches:

- the Standardised approach (TSA), which comprises of the simplest requirements;
- the Foundation approach (which is also an internal ratings based approach); and
- the Advanced Internal Ratings Based (AIRB) approach, where internal ratings imply that banks themselves assign the assessments of the relative credit risks of borrowers and/or facilities.

The ability of a bank to choose among these three approaches is generally the substantial revision that was introduced by the BCBS, thereby modifying the way in which risk weights are determined in order to make them more risk sensitive (Saita, 2007:11). These approaches are consistent with the BCBS’ goal of moving away from a one-size-fits-all approach to capital adequacy (BIS, 2001a:27). The approaches were proposed in a continuum of increasing sophistication to calculate required capital for credit risk (BIS, 2001a:27).

The BCBS permits banks a choice between two broad methodologies for calculating capital requirements for credit risk. The first alternative is to measure credit risk in a standardised way whilst being supported by the assessment of external institutions. The alternative methodology, which can be divided into “foundation” and “advanced” approaches, is subject to the approval of the bank’s supervisor, and allows banks to use their own internal rating systems (BIS, 2003:6). The major

difference between TSA and the AIRB approach lies in the fact that supervisory weights are used for TSA, whereas the AIRB approach relies on internal ratings (Bessis, 2002:43).

The BCBS encourages banks to move along the spectrum of available approaches as set out above as they develop more advanced measurement systems and practices (BIS, 2003:120). A bank will, however, not be allowed to choose to regress to a simpler approach once it has been approved for a more advanced approach without the proper supervisory approval. Also, if the relevant supervisor establishes that the bank using a more advanced approach no longer meets the criteria for this approach, it may require the bank to regress to a simpler approach until it meets the requirements specified by the supervisor for returning back to the more advanced approach (BIS, 2003:120).

2.8.1.1. TSA

TSA is a refinement of the 1988 Basel I Accord, in that it tries to discriminate better among borrowers that comprise of different risks, based on their external rating (Saita, 2007:80). More precisely, TSA is an effort to refine the simplicity of the risk weights defined by the 1988 Capital Accord (Saita, 2007:81).

Risk-weight adjustments are applied to the value of a bank's on-and-off balance sheet assets according to the riskiness of the underlying assets (Yeh *et al.*, 2005:7). Risk weights based on assessments or ratings by external credit assessment institutions or in short, rating agencies, or Export Credit Agencies (ECAs) for sovereign risks are assigned to various types of counterparties, namely sovereigns, banks and corporates (Bessis, 2002:43). This is in order to increase capital requirement risk sensitivity, and to increase the amount of risk-weight categories applied to the underlying assets. This ensures that TSA differentiates general riskiness not only within asset classes, but also across different asset classes (Yeh *et al.*, 2005:7).

In TSA, the RWA are therefore the product of the exposure amount and supervisory determined risk weights. Similar to the 1988 Accord, the risk weights are dependent on the category of the borrower, that is, sovereign, corporate or bank (Bessis, 2002:43). A claim on a sovereign is generally a claim against the central bank or the government of the sovereign country. Banks use the risk weightings assigned by Export Credit Agencies (ECAs), while claims on sovereigns are risk weighted.

2.8.1.2. Internal ratings based (IRB) approaches

The IRB approach is based on measures of unexpected losses and expected losses, and the so-called "risk-weight functions" produce the capital requirements for the unexpected loss portion (BIS, 2006a:52).

Two versions for the IRB approach exist, namely the "foundation" (FIRB) and the "advanced" approaches (or the AIRB approach). The IRB approaches lay down the principles for evaluating credit risk economically (Bessis, 2002:44). There are five key elements (BIS, 2001b:4):

- a general classification of exposures by a broad exposure type;
- for each exposure class, or asset class, certain risk components that should be provided by the bank by using standardised parameters or its own internal estimates;
- a risk-weight function, which provides risk weights – and thereby also capital requirements – for a given set of these components;
- a set of minimum requirements that should be met by a bank in order to be eligible for IRB treatment for that exposure; and
- across all defined asset classes, supervisory compliance review with the set minimum requirements.

Each of the above elements will be discussed in more detail below.

2.8.1.3. Categorisation of exposures

Banks' credit-related business is managed in broad business lines, and each of these business lines encompasses a variety of relative borrower and exposure types. The key common bonds that define a portfolio or business line are mostly related to the nature of the customer – e.g. governmental, household, corporate – , the nature of the transaction, or a combination of customer nature and transaction nature (BIS, 2001b:5).

Under the IRB approach, banks are required to assign banking-book exposures into broad classes of exposures with different underlying credit risk characteristics (BIS, 2001b:5). The “banking book” refers to general commercial banking activities, and therefore includes all lending and borrowing (Bessis, 2010:24).

According to IRB approaches, all exposures in the bank are classified into different exposure classes, or asset classes (Saita, 2007:82):

- corporate exposures;
- sovereign exposures;
- bank exposures;
- retail exposures; and
- equity exposures.

The five broad asset classes, as set out above and as defined by Basel II, also consist of several subcategories, which will be described in more detail below. In particular, the corporate asset class can be subdivided into five classes (BIS, 2006a:53).

2.8.1.3.1. Exposures to various asset classes

A corporate exposure is generally defined as a debt obligation of a corporation, partnership, or proprietorship. Banks have permission to distinguish between their exposures to small- and medium-sized entities (SME) (BIS, 2006a:53).

The five broad asset classes, as set out above and as defined by Basel II, also consist of several subcategories; in particular, the corporate asset class can be subdivided into five classes, namely project finance, object finance, commodities finance, income-producing real estate and high-volatility commercial real estate (HVCRE) (BIS, 2006a:53).

The sovereign asset class under IRB covers all exposures to such counterparties that are treated as sovereigns under TSA. This includes sovereigns and their central banks, certain public sector entities (PSEs) identified as sovereigns in TSA, as well as multilateral development banks (MDBs) that meet the criteria for a 0% risk weight under TSA (BIS, 2006a:55).

Exposures to banks and securities firms are included under Bank exposures. This includes MDBs that do not meet the criteria for a zero per cent risk weighting under TSA (BIS, 2001b:73). Bank exposures also include claims on domestic PSEs that are treated like claims on banks under TSA (BIS, 2006a:55).

For retail exposures, the BCBS undertook to supply an objective definition of “retail portfolios” in order to ensure consistency in the application of the regulatory IRB framework (BIS, 2001b:55). An exposure will therefore be categorised as retail in the instance that it meets each of the following criteria (BIS, 2001c:55):

- the following lending types are considered retail:
 - credit cards;
 - instalment loans;
 - revolving credits;
 - residential mortgages; and
 - small business facilities.
- the exposure is to an individual person, and/or guaranteed by such person;
- the exposure is one of a large pool of loans that are managed by the relative bank in a comparable fashion; and
- each individual exposure has a low value.

2.8.1.4. Risk components

The capital charge calculated for exposures within each of the above five asset classes will be dependent on a specific set of risk components. These risk components are inputs to the capital charge calculation. Under the IRB framework of Basel II, these inputs can be provided either through the

utilisation of standardised supervisory rules, referred to as the “foundation” methodology, or internal assessments, referred to as “advanced” methodology (BIS, 2001b:5). Depending on the approach that the bank chooses to follow, the bank shall utilise either its own estimates of the risk components, or the standardised supervisory estimates. These risk components are the PD (Probability of Default), Loss Given Default (LGD) and Exposure at Default (EAD) (Bessis, 2002:44).⁵

A PD quantifies the chances that a borrower might default (Bessis, 2010:235). A default has occurred when either or both of the following events have taken place (BIS, 2006a:100):

- the bank considers that the obligor is unlikely to pay its credit obligations to the banking group in full, without recourse by the bank to actions such as realising security; or
- the obligor is past due more than 90 days on any material credit obligation to the banking group. In the case of overdrafts, these will be considered as being past due once the customer has breached a limit, or been advised of a limit smaller than the current outstanding amounts.

The second risk component that is also a key input in credit risk analysis is the Loss Given Default, or the LGD. The LGD is defined as 1 minus the recovery rate. The recovery rate is the amount of money, expressed as a percentage of the par amount that can be recovered on loans or bonds that have defaulted (De Servigny & Renault, 2004:117). The PD typically summarises the creditworthiness of a company, whereas the recovery rate is mostly specifically focused on the facility level (De Servigny & Renault, 2004:177).

The LGD can be defined simply as the ratio of the loss incurred on an exposure, relative to the EAD of the exposure (Saita, 2007:90). As discussed above, a bank is to provide an estimate of the LGD for its exposures, and there are two approaches for deriving this estimate, namely the foundation approach and the advanced approach.

Under the foundation approach, senior claims on corporate, sovereigns and banks not secured by recognised collateral will be assigned a 45% LGD (BIS, 2006a:67). A partial reduction is possible when collateral is available (Saita, 2007:91). Furthermore, all subordinated claims on corporate, sovereigns and banks will be assigned a 75% LGD (BIS, 2006a:67). A subordinated loan is a facility that is expressly subordinated to another facility (BIS, 2006a:67).

Under the advanced approach, supervisors may permit banks to use their own internal estimates of LGD for corporate, sovereign and bank exposures. Under the advanced approach, supervisors stress that the bank “must estimate an LGD...that aims to reflect economic downturn conditions where necessary to capture relevant risks.” (BIS, 2006a:103). This LGD cannot be less than the long-run default weighted average loss rate given default (BIS, 2006a:103).

⁵ See section 2.7 for detail on the risk components.

EAD for an on-balance or off-balance sheet item is defined as the expected gross exposure of the facility upon default of the obligor (BIS, 2006a:104). It is true that for certain kinds of loans, the amount the bank is lending is fixed and predetermined. The issue however of EAD is particularly relevant for loans commitments; the reason being that a distressed borrower is likely to use a substantial part of initially undrawn loan commitments before defaulting, unless there is a chance that the bank is able to anticipate the problem and therefore could revoke the commitment (Saita, 2007:93). This problem is specifically more relevant for high-quality borrowers, seeing that they are able to obtain larger commitments, and also, the difference between the drawn portion in normal conditions and at default, may be larger (Saita, 2007:93).

As a consequence, therefore, Basel II are forcing banks to adopt either the standardised or the foundation IRB approach to translate their off-balance sheet items – such as loan commitments – into credit exposure equivalents by multiplying them by a credit conversion factor (CCF) (Saita, 2007:93).

CCFs serve to address exposures that are commitments, and not cash exposures (Bessis, 2010:236). By considering both on- and off-balance sheet positions, it is required that all exposures be measured gross of specific provisions or partial write-offs. Further, the EAD on drawn amounts should not be less than the sum of the amount by which a bank's regulatory capital would be reduced if the exposure were written off in full, and any specific provisions and/or partial write-offs (BIS, 2006a:73).

Considering the above, when the difference between the instrument's EAD and the sum of the two components (the amount by which a bank's regulatory capital would be reduced if the exposure were written off in full, and any specific provisions and/or partial write-offs) is positive, the amount is termed a discount (BIS, 2006a:73).

A summary of the foundation and advanced approaches

The AIRB approach is intended for banking organisations that meet more rigorous supervisory standards, as more of the risk components mentioned above are to be estimated by the bank internally (BIS, 2001a:2). This approach requires banks to provide their own estimates of PD, LGD and EAD, as well as their own calculation of maturity (M); this is subject to meeting minimum standards (BIS, 2006a:59). The full collection of approaches will now be summarised briefly.

Corporate, sovereign, and bank exposures. The foundation approach requires that banks supply their own estimates of PD as associated with each of the borrower grades; the supervisory estimates for the rest of the relevant risk components (i.e. LGD, EAD and M) should however be utilised (BIS, 2006a:60).

Under the advanced approach, banks are required to calculate the effective maturity, or M, while providing their own estimates of PD, LGD and EAD (BIS, 2006a:60).

The specialised lending categories. In the event that banks do not meet the requirements for estimating a PD under the corporate foundation approach for their specialised lending exposures, these banks are required to map their internal risk grades to five supervisory categories. Each of these categories is associated with a specific risk weight. The BCBS (BIS, 2006a:60) terms this version the “supervisory slotting criteria approach”.

It is further stipulated that banks that do not meet the requirements for estimating the PDs of their exposures, are able to utilise the foundation approach to corporate exposures in order to obtain risk weights for all classes of specialised lending, except for HVCRE. Banks that do meet the requirements for estimating PDs, LGDs and EADs may use the advanced approach to corporate exposures for deriving risk weights for all classes of specialised lending, except HVCRE (BIS, 2006a:60).

Retail exposures. Banks are responsible for providing their own estimates of PD, LGD and EAD for all retail exposures. There is no distinction between the foundation and advanced approach under the retail asset class (BIS, 2006a:60).

Equity exposures. For equity exposures not held in the trading book, there are two general approaches for calculating RWA. The first approach is the PD/LGD approach, which remains available for banks adopting the advanced approach for the other exposures types. The other approach is the market-based approach (BIS, 2006a:60). Under the market-based approach, a financial institution can calculate the minimum capital requirement for the equity holdings of the banking book by utilising either one, or both, of two different methods, namely the simple risk weight method, or the internal models method (BIS, 2006a:79).

According to the regulations, the simple risk-weight method requires that a 300% risk weight be applied to equity holdings that are publicly traded, that is, any equity that is security traded on a recognised security exchange. A 400% risk weight should be applied to all other equity holdings (BIS, 2006a:79).

The internal models method is where an IRB bank may, or is required by the supervisory, to use internal risk measurement models for the calculation of risk-based capital requirements (BIS, 2006a:79).

Eligible purchased receivables. Under the Basel II Framework, the treatment of eligible purchased receivables overlaps two asset classes. For eligible corporate receivables, banks may utilise both a foundation and advanced approach, subject to certain operational requirements being met. For eligible retail receivables – similarly to the retail asset class – no distinction is made between the foundation and advanced approach (BIS, 2006a:61).

2.8.1.5. Risk-weight functions

The three risk components, as set out above, are converted into actual risk weights by the use of a risk-weight function. These risk weights are used to calculate RWA. Risk weights are a function of PD and LGD (Bessis, 2010:45). The risk weights, as defined for the IRB approach are defined as a single continuous function of the PD, LGD and in certain instances, M, of an exposure. A mechanism is provided by this function whereby the risk components mentioned above are converted into the actual regulatory risk weights (BIS, 2001a:19). The IRB approach is based on measures of unexpected losses and expected losses. The risk-weight functions produce capital requirements for the unexpected losses portion (BIS, 2006a:52).

2.8.1.6. Minimum requirements

In order for a bank to be entitled to apply the IRB approach, it is required to meet a full set of minimum requirements. These requirements are to be met not only at the outset or beginning of application, but also on an on-going basis (BIS, 2001a:20). These serve as evidence, inter alia, to the evaluation and quantification of the inputs utilised, and also to the heftiness of the banks' internal rating system and in general, the credit risk management process (BIS, 2001b:7).

A significant challenge arises here given the varying approaches that might be followed for assigning ratings and estimating loss characteristics; also, inherent in measuring these characteristics, there is a degree of imprecision. Therefore, bank and supervisory practices for validation are vital to the successful implementation of the IRB approach (BIS, 2001b:8).

As stated above, the BCBS recognised the vital role that supervisory practices will have for validation purposes, and therefore also for the successful implementation of the IRB approach in financial institutions. In addition, it was noted that market discipline will play a key part in this respect and therefore, the disclosure requirements, as set out as part of Pillar 3 requirements, are attached to the use of the IRB approach (BIS, 2001b:8).⁶

In summary, the disclosure requirements, as set out in the Pillar 3 requirements, allow market participants the assessment of key pieces of information on the risk exposures and capital, assessment and management processes, and most importantly, capital adequacy of financial institutions under the IRB approach (BIS, 2001b:8).

2.9. Conclusion

This chapter's aim was to provide more insight and background into the definition of capital. This is of importance as the purpose of this study is to explore the various approaches that are followed for

⁶ See discussion on Pillar 3 in section 2.5.1.3 that covers Pillar 2 on Market Discipline.

the classification of operational risk losses relating to credit risk. Furthermore, improper risk classifications and subsequent improper regulatory treatment of losses, can lead to significant capital implications for a financial institution. Capital and a proper definition thereof, therefore, are important considerations, and foundational to this study.

The main purpose of capital is for the absorption of financial risks. Creditor protection is a first priority when it comes to the role of capital. Capital serves as a buffer against future, unidentified losses and in the process, depositors are protected against any significant risks.

In terms of credit risk in particular, the BCBS prescribes two approaches that can be used for measurement purposes. These two approaches are TSA, and the IRB approach, which consists of the foundation and the advanced approach. The IRB approaches are intended for banks that meet more rigorous reporting standards. Capital calculation can be summarised starting from the asset class, differing according to the broad approaches. In TSA, the risk weights are supervisory, depending on the applicable risk weightings as described in the sections above. In the IRB approach risk-weight functions depend on all the credit risk components, and also differ by asset class. Banks have the flexibility of using their own estimates under the advanced approach for both the inputs of the risk-weight functions, and for credit risk mitigation (Bessis, 2010:244).

Chapter 2 laid the groundwork for the background on capital, and the importance thereof. The history of the BCBS is also an important aspect, as there are regulatory requirements from the BCBS in terms of capital measurement for credit risk and operational risk, and for boundary events specifically. In addition, the background and information on credit risk in this chapter are of importance as the focus of this study is specifically in terms of operational risk losses relating to credit risk. Chapter 3 follows the same approach as Chapter 2 in that operational risk is explained in terms of the regulatory requirements and the measurement approaches that exist for the operational risk type.

Chapter 3

The Basel II Approach to Operational Risk

3.1. Introduction

“When anyone asks how I can best describe my experience in nearly 40 years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like, but in all my experience, I have never been in any accident of any sort worth speaking about... I never saw a wreck and never have been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort – E.J. Smith”. (Ostrowski, 1997)

Subsequent to commanding passenger ships for 26 years, and having logged about two million sea miles, Edward John Smith had a fairly good idea what it was that comforted passengers. As such, Smith was considered highly experienced, capable and therefore enjoyed the extraordinary reputation as the “Millionaire’s Captain”. Today, no significant importance would be attached to what he said, had he not been the captain on the maiden voyage of the Titanic, which had been widely acclaimed as “practically unsinkable” until it went down after hitting the iceberg and taking 1 500 lives – including that of the captain (Buchelt & Unteregger, 2004:86). To this very day there have been great debates on why the Titanic sank. It seems as if a chain of inadequacies and errors were the cause, and this is also often the case in all catastrophes of this dimension. Firstly, the myth that the Titanic was unsinkable caused the captain to navigate too carelessly and too fast through the iceberg waters. There were also some inadequate safety measures, such as a shortage of lifeboats. Poor drills and emergency planning, as well as a lack of discipline, led to many lifeboats not being lowered to the water fast enough. In addition, some lifeboats were half empty, as some passengers just refused to get in (Buchelt & Unteregger (2004:86).

It can therefore be concluded that the entire accident appears to have been the outcome of the failure of a few interrelated factors: people (the crew as well as the passengers), systems (the ship, together with its equipment) and processes (emergency procedures), being triggered by an external event, namely the iceberg (Buchelt & Unteregger, 2004:86).

The factors responsible for the Titanic accident are very similar to the classical causes of what constitutes operational risk – people, systems, processes and external events. At the end of that historic night, the ship lay at the bottom of the Atlantic Ocean. This seemed like a punishment for the condescension of its engineers and operators, reducing it to the bitterly learned lesson that not to know one’s risks – or blatantly refusing to see them – does not necessarily suggest that there are no risks (Buchelt & Unteregger, 2004:86). Of importance is that banks are not unsinkable either. The comparison of typical banking risks with those of maritime navigation is unconvincing only at first sight (Buchelt & Unteregger, 2004:86).

The fact remains that the meaning of operational risk is a lot closer to the original meaning of risk – which is derived from the Spanish *risco* or Italian *rischio*, which means “a cliff” – than for the other risks within the banking business. Operational risk cannot be ignored, as it can generally be stated that for most banks, it may be much greater than market risk and it can constitute the second-largest risk category after credit risk (Buchelt & Unteregger, 2004:87).

This chapter focuses on operational risk, its definitions as well as the capital requirements of operational risk. In addition, a two-step approach is discussed for a bank to construct an operational risk framework; this also assists in providing a simplified view of an operational risk framework in a financial institution.

3.2. Operational risk – An evolution of definitions

Operational risk is one of the oldest risks within the financial and banking sector; yet the BCBS has only recently⁷ seriously worked on a regulatory framework for managing this risk type. Only since this time has operational risk been seen and perceived as an important theme for banks and financial institutions.

Various definitions of operational risk have passed and progressed through numerous iterations since the widespread discussions began on this topic (Hoffman, 2002:34). A high-level coverage of the thought process – since the inception of the term – will be discussed in this section.

A vital part of the evolution process of the operational risk definition includes an operational risk management strategy that was initiated in about 1990 by asking a simple question. What specific risks were not being addressed by the market risk and credit risk management models of the time? In addressing this question, an identification of the risks associated with key resources of a firm was reached: relationships, people, technology/processing, physical assets, and other external sources. This process was highly instructive in that it provides a complete understanding of the importance of the thought process for any financial organisation in developing its own definitions and classes of risks (Hoffman, 2002:35).

One of the first official definitions of operational risk was anything that is not credit or market-related (Hoffman, 2002:35). Understandably, this approach has been widely criticised but served as a practical starting point at the time (Hoffman, 2002:35). The process, as explained at that time, was straightforward in that information on any loss that was not market-related or credit-related was gathered. Market-related events can include, for example, events caused by movements in asset prices, where credit-related events can be caused by a client not being able to meet payment obligations. In this way, a variety of both industry and proprietary losses were captured and could be categorised (Hoffman, 2002:35).

⁷ Since the 1990s, the BCBS has worked on a regulatory framework for managing operational risk.

Following some trial and error during this process of pattern identification and inclusive definitions, a definition was arrived at that spanned several risk classes. This definition stated that operational risk is the risk of loss that might arise from disruptions in business, control failures, misdeeds, errors or any events of an external nature (Hoffman, 2002:35)

Operational risk can manifest itself in five key risk classes. At the time these five key risk classes were decided on, the regulatory developments for operational risk were not yet universally accepted, and still very fluid. These five classes were selected as they represent accountability and responsibility, not only on a firm wide basis but also within individual business lines and/or profit centres. The principle that ensures that categories are Mutually Exclusive and Collectively Exhaustive – or the “MECE” Principle – can be applied. The five primary operational risk or exposure classes are defined as people risks, relationship risks, technology and processing risks, physical risks and other external risks (Hoffman, 2002:36).

People risks can be defined as the risk of loss caused either intentionally or unintentionally by an employee. An example might include an employee error or employee misdeed. Also, the risk of loss caused intentionally or unintentionally merely involving employees, such as for example in the area of employment disputes.

The next primary operational risk type, namely relationship risk, includes non-proprietary losses to a firm, generated through the relationship or contact that a firm has with its clients, regulators, third parties, or shareholders. Examples include penalties paid, reimbursements to clients, etc.

Thirdly, technology and processing risks are the risks of loss by failure, breakdown, or any other disruption in processing, systems and/or technology. Also included are for example the loss from piracy or theft of information or data, and loss from technology that fails to meet the intended business needs.

The next risk type, namely physical risks, can be defined as the risk of loss through any damage to properties or loss to physical property or assets for which the firm is responsible. Finally, other external risks include risks of loss caused by any actions of external parties. For example, the perpetration of fraud on the firm or, in the case of regulators, the promulgation of change that would make a change to the firm’s ability to continue doing business in certain markets.

The five risk classes for operational risk as discussed above, are merely the thought processes followed for one bank, as set out in Hoffman (2002:36). Various processes were followed and papers have been written by the BCBS. It is not the intention of this study to go into the detail thereof, but rather to focus on the definition that the BCBS (2006a:144) has finally arrived at:

“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.”

3.3. Operational risk capital – Expected and unexpected losses

Prior to starting with a discussion on operational risk capital, it is appropriate to set out a definition of operational risk capital. This is important as different definitions are sometimes used in practice. A definition for operational risk capital that is utilised by some is that it is the sum of expected and unexpected operational losses. Another definition utilised is that operational risk capital is for unexpected operational losses only. Finally, some see operational risk capital as unexpected operational loss considering only losses over a certain threshold (Saita, 2007:125).

With regards to expected losses and unexpected losses, the BCBS explicitly states that – unless a bank can demonstrate to the supervisor that it adequately captures expected losses as part of its internal business practices – it will be required that a bank has to calculate its regulatory capital requirement as the sum of unexpected loss and expected loss. The regulatory requirement is that a bank should be able to demonstrate sufficiently that its expected loss exposures have been accounted for, and only in this instance, will it be allowed to base the minimum regulatory capital requirement only on unexpected losses (BIS, 2006a:151).

Several issues have been raised with regards to the measurement and treatment of expected losses for operational risk purposes. The BCBS sets out some possible reasons for complications in expected loss calculations (BIS, 2005:1). Basel II puts forth the Basic Indicator Approach (BIA), TSA and the AMA as approaches that banks can follow for calculating regulatory capital for operational risk. Basel II also allows great flexibility for financial institutions that implement the AMA. For this reason, financial institutions have developed a wide variety of different methods to determine operational risk capital. In the process, varying emphasis has been placed on the expected loss calculations relative to total capital. Secondly, the ability of financial institutions to establish account reserves for expected future operational risk losses is extremely limited throughout various jurisdictions. Finally, because many financial institutions have only collected historical operational risk losses exceeding a specific threshold, data issues are a potential problem. Additionally, most financial institutions’ datasets are mostly based on relatively short time series, with very few high severity losses incorporated.⁸ Where these exist, such losses can have a dominating effect on institutions’ historical loss experience. The culmination of these issues may cause complications for the calculation of expected loss (BIS, 2005:1).

⁸ Most financial institutions’ datasets mostly comprise of high frequency loss events.

The BCBS has provided banks with guidelines and principles that will facilitate consistent implementation of this requirement that is stipulated for the treatment of expected losses and unexpected losses for operational risk. For expected losses in operational risk to be measured to the satisfaction of national supervisors, the institution's measure of expected loss must be consistent with the "expected loss plus unexpected loss" capital charge calculated using the AMA model approved by the supervisors. For operational risk expected loss to be "accounted for" to the satisfaction of national supervisors by means other than holding capital or establishing provisions, a bank should be able to demonstrate that the corresponding losses are highly predictable and reasonably stable. Also, the estimation process should be consistent over time (BIS, 2005:1).

The next principle provided by the BCBS is that the maximum offset for operational risk expected loss is to be bounded by the expected loss exposure calculated by the bank's AMA model, as approved by the supervisor (BIS, 2005:1).

Thirdly, the principle is set that allowable offsets for operational risk expected loss must be clear capital substitutes. Otherwise, it should be available to cover expected loss with a high degree of certainty over a one-year time period (BIS, 2005:2). Finally, per Basel II requirements, the banks should clearly document how their operational risk-expected loss is measured and accounted for (BIS, 2005:2).

3.4. Basel II Operational Risk Measurement Approaches

Operational risk is defined as adverse deviations of the performance of a firm due to how the firm is operated, instead of how the firm is financed (King, 2001:7). However, subsequent to inclusion of operational risk in the Basel II framework, the BCBS defined operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (BIS, 2006a:144). It is thus clear that the BCBS supplied this regulatory definition of operational risk, and as with credit risk, three different approaches are defined for minimum regulatory capital for operational risk. These approaches, in a continuum of increasing sophistication, are (BIS, 2003:120): The BIA; TSA and the AMA. Each of these approaches will be discussed in the sections that follow.

3.4.1. BIA

In the BIA, gross income serves as a proxy for the measurement of operational risk exposure of a bank (BIS, 2006a:217). Banks utilising the BIA should hold capital for their operational risk equal to the average across the previous three years of a fixed percentage of their positive annual gross income (BIS, 2006a:144). Gross income in this case is defined as net interest income plus net non-interest income (BIS, 2006a:144). This measure should be gross of any provisions and/or operating costs, it should rule out realised profits/losses from the sale of securities in the banking book, and finally, it

should exclude unexpected or irregular items (Cosma *et al.*, 2009:315). The charge is expressed as follows (BIS, 2006a: 144):

$$K_{BIA} = [\sum(GI_{1,...,n} \times \alpha)] / n, \quad (3.1)$$

where:

- K_{BIA} = the capital charge under the BIA;
- GI = annual gross income - where positive - over the previous three years;
- N = number of the previous three years for which gross income is positive; and
- = 15%, as set by the Committee, and relates to the industry wide level of required capital to the industry wide level of the indicator.

3.4.2. Standardised Approach

TSA is the second approach to operational risk capital measurement that is proposed by the BCBS. TSA is often seen as the approach that best reflects the real level of risk that a complex organisation with a variety of business activities faces; at the same time, it does not require using complex and sometimes controversial mathematical models (Gallati, 2003:332). TSA builds on the BIA, and divides banks' activities into eight broad business lines, namely corporate finance, trading and sales, retail banking, commercial banking, payments and settlements, agency services, asset management, and finally, retail brokerage (BIS, 2006a:146).

Within each of the above business lines, the operational risk capital charge is calculated by multiplying an indicator of operational risk by a fixed percentage, or a "beta factor". The beta factor serves as an estimated proxy for the relationship between the industry's operational risk loss experience for the respective business line, and the broad financial indicator that represents the financial institution's activity within that specific business line, calibrated to a desired supervisory soundness standard (BIS, 2001c:7). The beta factor and the indicator may differ across the business lines (BIS, 2001a:28).

Within each business line, gross income is the broad indicator that serves as proxy for the scale of business operations, and therefore also the likely scale of operational risk exposures within each of the business lines (BIS, 2006a:146).

In order to arrive at the total capital charge for operational risk, the sum of the regulatory capital charges across the above business lines is calculated (BIS, 2001a:28). The associated capital charge for each business unit is defined by the level of certain indicators. Firstly, bank activities are split up into standardised units, as set out above. Then, the relevant supervisor specifies an exposure indicator for each respective business unit. The bank is responsible for the provision of the indicator data, for

example, the gross revenue. An opportunity exists to migrate towards increasingly more advanced approaches on a business unit basis (Gallati, 2003: 332).

In terms of the actual total capital charge calculation for operational risk, the BCBS stipulates that it should be calculated as the three-year average of the simple summation of the regulatory capital charges across each of the above business lines for each year. It holds that negative capital charges might result from negative gross income, and therefore, the negative capital charges in any business line for a given year may offset positive capital charges without limit. In instances where the aggregate capital charge across all the business lines for a given year is negative, the input to the numerator will be zero for that year (BIS, 2006a:147). The BCBS (BIS, 2006a:147) expresses the total capital charge as:

$$K_{TSA} = \{ \sum_{years 1-3} \max [\sum (GI_{1-8} \times \beta_{1-8}), 0] \} / 3, \quad (3.2)$$

where

K_{TSA} = the capital charge per TSA;

GI_{1-8} = the annual gross income for a given year for each of the eight business lines; and

β_{1-8} = a fixed percentage as set by the Committee that relates the level of required capital to the level of the gross income for each of the above eight business lines. This is also referred to as the *beta*.

Based on data from a sample of 23 internationally active banks, the Committee has estimated the preliminary beta factors (BIS, 2001c:22). The values of the betas, as set by the BCBS in the “International Convergence of Capital Measurement and Capital Standards” (BIS, 2006a:147) are made available for participating institutions.

TSA, as described above, is a better measure than the one-size-fits-all approach that is based on gross revenue (Gallati, 2003:333). Banks applying TSA to calculating the required regulatory capital for their operational risks will not have to go through the arduous and complicated exercise of collecting and assessing internal loss data required under the third and most advanced, sophisticated approach; these banks will, however, have good reason to start considering their business lines’ operational risks and how they might optimise the risk management thereof (Gallati, 2003:334).

An important feature of this approach is that it serves as basis for banks to move, on a business unit by business unit basis, towards the more advanced approaches; this will assist in encouraging the development of more advanced risk management within banks (BIS, 2001c:8).

There is, however, a shortcoming in the utilisation of the BIA and Standardised Approach as described above. An assumption is made that operational risk is linear and therefore directly in relation to the size of the business line or institution. A concern with regards to the third method – the AMA – is that it suggests a fixed relationship between unexpected losses and expected loss; there is a view that such a relationship does not exist (Gallati, 2003:334). The AMA will be discussed in the following section.

3.4.3. Advanced Measurement Approaches

The AMA is aimed at individual banks that meet more demanding supervisory standards. The regulatory capital requirement under the AMA is equal to the risk measure produced from the bank's internal operational risk measurement system. Various qualitative and quantitative criteria for the AMA are to be met by banks in order to comply with AMA (BIS, 2006a:147); these criteria are to be discussed in the sections that follow.

Under the AMA, operational data are divided into eight business lines, and seven event type classes. Ultimately, the AMA technique selected by a bank should utilise a matrix of eight business lines and seven event types (Rippel & Teply, 2008:6). Hereby, it is required that all the activities in the bank be mapped into the eight level 1 business lines, in a mutually exclusive and jointly exhaustive manner. The business lines, on the first level, include corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management and retail brokerage (BIS, 2006a:303).

The detailed loss event type classification required by the BCBS under the AMA is set out as follows:

Table 3.1: Loss-event type classification

Event-Type Category (Level 1)	Categories (Level 2)
Internal fraud	Unauthorised Activity
	Theft and Fraud
External fraud	Theft and Fraud
	Systems Security
Employment Practices and Workplace Safety	Employee Relations
	Safe Environment
	Diversity and Discrimination
Clients, Products and Business Practices	Suitability, Disclosure and Fiduciary
	Improper Business or Market Practices
	Product Flaws
	Selection, Sponsorship and Exposure
	Advisory Activities
Damage to Physical Assets	Disasters and other events
Business disruption and system failures	Systems
Execution, Delivery and Process Management	Transaction Capture, Execution and Maintenance
	Monitoring and Reporting
	Customer Intake and Documentation
	Customer/Client Account Management
	Trade Counterparties

Event-Type Category (Level 1)	Categories (Level 2)
	Vendors and Suppliers

Source: BIS (2006a:305)

Under the AMA, the regulatory capital requirement for operational risk will ultimately be equal to the risk measure generated by the bank's internal operational risk measurement system using the qualitative and quantitative criteria that were set out by the Basel II framework (Rippel & Teply, 2008:6). A bank wanting to utilise the AMA should obtain supervisory approval (BIS, 2006a:147). In addition, its internal measurement system should reasonably estimate unexpected losses by utilising a combination of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors. An allocation of economic capital for operational risk across business units should be supported; this should provide incentives to improve the management of business line operational risks (BIS, 2006a:150).

The bank's AMA is subjected to a period of initial monitoring by the respective supervisor before it can be applied for regulatory purposes (BIS, 2006a:15).

The subsections of the AMA, and also the various criteria that are to be met by banks wishing to adopt the AMA, are discussed below.

3.4.3.1. General criteria

Firstly, the board of directors and senior management of the financial institution should be dynamically and actively involved in the management and supervision of the framework of operational risk management (BIS, 2006a:149). Secondly, the financial institution should comprise of an operational risk management system that is implemented with integrity, and also operates in a manner that is conceptually sound. Finally, sufficient resources should be applied within the approach in the major business lines, and also in the control and audit areas (BIS, 2006a:149).

3.4.3.2. Qualitative standards

There are also qualitative standards that should be met by a bank in order to be permitted to use the AMA for operational risk capital.

Firstly, the bank should have an independent operational risk management function in place to design and implement the operational risk management framework of the institution. Secondly, the internal operational risk measurement system that the bank applies should form a central part of the bank's daily risk management processes. Thirdly, the management of the various business units, senior management and the board of directors should receive regular reports on the operational risk exposures and losses. Fourthly, not only should the financial institution's operational risk management system be well documented, but it should also have a routine in place that ensures compliance with the institution's documented internal policies, controls and procedures that pertain to

the operational risk management system. Finally, regular reviews and validations of the operational risk measurement system should be performed by internal and/or external auditors (BIS, 2006a:150).

3.4.3.3. Quantitative standards

The quantitative standards that are to be met include the AMA standard of soundness, detailed criteria, criteria on internal data, criteria on external data, criteria on scenario analysis and business environment and internal control factors (BIS, 2006a:151). Each of these criteria factors are discussed briefly in the sections that follow.

3.4.3.3.1. AMA standard of soundness

There exists no definite specification from the Basel II framework's perspective of the approach or distributional assumptions that should be applied to generate the operational risk measure for regulatory capital purposes. According to this standard, however, the bank should be able to demonstrate that the approach followed captures possible severe "tail" loss events (BIS, 2006a:151). A tail event refers to the type of events that occur less frequently, but are more extreme and severe in nature.

Regardless of the approach utilised by the bank, it should be able to demonstrate that the operational risk measure applied meets a standard of soundness that is comparable to that of the IRB approach for credit risk. For example, this should be comparable to a one-year holding period, with a 99.9th percentile confidence interval (BIS, 2006a:151). Banks are thus allowed to develop their own models (Rippel & Teply, 2008:6).

3.4.3.3.2. Detailed criteria

The bank will be required to determine regulatory capital requirements as the sum of the expected loss and unexpected loss, unless it is able to demonstrate that expected loss is being adequately captured in its internal business practices (BIS, 2006a:151). In order to capture the major drivers of operational risk that affect the actual shape of the tail of the loss estimates, the risk measurement system applied by the bank must be amply "granular" (BIS, 2006a:151).

In addition, for purposes of determining the regulatory minimum capital requirement, there should be risk measures in place for different operational risk estimates. Provided that the bank can demonstrate sufficiently to the national supervisor that its systems for determining correlations are sound, it is permitted to utilise internally determined correlations in operational risk losses across individual operational risk estimates. The systems used for determining correlations should take into account the uncertainty surrounding any such correlation estimates, particularly in periods of stress (BIS, 2006a:152).

Four elements to operational risk are designed to help a bank qualify for the AMA, and therefore, they make various uses of the four mandatory components, namely internal loss data, external loss data,

scenarios, and the business environment and control factors (KPMG, 2005:30). These elements are key features and crucial in a bank's operational risk measurement system (BIS, 2006a:152).

Internal data. As internal loss data is important for tying a bank's risk estimates to its loss experiences, the tracking of internal loss-event data is a fundamental precondition to the development and functioning of a credible operational risk measurement system. This is achieved in various ways, such as utilising internal loss data as the foundation of empirical risk estimates (BIS, 2006a:152).

The bank should have documented procedures for measuring the on-going relevance of historical operational risk loss data (BIS, 2006a:152). Internally generated operational risk measures used for regulatory capital purposes should be based on a minimum five-year observation period of internal loss data. This internal loss data might be used directly to build the loss measure or to validate it (BIS, 2006a:152).

In order for a bank to qualify for regulatory capital purposes, its internal loss-collection processes are to meet specific standards; the most important standards will now be briefly set out (BIS, 2006a: 152). Firstly, the bank should demonstrate its ability to map all historical internal loss data into the stipulated level-one supervisory categories. Secondly, the internal loss data utilised and captured by the bank should be fully comprehensive. Also, apart from information on gross loss amounts, the bank should keep information about the event date, recoveries of gross loss amounts, and some descriptive information about the driver and the causes of the loss event (BIS, 2006a:153).

Specifically important for the purposes of this research, it is required that operational risk losses that are related to credit risk and have historically been included in banks' credit risk databases, such as, for example, collateral management failures, will continue to be treated as credit risk for purposes of calculating minimum regulatory capital under the Basel II Framework. Such losses will therefore not be subject to the operational risk capital charge. For the purposes of internal operational risk management, however, banks are to identify all material operational risk losses consistent with the scope of the definition of operational risk, inclusive of those related to credit risk. It is further required that material operational risk-related credit risk losses be flagged separately within a bank's internal operational risk database (BIS, 2006a:153). Operational risk losses related to market risk should be treated as operational risk for the purposes of calculating minimum regulatory capital under the Basel II Framework. Such losses will therefore be subject to the operational risk capital charge (BIS, 2006a:153).

External data. The BCBS also stipulates requirements in terms of external data. Particularly in instances where there is sufficient reason to believe that a bank is exposed to infrequent but potentially severe losses, such a bank's operational risk-measurement system should make use of relevant external data. External data might be either public data and/or pooled industry data. Banks

should have systematic processes for determining the circumstances under which external data are to be used, and the methodologies applied to incorporate the data (BIS, 2006a:153).

Scenario analysis. Banks are to use scenario analysis of expert opinion together with external data in order to evaluate its exposure to high severity events. Such an approach typically draws on the knowledge of experienced business managers and risk management experts for the derivation of reasoned assessments of severe losses (BIS, 2006a:154). It is also required that the expert assessments should be validated and re-assessed over time by means of comparison to actual loss experience, in order to ensure their reasonableness (BIS, 2006a:154).

Business environment and internal control factors. The BCBS also stipulates requirements in terms of key business environment and internal control factors. Key business environment and internal control factors that might be responsible for changing a bank's operational risk profile should be adequately captured in the bank's firm-side risk assessment methodology (BIS, 2006a:154). Such factors will typically make a bank's risk assessments more forward-looking and more directly reflect the quality of the bank's control and operating environments. In addition, business environment and internal control factors will also assist in the process of aligning capital assessments with risk management objectives (BIS, 2006a:154).

3.5. AMA Capital Calculation under Basel II

The BCBS prescribes several requirements with which banks must comply in order to adopt the AMA. It is therefore also advised that large international banks adopt the AMA and quickly adapt their quantitative data collection, theoretical modelling of risk exposure and statistical validation. This is to allow for the use of a proprietary model (Chapelle *et al.*, 2006:2).

A two-step approach is proposed for a bank to construct an operational risk framework. The first step – Phase I – consists of developing and laying a foundation for the future use of AMA. The actual modelling of losses – Phase II – is conducted when the bank comprises of adequate strategies in all other areas, especially in the area of data history, which would allow for operational risk modelling (KPMG, 2009:1). Phase I and Phase II will now be discussed.

3.5.1. Phase I: Building a basis for AMA

The first phase for adapting the AMA consists of the development of a foundation for the future use of AMA. Therefore, the first Phase for building an operational risk framework consists of an analysis of all elements currently utilised in the operational risk approach. The elements to be analysed are shown in Figure 3.1.



Source: KPMG (2009)

Figure 3.1: The basis for AMA.

These analyses include verification of the compliance with and fulfilment of the minimum regulatory requirements with regards to the use of advanced methods and benchmark, for purposes of also fulfilling best practices (KPMG, 2009:1). The final product of a typical Phase I implementation will consist of various approaches, which are discussed in the following sections.

3.5.1.1. Operational risk strategy

The first element for analysis is the *operational risk strategy*. Hereby, a clear definition of operational risk should be included in an adequate operational risk strategy. The operational risk strategy should typically comprise of a “top-down” process for the allocation of capital. A requirement is also clear guidance for the “bottom-up” processes of risk identification, assessment, management, reporting and supervision (KPMG, 2009:1).

A top-down approach typically comprises performing mathematical modelling of the bank’s risk profile at a high level. In this case, all the loss data within the bank are assumed homogeneous in terms of truncation and the threshold levels; therefore the data will be modelled as one set of data. Once the modelling has been done at the top level of the hierarchy, the capital results will be allocated to the business units according to weighting factors (Peters & Terauds, 2007:17). A bottom-up approach models data and expert opinion at much lower levels of the hierarchy. This will entail that business units typically assess material risk types for their relevant business. Any loss data associated with this specific business unit and risk type are modelled at this level. An aggregation process is then performed, combining all the business unit risk type loss profiles to a bank level (Peters & Terauds, 2007:17).

In essence, this decision as to whether a top-down or bottom-up approach should be followed, has a significant influence on the types of models, and in particular, how data is used in such models (Peters & Terauds, 2007:17).

3.5.1.2. Organisational structure

The second element to be analysed as part of phase one is the *organisational structure* of the financial institution. It is true that operational risk has a much broader scope than credit and market risk. Therefore, it is vital that a transparent and effective definition of roles and responsibilities of units and individuals should exist, as this forms an essential part of the process of defining an effective operational risk structure (KPMG, 2009:1).

3.5.1.3. Reporting

The third element for analysis is *reporting*. It should be ensured that all the elements set out and forming part of the operational risk structure should also be embedded in the reporting processes and systems for operational risk. Reporting for operational risk should cover two distinct aspects. The first aspect is the *delivery of relevant and defined operational risk information to management and risk control*. The second aspect is the *reporting of information that is aggregated by risk category to business line management, the board, as well as the risk committee* (KPMG, 2005:24).

3.5.1.4. Definitions/structures/linkages

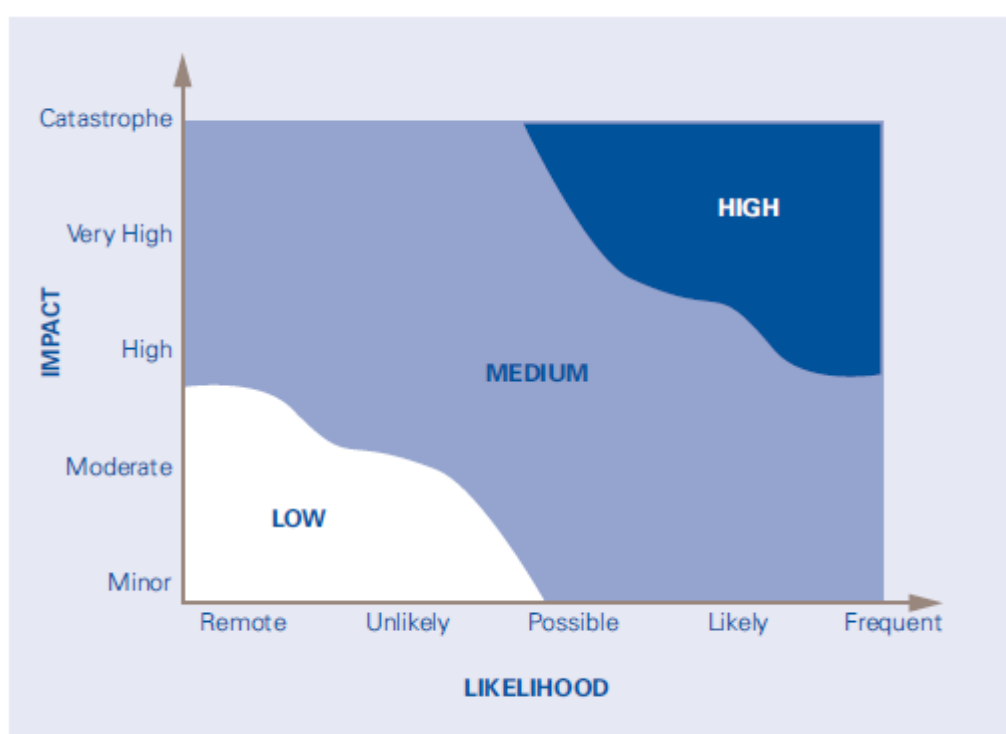
Definitions, structures and linkages should be analysed as part of phase one and in addition, clear definitions should be developed for all operational risks. These can include, for example, definitions of operational event types, definitions of operational loss types, as well as mapping to Basel event types and business lines (KPMG, 2009:2).

3.5.1.5. Risk self-assessment

Conducting regular *self-assessments* plays a key role in the risk-identification process for operational risks (KPMG, 2009:2). *Risk self-assessments* should therefore also be thoroughly analysed as part of the first phase for AMA implementation. A risk self-assessment is sometimes also referred to as a risk control self-assessment (RCSA), but a “risk assessment” should be defined separately from a “control self-assessment”. First of all, a risk-assessment interview is defined as a strategy that can range from simply asking a few easy questions to getting people thinking about the business, their risks, processes, and vulnerabilities, to the completion of some grids, to highly detailed business process and risk reviews (Hoffman, 2002:188). A control self-assessment can be defined as the process by which individual business units analyse their own business processes step by step to identify the weaknesses and strengths of their risk-control programs. Throughout the process, control gaps and risks are identified (Hoffman, 2002:193). Paragraph 676 of Basel II, also briefly stated in section 3.4.3.3.2,

generally specifies that a financial institution's firm-wide risk-assessment methodology should include the capture of key business environment and internal control factors, as these can change the operational risk profile (BIS, 2006a:154).

A typical RCSA programme will seek to embed a process in the operational risk framework of a bank by which risks and their controls are first of all identified, and then rated, in a consistent and structured manner within business. Risk assessment is a tool that assists in identification and, to a limited extent, even quantification of operational risk (KPMG, 2005:27). In addition, it picks up where loss data collection leaves off. Therefore, it also helps fill the knowledge gap left by backward-looking and often sparse loss data by attempting to establish risk-sensitive and forward-looking identification of operational risk. Figure 3.2 explains how the basic structure of a risk assessment is universal, being a set of matrices identifying and assessing operational risk with its subcomponents in terms of likelihood and impact of occurrence, based on a defined risk appetite (KPMG, 2005:27).



Source: KPMG (2005:27)

Figure 3.2: Operational risk-assessment structure.

The development of risk-assessment questionnaires and the choice of key respondents is therefore of importance for assuring a robust and effective risk-identification and mitigation system for operational risks (KPMG, 2009:2).

Ultimately, the benefits of an RCSA programme can be combined with a scenario-analysis process. Scenario analysis was briefly described in section 3.4.3.3.2. This will assist a bank in being able to quantify operational risk exposures.

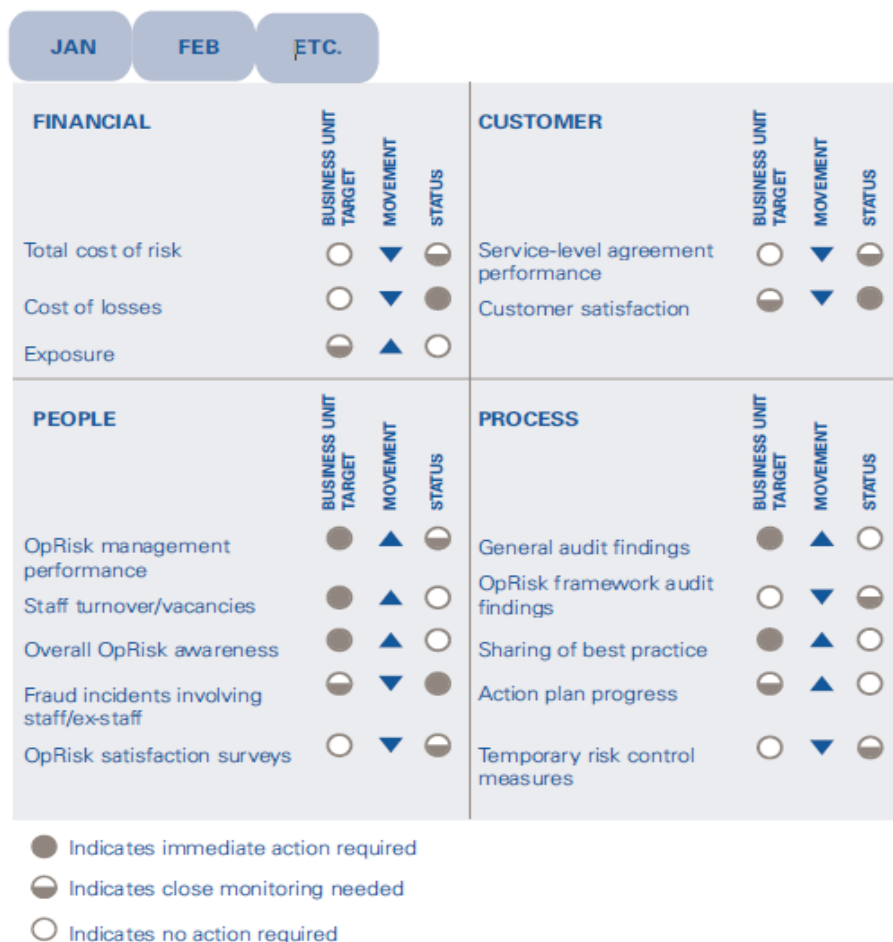
3.5.1.6. Internal loss data and external loss data

Analysis of the institution's *internal loss data* and *external loss data* also is key to a bank implementing AMA. Internal loss data is the best representation that a firm can use in profiling its own risk. A bank should have the support of all its areas for the collection of internal loss data. Loss events over a materiality threshold – including foregone income, indirect losses, and near misses – must be entered into a loss database and also be verified (KPMG, 2005:216).

The collection of data from internal databases within the bank allows for the identification, modelling, and budgeting for standard losses, and also therefore expected losses (KPMG, 2009:2). In certain instances, banks do not have enough large losses to give a reasonable representation of their large loss potential by using internal data alone (Hoffman, 2002:216). Events referred to as low-frequency/high-impact losses, such as natural disasters and IT system breakdowns are most of the time, by definition, not contained in an internal loss database purely because they may not yet have hit the bank. Consequently, data and information on such losses must essentially be derived from external sources (KPMG, 2005:26). In other words, it can be stated that external data compliments internal loss data where internal loss data might be limited, and therefore, external data are mostly used for representing unexpected operational losses.

3.5.1.7. Key risk indicators (KRIs)

KRIs can be seen as tools in providing an early warning mechanism (KPMG, 2009:2). KRIs should be analysed and considered as part of the first phase of AMA implementation. KRIs can also be seen as captured information that provides useful views of underlying risk profiles at various levels within an organisation (Hoffman, 2002:239). Figure 3.3 can be used to explain that a scorecard approach can assist a bank's operational risk division in the assessment of various risks and how they change over time (KPMG, 2005:28).



Source: KPMG (2005:28)

Figure 3.3: Scorecard approach for risk assessments.

Similar to loss data, KRIs are based on existing data. Unlike loss data, KRIs do not look at the “face value” of information – which is assuming that history may be repeated – but rather seek to predict certain future behaviour. An example hereof is staff turnover, not representing actual losses, but potential future losses should certain key employees and knowledge be lost (KPMG, 2005:29).

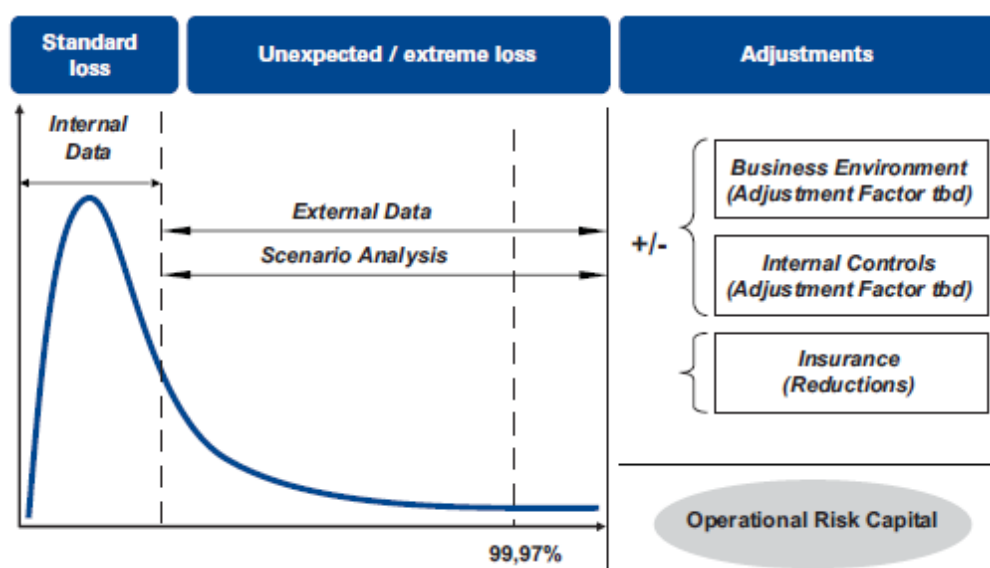
3.5.2. Phase II: Capital modelling

The actual modelling of losses is core to the AMA. Phase two is typically conducted when the bank has adequate strategies implemented in all other areas – especially in the data history area. This would allow for the second phase (operational risk modelling). Capital modelling for operational risk encompasses the calculation of regulatory and economic capital. It involves defining input data, which consists of internal and external loss data, scenario data, business environment, and control factors. These inputs assist in defining the mathematical and/or statistical relationships and assumptions for measuring operational risk. In addition, the inputs assist in the implementation of the model and the model validation (KPMG, 2005:30).

The goal of capital modelling for operational risk can be summarised by stating that it is to estimate expected losses, which should be taken into account in product pricing. In addition, it is used for calculating the Value-at-Risk (VaR) for operational risk (being the unexpected losses) that have to be buffered by economic and regulatory capital (KPMG, 2005:30). The AMA gives financial institutions the flexibility to build their own models, taking into account their own structure, correlation and diversification effects, insurance mitigation and other factors (KPMG, 2005:30).

Even though banks have developed common approaches to the quantification of credit and market risks over the past years, operational risk quantification tools are still at an early stage of development. It is also true that market consensus has not yet converged on a set of “best practice” approaches. However, over the few years that operational risk practices, management and quantification became more prominent and crucial in the banking industry, many banks tend to implement an approach based on a combination of loss data modelling and results of qualitative risk assessments (KPMG, 2009:2). An example of such a widely used approach consists of three components; these are set out in Figure 3.4.

Finally, adjustments can be applied to operational risk capital. Adjustments typically include changes in the business environment and the impact of internal controls (KPMG, 2009:2).



Source: KPMG (2009:2)

Figure 3.4: Modelling for operational risk.

Currently, three broad families of approaches for measuring operational risk required capital exist. The modelling of operational risk is not key to this study, but as these three approaches are considered preferred practice for any operational risk framework, background will be provided in the sections that follow. These include the loss distribution approach (LDA), the risk drivers and controls approach, and the scenario-based approach (KPMG, 2005:30).

3.5.2.1. The LDA

As mentioned in section 3.4.3, the Basel II Accord specifically mentions the LDA. The LDA is a statistical model, which is widely used in the insurance sector. The implementation of a compliant LDA model for operational risk does, however, involve many sensitive modelling choices. Generally, the LDA is an actuarial, bottom-up approach to computing regulatory capital (Chapelle *et al.*, 2006:2).

The BIA and SA methods for measuring operational risk are relatively straightforward as these methods merely determine the economic capital as percentage of gross revenues. As a consequence of this conceptual simplicity, these methods do not provide real insights into the drivers of operational risk; while in contrast, the LDA model lends itself to quantifying the impact of active operational risk management actions, making it the most popular methodology by far (Chapelle *et al.*, 2006:5). Following the LDA model might also bring about substantial capital reductions (Chapelle *et al.*, 2006:3).

The LDA is a parametric technique that separately estimates a frequency distribution for the occurrence of operational losses and a severity distribution for the economic impact of the individual losses. Both these distributions are subsequently combined through n -convolution of the severity distribution with itself, where n is a random variable that follows the frequency distribution (Chapelle *et al.*, 2006:5).

The fitting of frequency and severity distributions, as opposed to only fitting a single parametric annual loss distribution, forces the bank to make the mathematical choice of working with compound distributions (Peters & Terauds, 2007:18). Some key points relating to why it is important to model severity and frequency distributions separately can be highlighted. Growth typically needs to be accounted for in the process of forecasting the number of operational risk losses in future years. Therefore, the expected number of operational losses changes as the institution grows and expands. Through the scaling of the severity distribution, economic inflationary effects can be directly factored into the size of the losses. By directly changing severity distribution, factors such as the consequences of changed policy limits and excesses can be easily grasped and understood. Finally, transparency of changes in thresholds recorded for loss events, and the impact that this might have on the amount of losses, should be held in consideration (Peters & Terauds, 2007:19).

The output of the LDA methodology is a full characterisation of the distribution of annual operational losses of the bank. This distribution contains all the required, relevant information for the computation of the regulatory capital charge. Required information for the computation of the regulatory capital charge includes knowledge of the expected loss and of the 99.9th percentile of the distribution, together with necessary inputs for the assessment of the efficiency of the operational risk management (Chapelle *et al.*, 2006:6). This calculation requires four steps: 1) calculating the frequency

distribution; 2) calculating the severity distribution; 3) taking the Goodness of Fit⁹ (GOF) measurement; and 4) calculating the annual loss distribution. In order to provide the reader with some background on the calculation process, these steps will be discussed. Detail will not be provided on the technical statistical approaches, as this is not the purpose of this study. The purpose is to provide the reader with an overview of the approaches that are available for utilisation.

Step 1: The frequency distribution. The occurrence of operational loss events within a bank is modelled with the frequency distribution. By definition, such a distribution is discrete, and therefore, for short periods of time, the frequency of losses is often modelled either by a Poisson or by a (negative) binomial distribution (Chapelle *et al.*, 2006:6). The Poisson distribution is the most useful for fitting the frequency of operational loss events (Esterhuysen, 2006:193). As a general assumption, the Poisson distribution is used for frequency modelling, and except for the fact that this assumption is well supported by literature and research, the Poisson distribution is selected for frequency modelling mainly because it ensures consistency across all cells and segments, and it enables the integration of internal data and scenario models (Lubbe & Snyman, 2009:11).

Step 2: The severity distribution. In segments where light tail behaviour is observed, the Gamma, Beta, Chi-square, Exponential, Lognormal, Weibull, Normal, Inverse Gaussian and Rayleigh distributions are usually considered for severity modelling. Where heavy tail behaviour is observed, the Cauchy, Burr, F, Generalised Pareto, Log Gamma, Generalised Extreme Value, Pareto and t-Student distributions are tested for severity modelling (Lubbe & Snyman, 2009:10).

Classical distributions are unable to fit the entire range of operational risk loss observations in a realistic manner, and therefore, a distinction is made between ordinary – that is, high-frequency/low-impact – and extraordinary – that is, low-frequency/high-impact – losses (Chapelle *et al.*, 2006:6). Such losses originate from two different generating processes. The “ordinary distribution” includes all losses in a limited range, whereas the “extreme distribution” generates all the losses above a “cut-off threshold” (Chapelle *et al.*, 2006:6). The severity distribution is then defined as a mixture of the corresponding mutually exclusive distributions (Chapelle *et al.*, 2006:7).

The extreme value theory (EVT) is a branch of statistics focused on the study of extreme phenomena, that is, the rare events that are situated in the tail of a particular probability distribution (Rippel & Teply, 2008:10). These rare events are typically the low-frequency/high-impact losses referred to above. The EVT cuts loss data distribution into two parts – the body and the tail. The body is being modelled using a different method than the tail, and the EVT relies on a sufficiently large data sample. One way of selecting tail observations from a data sample is the Peak Over Threshold method (Rippel & Teply, 2008:10). This approach enables the simultaneous determination of the cut-off threshold and

⁹ Goodness of fit measures how well the data are modelled by the distribution (Heinrich, 2004).

the calibration of a distribution for extreme losses using all the observations above this threshold (Chapelle *et al.*, 2006:7).

It is, however, not the purpose of this study to analyse the technical statistical approaches to capital modelling, but merely to present on a high-level overview of the various approaches available for consideration.

Step 3: GOF measurement. Once a series of fits have been performed, various graphical or non-graphical GOF measures are utilised for evaluating the accuracy and appropriateness of each fit (Lubbe & Snyman, 2009:10). The purpose hereof is to avoid model risk, which is the risk of choosing a bad distribution for the LDA. A VaR that is underestimated will put into jeopardy the long-term ability of a financial institution to maintain a sufficient amount of capital reserves for its protection against catastrophic operational losses. A severely overestimated VaR will put a limit on the amount of funds available for investment (Rippel & Teply, 2008:12).

The most commonly used non-graphical tests include Kolmogorov-Smirnov, Anderson-Darling, Cramer von Mises, analysis of fit differences, Evaluation Quantile-Quantile (QQ), Chi-square tests and Mean Square error estimates (Lubbe & Snyman, 2009:10). The most commonly used visual test is the QQ-plot, which plots empirical data sample quantiles against the distribution's quantile that is being tested for fit.

Based on the various graphical and non-graphical GOF measures that can be applied, a decision can be made on the most suitable severity and frequency distribution for the data segment under consideration for a specific cell (Lubbe & Snyman, 2009:11).

Step 4: Aggregation of loss and frequency distribution – the annual loss distribution. The next step would be to fit the most suitable selected loss distribution and frequency distribution for each Basel II business line and Basel II event type.

Operational risk data are divided into the seven event type classes and the eight business lines as stipulated in the Basel II Framework. Therefore, a matrix of seven event types and eight business lines are utilised (Rippel & Teply, 2008:6). As mentioned throughout this section, the loss distribution model for operational risk is a combination of the frequency and severity distribution for a bank's operational risk loss events. This concept is presented in Figure 3.5.



Source: Compiled by the author

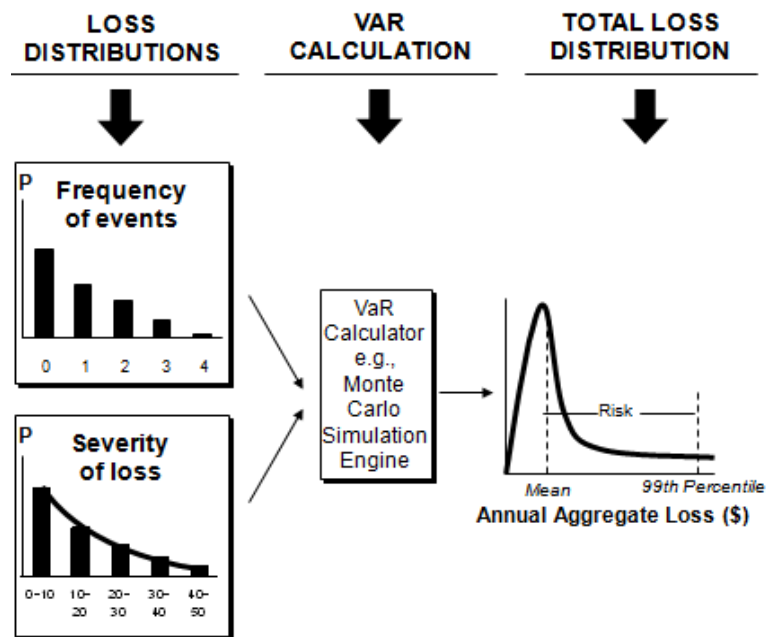
Figure 3.5: Combination of frequency and severity distribution for the LDA.

The aggregated loss distribution is obtained through a convolution of the frequency distribution and the severity distribution, and is calculated by means of a Monte Carlo simulation¹⁰, starting with a

¹⁰ A Monte Carlo simulation performs risk analysis by building models of possible results by substituting a range of values—a *probability distribution*—for any factor that has inherent uncertainty. It calculates results over and over, each time using a different set of random values from the probability functions. Depending on the number of uncertainties, a Monte Carlo simulation could involve thousands of recalculations before it is complete. The simulation produces distributions of possible outcome values (Palisade, 2012).

random extraction from the frequency distribution, and adding as many random extractions from the severity distribution as the value of frequency found (Esterhuysen, 2006:206). The result is an empirical dataset containing all possible annual combinations and permutations of loss or scenario realisations, and for each cell, this empirical distribution is incorporated into the model from a specified threshold (Lubbe & Snyman, 2009:12). The measure used for the estimation of the required capital charge is the VaR, and it is also stated that, in the context of operational risk, VaR is the total one-year amount of capital that would be sufficient to cover all unexpected losses with a high level of confidence such as 99.9% (Rippel & Teply, 2008:13).

The above process can further be described by recommending an algorithm which will now be briefly explained. First, a large number of Poisson random variables are simulated. For example, a sequence $n_1, n_2, \dots, n_{MC}$ is obtained representing scenarios of the total number of loss events in a one-year period. Second, for each of such scenarios n_k , simulate n_k number of loss amounts through the utilisation of a specified loss severity distribution. Third, for each such scenario n_k , the sum of the loss amounts obtained in the previous step above are taken in order to obtain cumulative one-year losses. Finally, Figure 3.6 illustrates that the sequence obtained in the last step is sorted in order to obtain the desired aggregate loss distribution (Rippel & Teply, 2008:14).

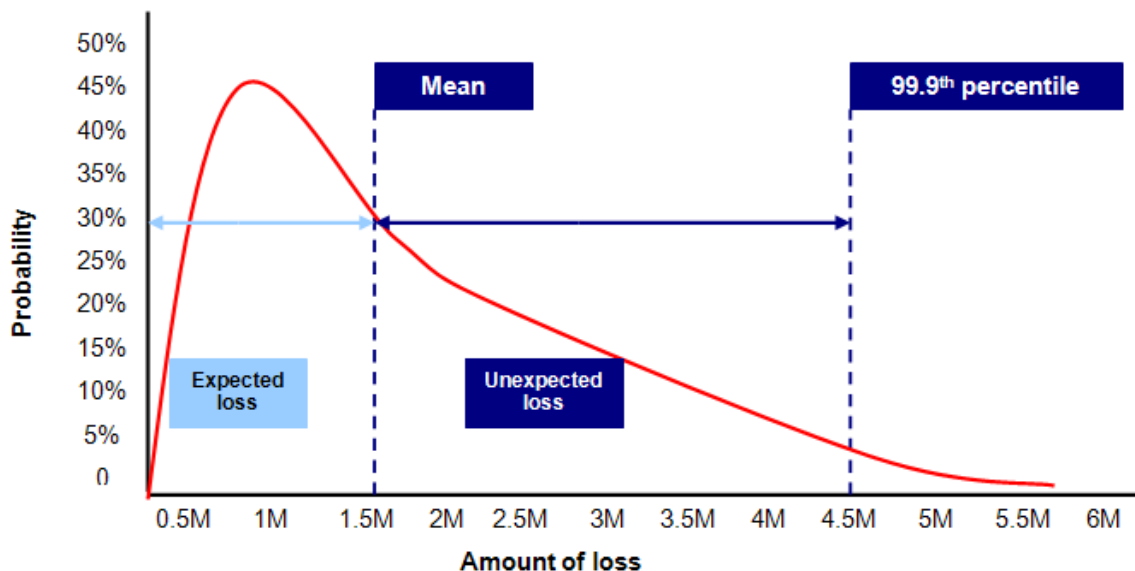


Source: Rippel & Teply (2008:14)

Figure 3.6: Total loss-distribution calculation.

The mean of the above density function is the average loss of the distribution. The 99.9th percentile is equal to 99.9% of the area under the distribution function. Keeping in mind that the total area under the distribution function is equal to 1, this will mean that the area from the 99.9th percentile to the y-axis is equal to 0.999 (Esterhuysen, 2006:208). To make this concept more understandable, it can be

stated that the 99.9th percentile means that 99.9% of all losses in the annual loss distribution are smaller than the 99.9th percentile. Using Figure 3.7 below as an example, it is clear that the 99.9th percentile is R4.5 million; therefore, 99.9% of the losses in this annual loss distribution are smaller than R4.5 million (Esterhuysen, 2006:208).



Source: Esterhuysen (2006:208)

Figure 3.7: An aggregated annual loss distribution.

As discussed earlier in this chapter, a bank's expected losses are the losses that the bank can expect to incur during the year. The BCBS advises that a bank should account for its expected losses in order to be allowed to base the minimum regulatory capital requirement on unexpected loss alone (BIS, 2006a:151). In Figure 3.7 above, the unexpected loss is the 99.9th percentile, excluding the expected loss, hereby meaning that the unexpected loss for the year is R3 million.

If provisions have been made for all of the expected losses, the VaR in Figure 3.7 above will be equal to R3 million. This is therefore the unexpected losses, and therefore, there is a 99.9% probability that the bank will not lose more than R3 million over the next year to operational risks. In the instance that no provision has been made for expected losses, the VaR will be equal to R4.5 million. In other words, a 99.9% probability exists that the bank will not lose more than R4.5 million expected or unexpected to operational risk over the next year (Esterhuysen, 2006:208).

3.6. Conclusion

This chapter laid a foundation for the study by providing a definition for operational risk. There was an evolution of definitions over time. The BCBS provided an official definition for this risk type, by stating it as the risk of loss due to inadequate or failed people, processes, systems, or due to external events.

A definition for operational risk capital that is often utilised is that it is the sum of expected and unexpected operational losses. With regards to regulatory capital for operational risk, the BCBS explicitly states that, unless a bank can demonstrate to the supervisor that it adequately captures expected losses as part of its internal business practices, it will be required that a bank has to calculate its regulatory capital requirement as the sum of unexpected losses and expected losses. In terms of economic capital for operational risk, some guidelines as provided by the BCBS have been highlighted – these will facilitate consistent implementation of the BCBS requirement in terms of the treatment of expected losses and unexpected losses for operational risk.

The various approaches set out by Basel II for the calculation of operational risk capital include the BIA, TSA and the AMA. There are general criteria, quantitative standards and qualitative standards set out by the BCBS that banks should adhere to, specifically for the implementation of the AMA. A proposed two-step approach can be followed for the construction of an operational risk framework under the AMA. Phase one consists of the development of a foundation for the future use of AMA, while phase two entails the actual modelling of the losses.

The information laid out in Chapter 3 is an important part of this study, as it provided the appropriate definitions of operational risk and operational risk capital. These are important elements to be considered before starting with the detail on boundary events in the next chapter. Together with the previous chapter that covered the measurement of credit risk, Chapter 3 completed the groundwork for the detailed discussions and explanations of operational risk losses that relate to credit risk. Chapter 4 builds on the foundation that was laid on bank capital, credit risk and operational risk. The definitions of credit risk and operational risk, as provided in Chapter 2 and Chapter 3 respectively, are utilised in Chapter 4 to arrive at a clear and proper starting point for the existence of a possible boundary event. In addition, the regulatory requirements of the BCBS in terms of credit risk and operational risk (as discussed in Chapter 2 and Chapter 3 respectively) serves as background to the regulatory requirement that the BCBS puts forth for operational risk losses related to credit risk. This will be discussed in more detail in Chapter 4.

Chapter 4

Credit Risk and Operational Risk – Boundary Events

4.1. Introduction

The global financial services sector experienced distressing times during the past four years. Operational risk is the broadest and most far-reaching type of risk that a financial institution can face, and from this perspective, 2008 was officially the worst on record. Numerous operational risk loss events took place during 2008, with credit, liquidity and market risk driving the severity of these events. An example hereof is \$7 billion unauthorised trading event at Société Generale that was uncovered in January 2008 (Cagan, 2009:2). This operational risk event included fraud that was originally undertaken prior to the global credit crisis; the state of the markets, however, escalated the severity (Cagan, 2009:2). There are countless examples of such events (Buchelt & Unteregger, 2004:87).

Operational risk is sometimes mistaken for credit risk, and specifically operational risk events are regularly identified as credit risk events. Credit risk is clearly at the heart of bank activity, and is most simply defined by the BIS as the potential that a bank borrower or counterparty will fail to meet his obligations in accordance with agreed terms. However, operational risk also plays an important role here (BIS, 2000:1).

The credit crisis has exposed weaknesses in risk management processes throughout the financial services industry. It also led to a critical look at the scope of the various risk types and the classification of loss events, and in turn the effects that incorrect risk classification might have on capital requirements (KPMG, 2009:2). In light of the significance of the issues surrounding boundary events and how the classification of these events can have a significant impact on the bank, it is important to first review operational risks that relate to credit risk.

The focus of this chapter is to guide the reader to a proper classification that can be utilised for more accurate categorisation of these risks and events. Operational risk as a separate risk type from credit risk is discussed. In addition, the view of the BCBS in terms of credit risk and operational risk boundary events is explained, together with all the comments, criticisms and concerns around the view of the BCBS. Thereafter, focus is placed on the factors that a financial institution can take into consideration when distinguishing between credit events, operational events and boundary events. These factors include a classification scheme or taxonomy of events, causal analysis, education of employees and staff and controls as mitigation techniques. These factors are then considered in the discussion of the “Bow-Tie” model of operational risk. Finally, this background information lays the foundation for the presentation of a decision tree that can be utilised for the classification of boundary events.

4.2. Boundary events – The current relevance of the issue

The objective of this section is to provide an overview of the current relevance of the issue of boundary events. These are highlights specifically pertaining to operational risk conferences that have been held recently, and attended by regulators and industry experts.

OpRisk Europe Conference – London, June 2010. At the *OpRisk Europe* conference held in London in June 2010 it was agreed that boundary events between credit risk and operational risk continues to be a significant source of concern for regulators and the general industry. It was also highlighted that boundary issues between credit risk and operational risk in the data from national contributors indicated that the amount of boundary events is highly significant compared with the overall pool of operational risk losses. Marcus Haas, banking and financial supervisor at Deutsche Bundesbank, stated that even though it was evident that legislators had no immediate intention of changing the defining line between risk events relating to operational risk and credit risk respectively, they will certainly be spending time on considering how to draw that line, more effectively, from an operational risk perspective (Tozer-Pennington, 2010).

Another point raised is that major operational risks are not condensed into the AMA framework, as these are related to credit risk (Tozer-Pennington, 2010). This can be viewed as a consequence of the boundary event identification and classification difficulties, specifically where some operational risk events are classified as credit risk losses and not indicated as boundary in the operational risk system for operational risk management purposes.

OpRisk North America Conference – New York, March 2010. At the March 2010 *OpRisk North America* conference, Mitsutoshi Adachi advised financial institutions to spend more time in studying intensely the approach to the classification of losses, in order to ensure that boundary events are accurately recorded (Tozer-Pennington, 2011). “*Although Basel II does not require such events to be accounted for in op risk regulatory capital, when a regulator suggests firms do something, it’s usually a good idea to do it*” (Tozer-Pennington, 2011).

OpRisk North America Conference – New York, March 2011. At the latest *OpRisk North America* conference, Adachi focused the attention on losses in the boundary areas. Studies indicated that boundary losses represent 30% of the total losses and 40% in terms of the value of losses. It was emphasised that financial institutions are to categorise these losses as accurately as possible, in order to ensure that capital levels are appropriate (Sands, 2011a).

Finally, even though operational risk losses that are related to credit risk, should be treated as credit risk losses for capital calculation purposes, it is of importance, especially for the purposes of firm-wide risk management, that financial institutions identify these material boundary event types of

losses, and utilise this data and information for the improvement of overall risk management in the institution (Sands, 2011a).

Now that it is clear that the issue of boundary events has led to intense and regular discussion during the past few years, more attention can be paid to the approach of classifying these events, and the factors that should be considered in the classification process. These points are discussed in the sections that follow.

4.3. Boundary events

Operational risk is commonly mistaken for credit risk, and specifically operational risk events are regularly identified as credit risk events. Although credit risk is considered the most prominent risk in the bank, there are numerous other risks and losses that can take place outside the direct relationship between the financial institution and the borrower. Examples of such risks and losses lie within the daily responsibilities of the people and employees responsible for dealing with the borrowers, or clients. The systems utilised within the institution, assisting with the lending business of the institution, can also carry their own risks and losses. It is therefore important to determine how an institution distinguishes between pure credit risks and losses, pure operational risks and losses, and boundary events. The first point of importance is that unique definitions for credit risk and operational risk should be established by the institutions. These risks should be viewed as separate risk types before the relation between the two risks can be defined and established.

4.3.1. Operational risk and credit risk as separate risk types

The growing complexity of the banking business promoted by the advent of information technology, and also the dependence thereon, growing globalisation and automation, new and changing business fields together with the emergence of increasingly complex products elevated the concept of operational risk (Buchelt & Unteregger, 2004:87). In addition, as the measurement of credit risk is becoming increasingly more sophisticated, the capital cushion that is used to soften the other risks is eroded. For this reason, the BCBS found it imperative and viable to create a separate view of operational risk (Buchelt & Unteregger, 2004:87). Since 1999, the BIS expressed the intention to introduce a new regulatory capital requirement for operational risk over and above market and credit risk (Saita, 2007:115).

Prior to discussing a new regulatory capital requirement for operational risk, the proper definition should be set out. Operational risk for any institution arises from the influence and interaction of internal and external factors and events on the people, processes and technology utilised in business processes within that institution. As institutions are generally distinctive in the way they combine people, processes and technology, it has always been complicated and for some impossible to create a

single generic definition of what constitutes operational risk (Gallati, 2003:290). There is, however, a common core operational risk definition as proposed by the BIS and as mentioned in Section 3.2: Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems, or from external events (BIS, 2006a:144).

Broadly speaking, operational risk can be defined as the risk of loss that results from an operational failure. It infuses the complete risk universe of a financial institution, and all aspects thereof; in other words, operational risk overlaps with – and exacerbates – all other types of risks, including credit risk. Based on the view that operational risk potentially contributes to the worsening of the other risk types, it can be concluded that, in the absence of operational risks and operational failure, all the other risks in a financial institution are of much less significance (Samad-Khan, 2008:26).

As discussed earlier in this study, credit risk can be defined as the potential that exists that a borrower of the bank or counterparty fails to meet his/her obligations according to the terms that were agreed between the two parties. Credit risk is inherent to any business of lending funds (Raghavan, 2003:842). Another definition of credit risk is that it is the risk of loss due to counterparty default, that is, a failure to meet a contractually pre-determined obligation (ORX, 2011:22). This definition is of significance, specifically within the issue of boundary events. Subsequently, it should be established whether the contractual relationship and obligation was legal in the sense that the relationship is based on the true identity and personal information of the client, and not that of a fraudulent applicant. In such a case, certain financial institutions might be of the view that such events or losses are due to operational risk. The Federal Deposit Insurance Corporation (2003) is of the view that the fraudulent use of credit cards or the fraudulent use of homeowner equity lines of credit via a check should be treated as operational risk losses, and not credit risk losses.

Operational risk may already exist within a bank even before credit risk. This point is illustrated in Figure 4.1 below.



Source: Adapted from Buchelt & Unteregger (2004:88)

Figure 4.1: Operational risk materialising directly or indirectly through credit risk/ market risk.

The view that operational risk should not be treated as a distinct risk type can become misleading from a management perspective. Critics objecting to the treatment of operational risk as a separate type of risk argue that major consequences will ultimately show up in the market or credit risk buckets (KPMG, 2005:11). However, as depicted in Table 4.1, these risks do have significant differences in almost every aspect. Subsequently, different responses from management are required. Overlooking key events and key aspects of losses, or misclassifying operational risks as credit risks can have some considerable and undesired consequences for banks (KPMG, 2005:11).

Table 4.1: Structural differences between credit risk, market risk and operational risk.

	Market	Credit	Operational
Inspection level	Trading desk/portfolio	Credit portfolio	Business line (can also include products, processes, portfolios and desks)
Risk categories	Interest/FX	Segments	Loss-event categories
Portfolio elements	Securities	Credits	Processes
Maximum total loss	Market value (excluding short sales/derivatives)	Credit volume	Bank's liquidation value
Maximum number of losses	Number of securities	Number of credits	Unlimited

Source: KPMG (2005:11)

4.3.2. Credit risk and operational risk – The boundary issue

Despite the distinction that exists between credit risk and operational risk, it might sometimes still appear difficult to distinguish among loss events that are attributed to the different risk types (Moosa, 2006:101). To complicate matters, operational risk is also frequently defined as any risk that is not categorised as market or credit risk, and is viewed as the risk of loss arising from a range of human or technical errors. It should therefore be recognised that this definition is not intended to include defaults, as defaults are to be covered in the scope of credit risks (Gallati, 2003:289). For this reason, the definition of operational risk distinguishes between direct and indirect impacts from operational risk causes. The impact might be observable and manifested in a credit risk event, resulting in a loss or a profit. Careless oversight of counterparty risks can, for example, lead to credit risk losses which at the same time, these losses could have been prevented by an appropriate internal control system, thus constituting operational risk (Gallati, 2003:291).

As far as the definition of an operational event is concerned, a bank could decide to adopt a stricter definition of operational risk; alternatively, appropriate definitions and guidelines should be instituted for other events or losses. One example is represented by credit losses deriving from operational errors, such as missing documentation that makes it impossible to take advantage of collateral in a case of default. Another relevant example might be human error in handling a loan-review process, resulting in missing the chance to take appropriate actions to reduce exposure with a borrower that will eventually default (Gallati, 2003: 291).

4.3.3. The view of the BCBS

When the banking industry was confronted with the issue of boundary events, the Basel Committee ruled that credit losses, which are driven by operational failure, should be treated as credit losses for purposes of capital adequacy (Samad-Khan, 2008:26). Such losses will, therefore, not be subject to any operational risk capital charges. However, for the purposes of internal operational risk management, banks are required to identify all material operational risk losses – this includes boundary events. Such material operational risks related to credit risk losses – or boundary events – should be flagged separately within a bank’s internal operational risk database (BIS, 2006a:153).

The Basel II Framework does not provide any further guidelines as to what constitutes such boundary events and as such, consistent guiding principles do not exist that banks can follow for accurately classifying and subsequently flagging such events.

This point further highlights the foundation and essence of this study. The potential exists that actual boundary events might be classified as purely credit risk, and correctly be included in the credit risk capital charge, but not be flagged separately within the bank’s internal operational risk database. Also, boundary events might be classified as operational risk and, therefore, be subject to the operational risk capital charge, instead of the credit risk capital charge. The latter misclassification might give rise to the potential for regulatory capital arbitrage¹¹. In any event, supervisors should be cognisant that capital requirements could encourage operational risk misclassification. The need is highlighted for banks to take a prudent approach to the identification and classification of operational risks within the credit risk environment. Attendant to this is an increasing need for proper guidelines in classifying credit risk and operational risk boundary events.

The BCBS’ view on boundary events is, however, not without its critics. This “compromise ruling” – being based on historical expedience and precedence – had the unintended effect of diminishing the overall importance of operational risk (Samad-Khan, 2008:26).

¹¹ Arbitrage can be defined as the practice of buying something in one place and selling it almost immediately in another place where it is worth more (Merriam-Webster, 2012).

Another point of significant criticism is that the focus of Basel II was mainly on capital measurement, instead of risk measurement for the purposes of management (Stein, 2010). A focus that was placed on the management side of operational risk would have forced the BCBS to distinguish between “control activities”, which include compliance activities, on the one hand, and “risk activities”. From the management perspective, operational risk has been captured by the control profession, and from the perspective of a control mentality, operational risk is viewed as a risk that has to be avoided. Not all operational risks are to be avoided; some operational risks should be accepted, this being consistent with the establishment of a risk tolerance, similar to other accepted risk tolerances (Stein, 2010). Specific details with regards to control activities for operational risk will be discussed in Section 4.4.4.

In further criticism of the view of the BCBS, Stein (2010) considers the ruling of Basel II being that if financial institutions used to define a loss as a credit risk, it should remain defined that way. Some examples can be utilised. Consider some banks lending money to Worldcom and Enron, based on fraudulent documents and financial statements. First, it is known that fraudulent activities are certainly included in the operational risk type. Therefore, an interesting question can be asked: *would it be reasonable to define the loss event by the mistaken existence of a credit line?* In addition, *would the inaccurate definition of the event type and loss categorisation improve the management of credit risk?* Also, *would the inaccurate definition of the event type and loss categorisation assist and contribute to the training of the risk-takers?* (Stein, 2010)

Returning to the example, the loss certainly appeared as a credit risk loss to the external auditors. Extending this view to the American Telephone and Telegraph Company (AT&T), one can also consider how the board of directors viewed this loss when they realised that they had participated in making AT&T competitive based on benchmarking to the Worldcom numbers. It certainly appeared as a credit risk loss in all these instances. Finally, from the perspective of regulators, internationally active banks, misled bankers and their regulators, however, this would definitely not have appeared as a credit risk loss (Stein, 2010).

As could be noted above, there are wide views, criticisms and concerns surrounding the view of the BCBS on boundary events. As the capital implication is still that certain losses pertaining to operational risk are included in the credit risk capital calculations, it is clear that correct classification is the first step in ensuring accurate capital inputs. This will, at least, ensure that losses pertaining to operational risk, and stemming from operational risks, are included, or flagged in the financial institution’s operational risk system, thus ensuring that these risks can be managed through the institution’s operational risk management framework.

The focus of this chapter is to guide the reader to a proper classification that can be utilised for more accurate categorisation of these risks and events.

4.4. Distinguishing between credit risk events, operational risk events and boundary events

Despite the distinction between operational risk and credit risk, it might sometimes still appear difficult to distinguish between loss events that are attributed to the different risk types (Moosa, 2006:101). Distinguishing operational loss events from credit and market loss events is not as difficult as it is always portrayed (Moosa, 2006:102).

The focus of the next section will be on the classification of loss events, and therefore also boundary events. As stated earlier, the consideration of causes and utilisation of classification frameworks and taxonomies are of importance. The “Bow-Tie” model of operational risk is explained as a valuable input into classification processes, and finally, a generic decision tree for the classification of boundary events is put forth.

4.4.1. ORX view on boundary events

ORX (2011:21) views credit risk as the risk of loss due to the default of a counterparty, and therefore, a counterparty’s failure to meet contractually pre-determined obligations. The requirements of ORX in terms of boundary events, is that all individual credit losses – that is, provisions or depreciations based on the member bank’s standards – above a certain threshold with an operational risk component within the credit risk regime, should be flagged as operational risk-driven credit risk. If this is not the case, then the loss is an outright operational risk loss (ORX, 2011:21).

ORX provides specific examples to serve as guidance to banks in terms of operational risks within credit that are to be included in reporting to ORX.¹² The examples set out by ORX are as follows (ORX, 2011:22):

- Collateral failure should be included in reporting to ORX. This is for instance where there existed failure to properly apply for loan insurance; also, failure to perform a public filing that is required to finalise a security interest in full. This also includes failure to monitor collateral and make timely and required collateral calls. ORX (2011:22) requires in such instances that only the lost collateral value is to be reported – this might be lower than the full default amount.
- ORX (2011:22) also uses procedural failures as an example. Processing errors might prevent recovery on a loan, or even enable a loss. An example hereof might be where a cash advance is made on a credit facility that was earlier cancelled by the credit officer. Fraud is also explicitly included here in the list that ORX reports. Fraudulent loans obtained in a fraudulent transaction should also be reported (ORX, 2011:22).

¹² This list is also of importance to this study, specifically when considering section 4.4.8, where the approach to classifying these types of losses more accurately, is proposed.

- Legal issues, such as where loan documents may contain legal defects like invalid clauses or ambiguous terms, are to be classified as boundary events according to ORX (ORX, 2011:22). Similarly, errors in scoring models should be seen as boundary events, as errors in scoring models may result in the approval of transactions that would otherwise not have been admitted (ORX, 2011:22). Certain sales practices may result in credit defaults and should be captured as boundary events. For capital purposes, ORX requires that any write-down due to loss of recourse be considered a credit risk loss (ORX, 2011:22).

There exists a wide variety of views on boundary events. By keeping in mind the examples of boundary events set out by ORX above, a view is held by the Federal Deposit Insurance Corporation (2003) that the fraudulent use of credit cards or the fraudulent use of homeowner equity lines of credit via a check should be treated as operational risk losses, as opposed to credit risk losses.¹³ According to the ORX (2011:22) examples, fraudulent loans obtained in a fraudulent transaction should be treated as a boundary event. ORX feels that this boundary between credit risk and operational risk is both accounting standard dependent and firm specific (ORX, 2011:22). It is therefore acknowledged by ORX that the boundary defining credit losses may be drawn differently in financial institutions (or member firms of ORX) for the same type of loss. ORX regards these ambiguities as not being higher than in the credit processes themselves and therefore being acceptable (ORX, 2011:22).

The International Accounting Standards (IAS) can be considered, as ORX makes reference to the fact that the boundary between credit risk and operational risk is accounting standard specific. The International Accounting Standards Board (IASB) explicitly states in the International Accounting Standards 39 (IAS39) that it would not be appropriate to recognise an impairment for losses that are expected to occur in a future period, because the necessary loss event (which might be, for example, the death of the borrower) has not yet occurred (IASB, 2009:71). Therefore, when considering the accounting standards, a loss should be recognised and written off in credit risk only once the loss has actually occurred. This is regardless of any other events that might have occurred prior to the loss event. For example, only once the “client” (or fraudster) involved in a fraudulent application has defaulted, can the loss be accounted for. According to IAS39, if the “client” actually consistently performs repayment, then impairment should not take place. Should the “client” default, then impairment is to take place irrespective of the fraudulent application. The reference that is made by the IASB to an event pre recognition is not to determine any classification. It is merely to ensure that write-off does not occur when repayment still exists, or even where it might be likely.

Therefore, the interpretation of specific events, such as, for example, fraudulent activity on credit cards and identity theft, is not only specific to a bank or firm, but it is also accounting standard dependent. Banks should be vigilant to the fact that losses might be logged for capital purposes in the

¹³ Refer to Section 4.3.1.

operational risk and the credit risk environment. This might, however, lead to double-counting. Losses in credit risk are mostly either embedded in trading profit and loss (P&L), or booked on specific accounts. For this reason it is necessary for the operational risk function in the bank to ensure that employees that are involved in the credit risk related processes are adequately educated and trained in recognising operational losses (ORX, 2011:22). This will assist in establishing processes for analysis, and also the proper recording of the operational risk component within these losses. It is therefore imperative that the operational risk-management function liaises with its credit risk counterparts (for instance, the credit risk impairment team) to promote consistency between firms on the implementation of the flagging of losses in the operational risk system (ORX, 2011:22).

Now that more detailed background was provided of the ORX view on boundary events, it is important to provide an understanding of classification frameworks and/or a taxonomy¹⁴. A taxonomy or classification framework will assist a financial institution in the classification of boundary events (Samad-Khan, 2008:28). In the following section, classification frameworks and taxonomies are discussed.

4.4.2. Classification Framework and Taxonomy

In order for a financial institution to manage operational risk structurally, it is of importance to have a mutually exclusive and exhaustive list of risk categories, according to the institution's risk universe (Samad-Khan, 2008:28). A proper taxonomy and classification framework for loss events will certainly assist in the classification of boundary events. The main reason for the difficulty and challenges behind the management of operational risk is that it is not easy for a financial institution to develop a workable classification scheme (Samad-Kahn, 2008:28).

Regardless of the high-level definition and the amount of risk classes defined, a financial institution should have a series of meaningful risk subclasses. This is the place and point at which a definition begins to hold significant meaning for an institution's business managers. It is also important to ensure that the actual cause behind the event has been identified in possibly assisting to classify the risk correctly for capital allocation purposes (Hoffman, 2002:40).¹⁵

From the definitions of operational risk provided, four high-level classes of operational risk events are clear: processes, people, systems, and external events. In Table 4.2, the following high-level examples of operational risks are set out:

¹⁴ A taxonomy is defined as the process or system of describing the way in which different things are related by putting them in groups (Merriam-Webster, 2012).

¹⁵ The view on cause identification and consideration is discussed in Section 4.3.2.2.2.

Table 4.2: Examples of operational risks per business area.

Business Area	Potential Risks
Process	• Breach of mandate • Incorrect/untimely transaction capture, execution and settlement • Loss of client assets • Mispricing • Incorrect asset allocation • Compliance issues • Corporate-action errors • Stock-lending errors • Accounting and taxation errors • Inadequate record-keeping • Subscription and redemption errors
People	• Unauthorised trading • Insider dealing • Fraud • Employee illness and injury • Discrimination claims • Compensation, benefit, and termination issues • Problems recruiting or retaining staff • Organised labour activity • Other legal issues
Systems	• Hardware and/or software failure • Unavailability and questionable integrity of data • Unauthorised access to information and systems security • Telecommunications failure • Utility outage • Computer hacking and viruses
External Events	• Operational failure at suppliers or outsourced operations • Fire or natural disaster • Terrorism • Vandalism, theft, robbery

Source: KPMG (2005:7)

The BCBS (BIS, 2006a:151) prescribed that the internal operational risk management system of a bank should be consistent with the scope of operational risk, as defined by the BCBS per the loss event types defined. The detailed loss event classification that a bank should utilise is set out below in Table 4.3:

Table 4.3: The detailed loss-event classification of the BCBS.

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
1. Internal fraud	Losses stemming from acts of a type intended to defraud, misappropriate property or circumvent the law, regulations, or company policy. Diversity and/or discrimination events, which involve at least one internal party, are excluded here.	1.1 Unauthorised activity	• Transactions intentionally not reported • Unauthorised transactions • Intentional position mismarking
		1.2 Theft and Fraud	• Fraud / credit fraud / worthless deposits • Theft / extortion / embezzlement / robbery • Asset misappropriation • Malicious destruction of assets • Smuggling • Check kiting • Forgery • Account take-over and impersonation and similar acts • Wilful tax non-compliance and/or evasion • Bribes / kickbacks • Insider trading (not on firm's account)
2. External fraud	Losses due to acts that were intended to defraud, misappropriate property or circumvent the law. This act is committed by a third party.	2.1 Theft and fraud	• Theft/robbery • Forgery • Check kiting
		2.2 Systems security	• Hacking damage • Theft of information
3. Employment practices and safety in the workplace	Losses due to acts committed that are inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity /	3.1 Employee relations	• Compensation, benefit, termination issues • Organised labour activity

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
	discrimination events	3.2 Safe environment	• General liability, for example slip and fall • Employee health and safety rules events • Workers compensation
		3.3 Diversity and discrimination	• All discrimination types
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.	4.1 Suitability, disclosure and fiduciary	• Fiduciary breaches / guideline violations • Suitability / disclosure issues in terms of, for example, Know Your Client (KYC) • Retail customer disclosure violations • Breach of privacy • Aggressive sales • Account churning • Lender liability • Misuse of confidential information
		4.2 Improper business or market practices	• Antitrust • Improper trade / market practices • Money laundering • Market manipulation • Insider trading (on firm's account) • Unlicensed activity
		4.3 Product flaws	• Product defects • Model error in product itself
		4.4 Selection, sponsorship and exposure	• Failure to investigate client per guidelines • Exceeding client exposure limits

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
		4.5 Advisory activities	Disputes over performance of advisory activities
5. Damage to Physical Assets	Losses arising from damage to physical assets from natural disaster or other events	5.1 Disasters and other events	- Natural disaster losses - Human losses from external sources (terrorism, vandalism)
6. Business disruption and failure in systems	Losses arising from disruption of business or system failures	6.1 Systems	- Hardware - Software - Telecommunications - Utility outage / disruptions
7. Execution, Delivery and Process Management	Losses from failed transaction-processing or process management. Also included are losses from relations with trade counterparties and vendors	7.1 Transaction capture, execution and maintenance	- Miscommunication - Data entry, maintenance or loading error - Missed deadline or responsibility - Model / system mis-operation - Accounting error / entity attribution error - Other task mis-performance - Delivery failure - Failure in collateral management - Reference Data Maintenance
		7.2 Monitoring and reporting	- Failed mandatory-reporting obligation - Inaccurate external report and loss incurred due to this
		7.3 Customer intake and documentation	- Client permissions and/or disclaimers missing - Legal documents missing and/or incomplete

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
		7.4 Customer / client account management	• Unapproved access given to accounts • Loss incurred because of incorrect client records • Negligent loss or damage of client assets
		7.5 Trade counterparties	• Non-client counterparty mis-performance • Various non-client counterparty disputes
		7.6 Vendors and suppliers	• Outsourcing • Vendor disputes

Source: BIS (2006a:305)

In addition to the requirement of the BCBS to submit losses in terms of the classification framework set out, ORX also requires of member banks to make their ORX submissions in accordance with the uniform definitions and standards as set out. Members are, however, free to adopt their definitions and methodologies for their internal loss recording (ORX, 2007:6). The classification of ORX events is consistent with the Basel categories but certain details do, however, differ (ORX, 2007:22). Table 4.4 sets out a comparison of the ORX loss-event classification, and the loss-event classification of Basel.

Table 4.4: Comparison of the ORX loss-event classification and the Basel II loss-event classification.

Basel Loss-Event Type Level 1	Basel Loss-Event Type Level 2	ORX Loss-Event Type Level 1	ORX Loss-Event Type Level 2
Internal fraud	Unauthorised activity	Internal fraud	Unauthorised activity
	Theft and fraud		General internal theft and fraud
			Internal systems security for profit
External fraud	Theft and fraud	External fraud	General external theft and fraud
	Systems security		External systems security for profit
		Malicious damage	Wilful damage and terrorism
			External system security (Wilful damage)
Employee practices and safety in the workplace	Employee relations	Employee practices and safety in the workplace	Internal system security (Wilful damage)
	Safe environment		Employee relations
	Diversity and discrimination		Safety in the workplace environment
Clients, products and business practices	Suitability, disclosure and fiduciary	Clients, products and business practices	Employment discrimination and diversity
	Improper business or market practices		Suitability, disclosure and fiduciary
	Product Flaws		Improper business or market practices
	Selection, sponsorship and exposure		Product flaws
	Advisory activities		Selection, sponsorship and exposure
Damage to physical assets	Disasters and other events	Disasters and public safety	Advisory activities
			Disasters and other events
Business disruption and failure in systems	Systems	Infrastructure and technology failures	Public safety and accidents
			Infrastructure and technology failures
Execution, delivery and process management	Transaction capture, execution and maintenance	Execution, delivery and process management	Transaction capture, execution and maintenance
	Monitoring and reporting		Errors in monitoring and reporting
	Customer intake and documentation		Customer intake and documentation
	Customer / client account management		Customer and/or client account management
	Trade counterparties		
	Vendors and suppliers		

Source: ORX (2007:36)

In terms of the guidelines set by the BCBS and ORX in terms of classification structures, banks and financial institutions have, in general, not strayed very far in the establishment of their own classification schemes and structures (MacLenaghan, 2007:25).

The reason for this, in part, is that the development of a workable classification scheme, or “taxonomy”, for operational risk is challenging. In order for a financial institution to manage operational risk structurally, it is of importance to have a mutually exclusive and exhaustive list of risk categories, according to the institution’s risk universe (Samad-Khan, 2008:28). This will make the classification task for the institution much easier, but banks globally, are still required to report their operational risk to their regulators using the Basel II classification structures.

This section mostly dealt with a classification framework for operational risks. As this study focuses on the boundary events between credit risk and operational risk, the next section provides an expansion of the classification framework to include credit risks.

4.4.2.1. Expansion of classification framework to include credit risks

In terms of a classification framework or taxonomy of events, a financial institution can utilise the frameworks provided by Basel or ORX as explained. These loss-event classification categories only cover the losses purely linked to operational risk. It was mentioned in Section 4.1, that credit risk, and therefore a loss relating directly to credit risk, can be defined as the potential that a borrower from the bank (or counterparty) will fail to meet her obligations in accordance with agreed terms (BIS, 2000:1). Also, the most common credit events (and for that reason also the risks) in financial institutions include repudiation, bankruptcy, and material adverse debt restructuring (Sungard, 2010). Based on this, a taxonomy or classification framework for general loss events can be expanded to include credit risk loss events. This will assist the institution with the classification of boundary events specifically. Refer to Table 4.5 for an expansion of the classification framework to include credit risks.

Table 4.5: Expansion of classification framework to include credit risks.

Event-Type Category (Level 1)	Definition	Categories (Level 2)
Client default	Losses stemming from the fact that the borrower from the bank, or counterparty, fails to meet the obligations in accordance with agreed terms (BIS, 2000:1)	Failure to meet obligations when due (Sungard, 2010).

Source: Sungard (2010)

In terms of the classification framework of credit risk (being a client failing to meet obligations) this should be the starting point for the identification of a possible boundary event. As was stated earlier, operational risk is frequently defined as any risk that is not categorised as market or credit risk, and is viewed as the risk of loss arising from a range of human or technical errors. It should therefore be

recognised that this definition is not intended to include defaults, as defaults are to be covered in the scope of credit risks (Gallati, 2003:289). Therefore, as soon as credit risk (and therefore a default) can be identified within a loss, it will typically be regarded as the first trigger to consider the possible existence of a boundary event. The impact might be observable and manifested in a credit risk event, resulting in a loss or a profit (Gallati, 2003:291).

The purpose of this research is not to go into the detail of the classification frameworks of risks and losses, but rather to look at approaches to the classification of boundary events. The approach of causal analysis will be utilised for the purposes of this study. The next section provides detailed information of causes. This is an important aspect of this study, as the focus in classification should not only be on effect, but also on cause. The focus, therefore, should be on where the loss is coming from (Hoffman, 2002:37).

4.4.3. Causes

According to Buchelt and Unteregger (2004:88) risk events and loss events for financial institutions are to be classified by the cause of the risk and not the consequence thereof. The view of the BCBS is that the distinguishing factor between pure credit risk and market risk losses, and those linked to operational risk, must be the cause of the loss (Moosa, 2006:102). Causes are conditions or circumstances that are in existence in or around processes and operations (Cech, 2007:39). They generally increase the chances or likelihood that an operational breakout can occur (Cech, 2007:39).

The Banking Council summarised the view of the BIS on boundary events by saying that operational risk losses, which relate to credit risk are those loss amounts that are written off or provided for within the credit process, whilst occurring either in part or fully from external events, or internal processes, people or systems that are inadequate or failing (Federal Deposit Insurance Corporation, 2003). However, the accounting guidance for losses relating to credit states that creditors should recognise credit losses when it is possible or probable that the involved creditor will not be able to collect all the amounts that are due per the obligations (Federal Deposit Insurance Corporation, 2003). As such, credit losses may occur as a result of the creditors' or financial institution's own underwriting, servicing, processing or administrative activities, together with the borrower's or client's failure to repay the institution per the loan agreement terms. While the creditor's personnel, policies and procedures, or systems may have an impact on the magnitude and/or timing of the credit loss, the BCBS keeps the character of the loss unchanged, and therefore, it is not changed from credit to operational for regulatory capital purposes (Federal Deposit Insurance Corporation, 2003).

In terms of the BCBS requirements for capital adequacy, credit losses can therefore be interpreted as losses that arise from a contractual relationship between the financial institution (the creditor) and the client (the borrower). In the instance that a write-off is performed outside the credit process due to

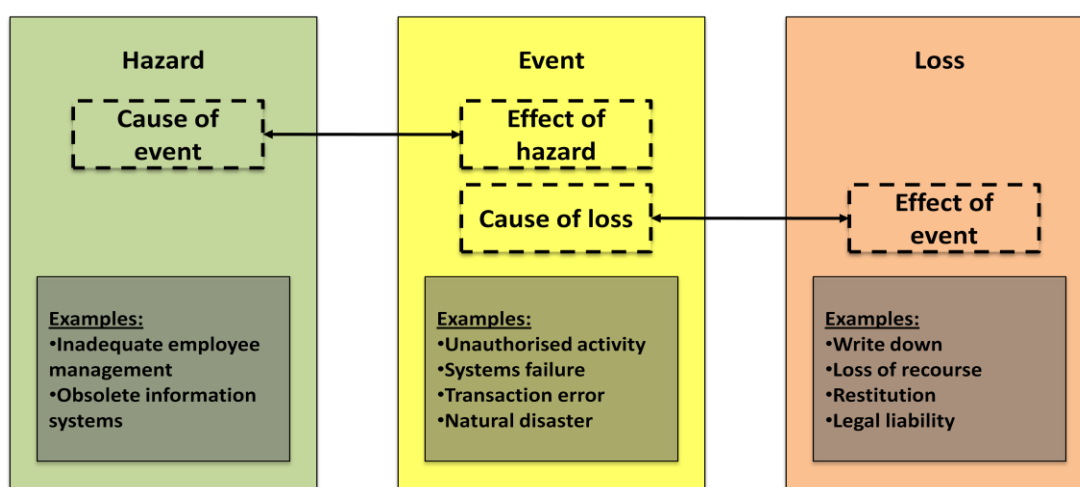
operational risk underlying the process, the amounts involved should be directly included in the operational risk capital calculation (Federal Deposit Insurance Corporation, 2003).

It is therefore of importance to consider the fact that operational risk events might be the actual cause of credit risk events; that is, leading to a borrower or counterparty failing to meet the obligations per the agreed terms. Operational risk for any financial institution – and within any business line – arises from the influence and interaction of internal and external factors and events on the people, technology and processes utilised in business processes within that institution (Gallati, 2003:290). The influence and interaction of these internal and external factors within any line of credit operations within a bank, might give rise to loss events. It should thus be noted that an operational risk loss in a credit process is not a boundary event, unless there is an associated default involved; otherwise, it is a pure operational risk event. The question therefore arises: *are these loss events classified as credit loss events, or operational loss events?*

4.4.3.1. The actual definition of a risk cause

To identify the causes of risks is the only rational way of arriving at an operational risk definition that allows a realistic differentiation from other risk categories (Buchelt & Unteregger, 2004:88). This view is clear when referring to Figure 4.2. The original Basel definition of operational risk has indeed been stated in causal terms by introducing the litany of “*people, processes, systems and external*”. In practice, however, managers of operational risk have developed an event-based measurement regime (Cech, 2007:59).

In the process of defining the various risk classes, the focus should be on cause and not just effect. Therefore, it can be stated that the focus should be on where the losses were coming from (Hoffman, 2002:37). Whilst referring to Figure 4.2, it is clear that there is a relationship between hazard, event and loss.



Source: Plesner (2007)

Figure 4.2: Relationship between hazard, event and loss.

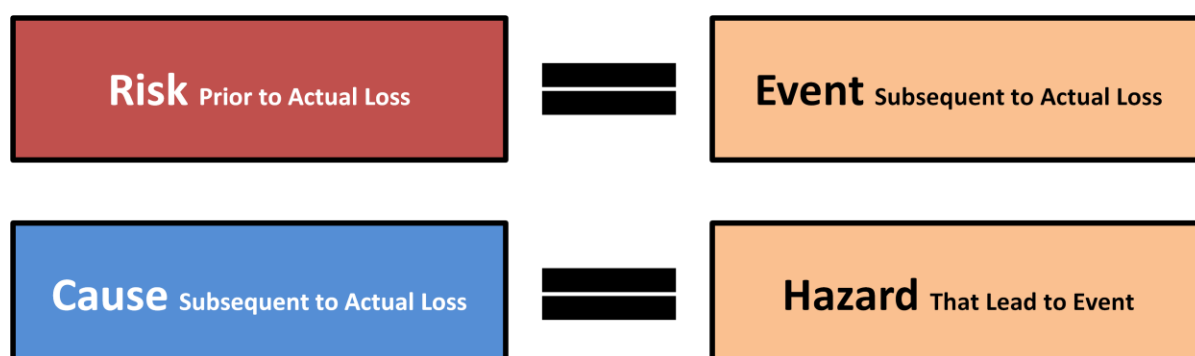
A hazard constitutes a factor, or factors, that increases the chances of an event occurring. Additionally, hazards can be viewed as anything that should have been done, but was not done (Izhar, 2010). The diagram in Figure 4.2 illustrates how a hazard can lead to an event, thereby also being the cause of the event. An event displays the effect of the hazard and, in turn, becomes the cause of a loss. A loss is ultimately the effect of the event. For example, inadequate employee management is a hazard that can lead to an event such as unauthorised activity, which, in turn, can lead to a loss such as write-down or restitution.

The cause(s) of an event should determine the classification as an operational loss event and not the consequences thereof (Buchelt & Unteregger, 2004:88). Operational risk may materialise either directly or indirectly through credit risk or market risk. (Cagan, 2009:2). Consider, for example, some transactions carried out with fraudulent intent (like at Barings Bank), in which market risk generated the loss (variation margin payments or price loss) but the cause was actually an operational risk (fraud or deficiencies in the organisation and its processes).

Causal conditions mostly exist in financial processing environments. Financial processing environments are usually complex, consisting of numerous linked processes and activities. These processes and activities might include staffing, team function, product definition, individual capability, process support, client service characteristics and business environment and other external factors (Cech, 2007:65). Under such circumstances, these causal conditions combine, producing an event (Cech, 2007:64).

There are rare cases where events have a single cause, as multiple causes are mostly identified. Events can sometimes have single, identifiable triggers, however, the patterns in the background of causal conditions contribute to their occurrence. Even though there would be an interest in where the loss had manifested itself, it is more important to classify the loss event. Hereby, the underlying source, circumstances and the causative factors behind each loss event will become clearer and more apparent. Furthermore, by focusing on people, for example, one may be more inclined to start analysing the human behaviour that might actually cause negative outcomes. This might include simple carelessness, peer pressure, inadequate control, or even dishonest tendencies. In contrast to this, the conventional approaches to risk definitions, which might be borrowed from auditing, regulatory or insurance communities, often tend to focus on the symptom or outcome rather than the underlying behaviour (Hoffman, 2002:38). It is therefore imperative to distinguish between causation, events, and losses. As set out in Figure 4.2, a hazard can be viewed as a cause, while the event is the effect of the hazard, but also the cause of the loss in the instance that a risk actually realises and leads to a loss. Per the figure, the hazard might be obsolete information systems, leading to an event, namely a systems failure that occurs. Subsequently, this causes a loss, which might be loss of recourse

in the event of default. In Figure 4.2, however, the actual risk is not evident. As the risk exists prior to the actual occurrence of a loss, the relationship as set out in Figure 4.3 holds true. This figure should be read in conjunction with Figure 4.2.



Source: Compiled by the author

Figure 4.3: Risk classification.

The risk, prior to the occurrence of the actual loss, is equal to the loss event subsequent to the loss that took place. At the same time, as set out in Figure 4.3, the cause of the loss is the hazard that led to the event taking place. For example, in the loss example that was utilised in Figure 4.2, the event that took place was system failure. This is an actual risk that exists within any financial institution, and therefore the risk is in existence until the loss actually occurs. The cause, subsequent to the actual loss taking place, is the hazard that led to the actual event. Subsequent to the occurrence of the loss, the cause can be viewed as the hazard that led to the actual event. This was obsolete information systems.

The classifications of Basel and ORX are according to events, as set out in the classification frameworks in Section 4.4.2 (Table 4.3 and Table 4.4). The classification by KPMG (2005:7) as set out in Table 4.2 is a cause-based approach. These are therefore two frameworks with significant differences, while each does attempt to classify operational risks and losses.

As mentioned earlier, the purpose of this research is not to go into the detail of the classification frameworks of operational risk losses in general, but rather to identify an approach to the classification of boundary events. The approach of causal analysis will be utilised for the purposes of this study. In the following sections, detail will be provided in terms of the various causes of operational risks.

4.4.3.2. The various causes of risks

In the sections that follow, the four “causal terms” will be discussed in more detail. These include *people, systems, processes and external events*. In addition to the four causes, the specific risks involved in the various causes are also discussed.

4.4.3.2.1. People as a cause of operational risk

The actions of *people* are a significant cause of operational risk events. The greatest asset of any services business is people. But, like any other asset, people are a source of risk, as well as reward. The most prominent risk associated with the staff and people involved in financial institutions, is the risk of fraudulent activity. The Federal Bureau of Investigation (FBI) statistics for 1998 show that about 32% of convictions for crimes against United States financial institutions involved bank employees (Sungard, 2010).

At this point, it should be clear that people are a cause of operational risks, and as part of this cause, there are specific risks involved with regards to the staff and people involved in banks. Table 4.6 sets out these key people risks.

Table 4.6: Key people risks.

Key people risks:	Including:
Employee fraud or malice	• Collusion; • Embezzlement; • Sabotage of bank reputation; • Money laundering; • Theft of physical and intellectual property; and • Programming fraud including virus introduction.
Unauthorised activity	• Misuse of privileged information; • Market manipulation; • Churning; • Activity leading to deliberate mispricing either with unauthorised counterparty or unauthorised product; • Limit breach; • Intentionally utilising incorrect models such as deliberate changes to parameters; • Illegal/aggressive selling tactics; • Activity outside exchange rules; and • Deliberately ignoring/short-circuiting procedures.
Employment law	• Wrongful termination of employment; • Discrimination/equal opportunity; • Harassment; • Non-adherence to other employment law; and • Non-adherence to Health and Safety regulations
Workforce disruption	• Industrial action; and • Other forms of disruption
Loss or lack of key personnel	• Lack of suitable employees; and • Loss of key personnel.

Source: Sungard (2010)

4.4.3.2.2. Systems as a cause of operational risk

The second causal term is *systems*. The reliance of literally all financial institutions on computer systems and technology infrastructure is absolute. This stretches from individual business lines to the core support functions of the institution – systems are the principal means for storing and managing great amounts of corporate, financial and transactional data and information (Sungard, 2010).

It should be clear that systems are a cause of operational risks, and as part of this cause, there are certain specific risks inherent in the systems utilised in the banks. Table 4.7 sets out these key systems risks (Sungard, 2010).

Table 4.7: Key systems risks.

Key systems risks:	Including:
Technology risk	• Inappropriate architecture
Systems development and implementation	• Inadequate project management; • Cost/time overruns; • Programming errors; • Failure to integrate and/or migrate from existing systems; and • Failure of system to meet business requirements.
Systems capacity	• Lack of adequate capacity planning; and • Inadequate software.
Systems failures	• Including network failure; • Interface failure; • Interdependency risk; • Software failure; • Hardware failure; and • Internal telecommunication failure.
Systems security breaches	• External security breaches; • Computer viruses; • Internal security breaches; and • Computer viruses.

Source: Sungard (2010)

4.4.3.2.3. Processes as a cause of operational risk

The third cause of operational risk loss events is *processes*. It is true that financial institutions have, through time, built expert “ways of doing things” in order to achieve their objective. This might include administering a checking account in the retail business, or confirming the details of a big swap transaction in the money markets. Listed below are some processes in the banking business that can contain significant risk for the bank (Sungard, 2010):

- trader hiring and vetting process;
- trader training and induction;

- compliance processes;
- limit-setting process;
- security and authentication process;
- marketing and sales process;
- new product approval process;
- making a trade;
- booking a trade;
- trade confirmation;
- exception management process;
- trade settlement;
- auditing process;
- market risk management;
- credit risk management;
- collateral management;
- documentation approval process;
- bonus allocation process;
- dispute resolution process;
- trader firing process; and
- investor communication.

Such processes within financial institutions are usually formal, and cover many of the risky activities in a bank. Some processes are merely routines performed by humans, while others form part of the core infrastructure of the institution. Few employees actually understand a complex bank process as a whole; therefore, the implications of sloppiness or even breakdowns in a typical process chain are often unclear (Sungard, 2010).

4.4.3.2.4. External factors as a cause of operational risk

Finally, *external factors* are the fourth cause of operational risk loss events. External factors can take various forms. External factors are a cause of operational risks, and as part of this cause, there are certain specific risks involved in the external factors that can take place. Table 4.8 sets out these key external risks (Sungard, 2010).

Table 4.8: Key external risks.

Key external risks:	Including:
Legal or public liabilities	• Breach of fiduciary duty
Criminal activities	• Money laundering; • Robberies; • Terrorism.
Outsourcing/supplier risk	• Breach of service level agreement; • Supplier failure.
In sourcing risk	• Failure of firm as supplier of services to third party
Disasters and infrastructural utilities failures	• Fire; • Flood; • Failure of critical supplies.
Regulatory risk	• Change of regulatory rules
Political/government risk	• Expropriation of assets; • Changes in tax regime; • Law and industry regime.

Source: Sungard (2010)

4.4.3.3. A risk and cause taxonomy

It is clear that there are endless risk and causation breakdowns for operational risks and loss events. As stated in the Section 5.4.3.2, there is a clear distinction between causes, events and losses. It is evident that there are four key causes of losses namely people, processes, systems and external factors. Within these causes, there are certain risks that can be identified – these risks, in turn, are what can unfold as losses in the future. These are set out in Table 4.9.

Table 4.9: A risk and cause taxonomy.

Cause	Risks	Basel Event Category
Human factor	Unauthorised activities	1.1
	Internal theft and fraud, that is, fraud by employees	1.2
	Internal system security	
	Relations with employees	3.1
	Discrimination acts and diversities	3.3
	Improper market practices and/or business practices	4.2
Processes	Safety in work environment	3.2
	Suitability, disclosure and fiduciary	4.1
	Flaw(s) in product(s)	4.3
	Selection, sponsorship and exposure	4.4
	Advisory-related activities	4.5
	Accidents and general safety	
	Maintenance of transaction capture and execution	7.1
	Reporting and monitoring	7.2
	New client intake and documentation	7.3
	Client account management	7.4
Systems	Inadequate, inefficient, poor functioning of IT systems	6.1
External	External theft and fraud	2.1

Cause	Risks	Basel Event Category
factors	External system security	2.2
	Other intentional fraudulent activities	
	Natural disasters and other events	5.1
	Disaster caused by human factors	
	Legal and political risk	
	Public services and/or public information – unavailability of providers	
	Counterparties in trade	7.5

Source: Compiled by the author

4.4.4. Controls and mitigation techniques

Operational risk is mainly defined as the risk of losses arising from external events, or processes, people and systems that are inadequate or failing. In order to have more control over operational risks, internal controls and internal audit systems are utilised as primary means. Operational risk losses can therefore generally be associated with weak links in the internal control procedures of financial institutions. In general, control techniques are used to prevent risks from occurring, whilst mitigation techniques can be utilised for the minimisation of losses in the event of realisation. This concept applies to both credit risk and operational risk.

The key to the successful management of operational risks thus lies in the ability of the institution to assess all processes for weaknesses and vulnerability, and to establish controls together with safeguards (Raghavan, 2003:848). The opposite also holds: an efficient and effective operational risk management framework will reinforce and improve the financial organisation's internal controls (Badea & Socol, 2010:42).

While it is clear that the mitigation and control of operational risks lie with the internal controls and audit systems of the institution, it is also necessary to look at mitigation techniques for credit risk. Credit risk involves the probability of a loss in the instance of the borrower or guarantor not fulfilling agreed financial obligations (Bagchi, 2005:549). Banks and other financial institutions therefore seek to be covered by proper, tangible, realisable securities. Third party guarantees are also applicable to avert, or at least minimise, the loss in the event of the guarantor or borrower defaulting. (Bagchi, 2005:549). The risk management techniques for credit risk include limits, intake of collateral, the diversification of the credit portfolio, securitisation, and the use of credit derivatives (Benedek & Homolya, 2007:5). These are therefore typical mitigation techniques that a financial institution can utilise to minimise the loss in the case of default by assisting in obtaining maximum recovery.

It should, however, be kept in mind that the focus of Basel II was mainly on capital measurement, instead of risk measurement for the purposes of management (Stein, 2010). Focusing on the management side of operational risk would have forced the BCBS to distinguish between “control activities”, which include compliance activities on the one hand, and “risk activities”. From the

management perspective, operational risk has been captured by the control profession, and from the perspective of a control mentality, operational risk is viewed as a risk that has to be avoided. Not all operational risks are to be avoided, and specifically for this reason, operational risk management should be adjusted to be made a risk discipline rather than merely a control or a compliance discipline that is primarily utilised for satisfying requirements such as the Sarbanes-Oxley Act (Stein, 2010).

Ultimately, controls and mitigation techniques for credit risk and operational risk do differ substantially and are an important aspect of the difference between the two risk types. Education of employees within financial institutions is also an important aspect in the classification processes. More detail is provided in Section 5.4.5.

4.4.5. Education

Risk education of bank personnel is of importance within the process of accurately classifying losses. Risk education and familiarisation with complex processes and procedures within the operations of the financial institution for all levels of staff can also reduce the risk of operational losses (Raghavan, 2003:848).

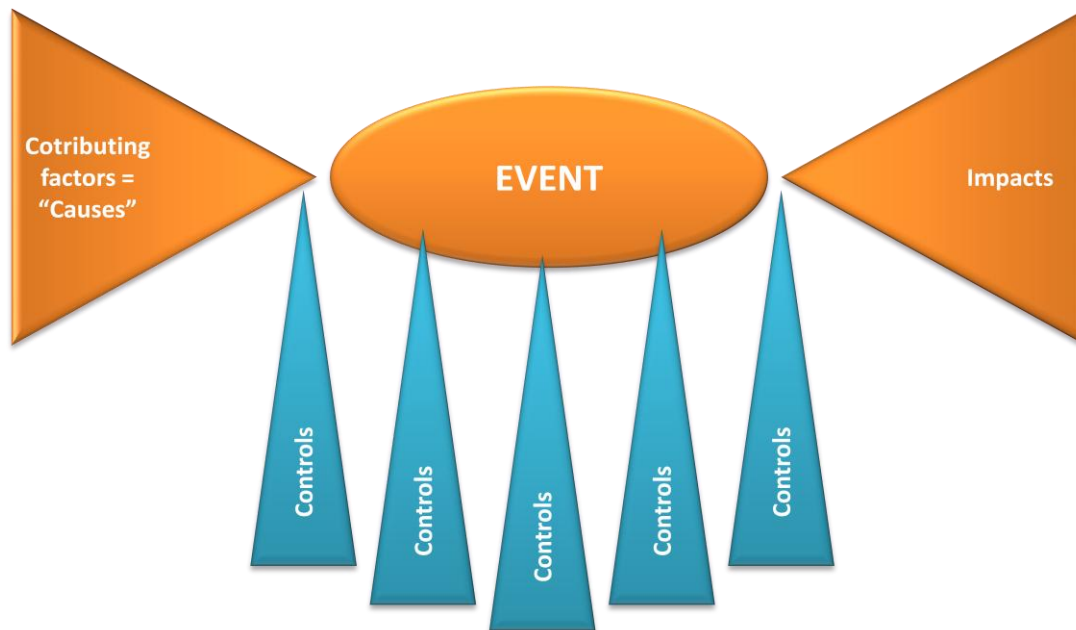
Operational risk practitioners, or “experts”, with the focus on specifically those with some background and history on taxonomies, have aimed at classifying losses based purely on their own understanding of the common intent behind the descriptions of the various loss event categories. The main challenge still exists, because those individuals and employees in the financial institutions that are actually responsible for entering the losses and data often do not have this type of background. In addition, it has been found that the common understanding among the experts is quite often not that common (MacLenaghan, 2007:30).

It is thus vital that all employees are completely informed regarding all the various risk types and the detail behind the various classification schemes. In order to ensure that staff is adequately informed on the various risk types, senior management should set the overall strategic direction and embed risk management philosophy across the business. This will ensure the accurate classification, measurement and management of the various risk types. Clear guidance reflected in explicit policies and procedures should be provided. Clear expectations of compliance with these policies and procedures should also be set (KPMG, 2009:10).

4.4.6. The “Bow-Tie” model of operational risk

Some of the points discussed earlier, can now be summarised in the explanation of the “Bow-Tie” model for operational risk that has been proposed by Cech (2007:39). Operational risks can be seen as resembling a “bow tie” (Cech, 2007:39). When referring to Figure 4.4, the left-hand side of the tie represents contributing factors or causes, the right-hand side represents impacts or effects and the knot

in the middle represents the actual event (Cech, 2007:39). The fourth component in the schematic is controls (Cech, 2007:39).



Source: Cech, 2007:39

Figure 4.4: The “Bow Tie” of operational risk, incorporating controls.

These four attributes, namely causes, events, impacts and controls, perfectly correspond to four simple but vital questions that should be asked regarding operational losses in a financial institution: *What happened? Why did it happen? What controls failed in keeping it from happening? What effects or impacts occurred as a result of the happening?* The question that can be asked now is: *Of these approaches to analysing risks, which is the best for classification?* (Cech, 2007:39)

The view is expressed that contributing causes are effective for root-cause analysis, as was seen in this section. It should, however, be kept in mind that most operational losses that are actually worth recording, are likely to have a wide variety, and a broad range of contributing causes. Actually, the list of causes per individual loss can easily span all four of the pillars in the Basel definition, namely people, process, systems and external. There are rare cases where events have a single cause, as multiple causes are mostly identified. Events can sometimes have single, identifiable triggers, however, the patterns in the background of causal conditions contribute to their occurrence.

The view can be held that an impact is the hard and objective fact that resides in the general ledger, after the occurrence of a loss (Cech, 2007:39). Impacts however provide limited insight into the instigation of a loss (Cech, 2007:39).

The next aspect to consider is controls. Controls have been discussed in Section 4.4.4. Most of the time, risk managers spend a substantive amount of their daily activities on managing controls. For this reason, controls might appear as a comfortable basis on which to construct a loss-classification system

(Cech, 2007:39). There are however some points to consider. On the one hand, a typical operational loss regularly involves the failure of an entire suite of controls – this can include single controls of various types. Certain losses do not have any associated controls. Therefore, even though a financial institution’s success in operational risk management is strongly linked to the effectiveness and functioning of its control implementation and design, this approach also does not ultimately provide a good basis for classification (Cech, 2007:39).

There is a view that events do leave a workable platform for loss event classification (Cech, 2007:39). An event resides at the crux of an occurrence. An event, as recorded in a database or report, ultimately includes references to all the causes, impacts and control failures that can be associated with it. An event is ultimately the first occurrence that happened – or failed to happen – in the materialisation of operational risk. In addition, occurrences can be uniquely assigned to a set of unique event-type categories (Cech, 2007:39).

Event classification is not problem-free. At present, it seems to be the most appropriate alternative to utilise (Cech, 2007:39). Several aspects of event classification have been discussed in the previous sections. In the following section, a decision tree is proposed specifically for the classification of boundary events.

4.4.7. A decision tree for boundary-event classification

A decision tree can play a positive part in the classification process of loss events, as the most important requirement that ORX sets out for event classification is consistency. Therefore, it is required that the classification takes place in accordance with agreed definitions and rules. Once a set of classification rules has been determined, various mechanisms and tools can be utilised for the automation of the classification process, and one of these is the use of decision trees (ORX, 2007:22). For the purposes of this study, a decision tree is utilised for the sole purpose of assisting with the thought process, and therefore with the accurate classification and identification of boundary events.

In order to propose an approach for purposes of defining a decision tree specific to credit risk events, operational risk events, and/or boundary events, the diagram in Figure 4.5 is proposed. All the concepts, as explained in the various sections of this chapter, are combined and incorporated to form the view as set out in Figure 4.5.

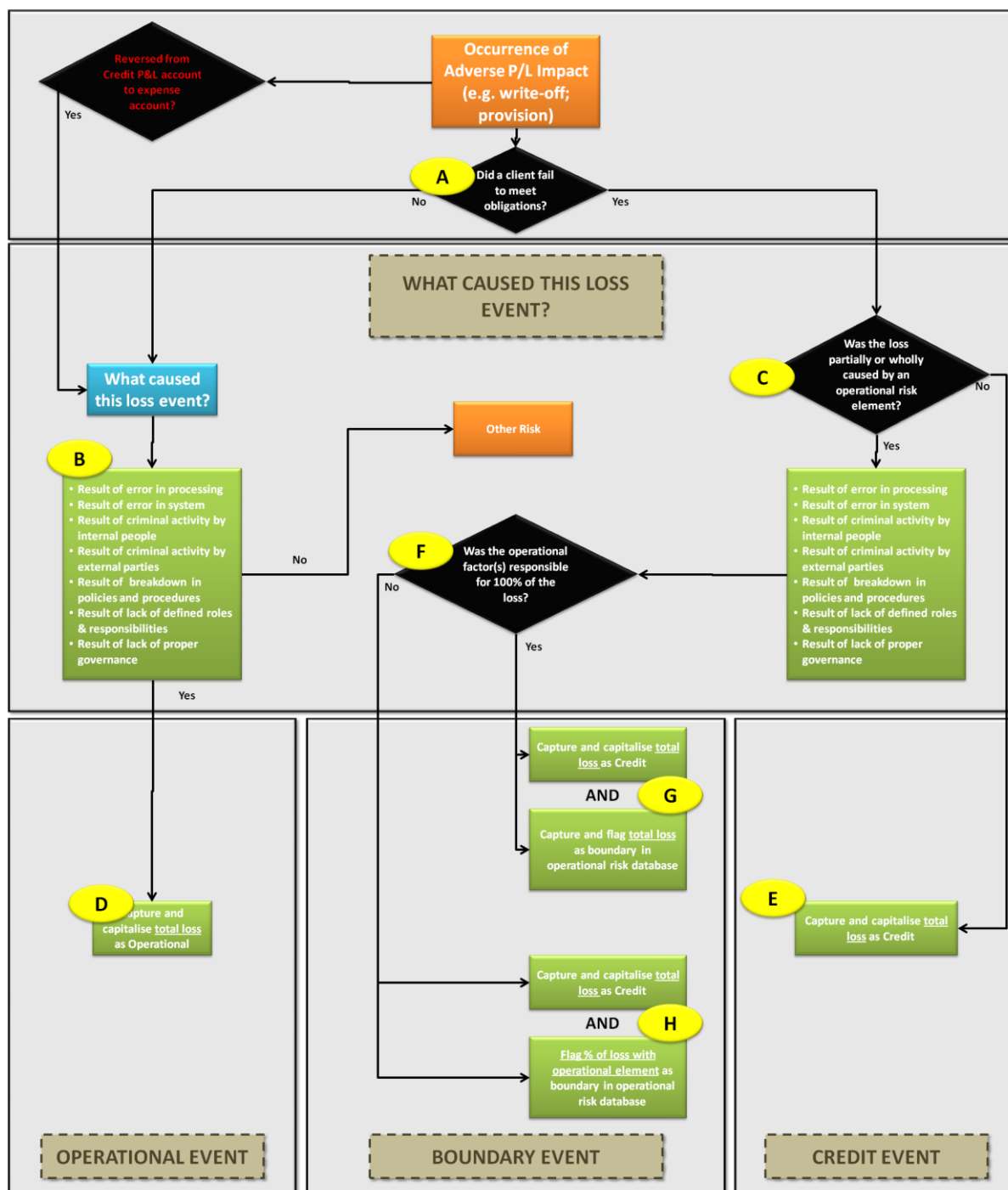
It is to be noted that the existence of a credit loss should be the starting point for the identification of a possible boundary event. Credit risk is viewed as the risk of a failure to meet a contractually pre-determined obligation.¹⁶ As was stated previously, credit losses are interpreted as losses that arise from a contractual relationship between the financial institution and the client. Furthermore, the view of the IASB has been considered earlier, where it is stated that any loss should be recognised and

¹⁶ Refer to Section 4.3.1.

written off in credit risk once it has occurred, irrespective of any other events that might have occurred prior to the loss event.¹⁷ The starting point for the consideration of a possible boundary event is therefore the identification of the element of default, and then, subsequently the identification of a possible element of operational risk surrounding the loss that took place. Furthermore, the decision tree in Figure 4.5 aims at guiding a user to identify the operational risk component of the total loss amount, as only the operational risk component is to be flagged as operational risk.

ORX (2011:21) requires that members report the operational risk component only. In the event that the member is not able to identify the operational risk component, then the total loss or loan amount is to be reported as an operational risk driven credit risk event (ORX, 2011:21). The total loss amount is therefore to be capitalised as credit risk, and flagged as a credit risk boundary event in the operational risk system of the bank. These principles are followed throughout the decision tree proposed in Figure 4.5.

¹⁷ Section 4.4.1 discusses the guidance of the IASB in more detail.



Source: Compiled by the author

Figure 4.5: A decision tree for boundary event classification.

Figure 4.5 can be explained as follows by utilising the steps set out in Table 4.10.

Table 4.10: Boundary event decision tree steps.

Step	Explanation
A	For the purposes of a decision tree specifically laid out for boundary events, the two “legs” to the tree include operational risk events, and credit risk events. Specifically for boundary events, the first point to consider is whether the client has defaulted. This exogenous risk event is a pre-requisite for the loss event to be further considered as possibly being a boundary event loss. As discussed in Section 4.4.2.1, as soon as credit risk – and therefore a default – can be identified within a loss, then this will typically be the first trigger to consider the possible existence of a boundary event. If there was no client default within this loss event, then this is the first indication of a pure operational risk loss. From here, the next step is B. If the client has defaulted on his obligations to the bank, then this serves as the first indication of a possible boundary event, and therefore, the next point to consider is whether an operational risk element(s) was involved in the loss event. From here, the next step is C.
B	As no client default was involved with the loss event, the next step is to verify whether operational element was responsible for the loss. In the event that no operational element could be identified as being responsible for the loss, the loss is due to another risk type, which is out of the scope of this study. In the event that an operational element could be identified as being responsible for the loss, then the next step is D.
C	Since the client has defaulted on his obligations to the bank, serving as the first indication of the possibility of a boundary event, it should be considered whether an operational element wholly or partially caused the loss event. In the event that no operational risk element was responsible for the loss, then the next step is E. In the event that an operational risk element was responsible for the event as a whole or partially, could be identified, then the next step is F.
D	As no client default is involved in the loss event, and it could be confirmed which operational risk element caused the loss event, then the loss is captured and capitalised as an operational risk loss. <End Process>
E	In the event that no operational risk element could be identified as being responsible for the loss event, then the loss is captured and capitalised as a credit risk loss. <End Process>
F	In the event that an operational risk element(s) was responsible for the loss, then the question should be asked whether the operational risk element(s) was responsible for the total loss, or only part of the loss. In the event that the operational risk element(s) was responsible for the total loss, then the next step is G. In the event that the operational risk element(s) was responsible for only a part of the total loss, then the next step is H.
G	The total loss amount should be captured and capitalised as credit risk AND The total loss amount should be captured and flagged as a boundary event. <End Process>
H	The total loss amount should be captured and capitalised as credit risk AND The total loss amount should be captured in the operational risk database, and only the percentage of the loss with the operational risk element, should be flagged as a boundary event in the operational risk database. <End Process>

Source: Compiled by the author

Credit losses are usually booked either on specific accounts, or embedded in trading P&L.¹⁸ As set out in the decision tree in Figure 4.5, in the event that a loss or adverse P&L impact is reversed from the credit environment, these losses are to be captured and capitalised in the operational risk environment.

4.5. A generic incident management lifecycle

A final consideration to this chapter is the use of an incident management lifecycle as it is vital that certain steps be taken by a bank subsequent to the occurrence of a loss. This will assist the bank in ensuring that the event is properly and adequately captured, investigated, analysed and reported prior to being closed. Of importance is also the fact that not all the business units within a financial institution will follow a similar incident management lifecycle process, purely because the various stages and supporting processes across the business units might be different.

As stated earlier, logical parameters should be set around how financial institutions report events relating to boundary events. At the same time, flexibility should be retained in how these events are managed and dealt with. Financial institutions then also need to collect sufficient data around operational risk loss events that have been classified elsewhere, as it is good practice especially from a risk management perspective to know exactly where losses are occurring (Tozer-Pennington, 2010). For this specific reason, it is important to consider an incident management lifecycle, as the collection of data for these incidents is increasingly important.

4.6. Conclusion

No explicit guidelines exist or are currently provided by the BCBS to assist financial institutions with the classification of boundary events. Literature relating to this subject is also limited. For this reason, the question can be asked: *what guidelines, policies, procedures and logic do banks and financial institutions actually follow with regards to the classification of such events?*

The topic of boundary events has been a relevant topic during the recent past, as boundary events between credit risk and operational risk are a significant source of concern for the industry, as well as for regulators. There are concerns that some major operational risks are not condensed in the AMA framework, as they are related to credit risk. This is a consequence of the boundary event classification challenges. Also, for the purposes of firm-wide risk management, financial institutions are to identify material boundary-event types of losses, and utilise this information for their overall risk management improvement.

Classification schemes, or taxonomies, play a key role in the classification process of events and losses. It is important for a financial institution to have a mutually exclusive and exhaustive list of risk categories according to the institution's risk universe. Causal analysis, education and control and

¹⁸ Refer to Section 4.4.1.

mitigation techniques can also be factors to consider in the classification processes of risks and losses. The BCBS is of the view that the distinguishing factor between pure credit risk and market risk losses, and those linked to operational risk, must be the cause of the loss. Another important aspect to consider is the controls and mitigation techniques that are utilised for the two risk types, as these do differ substantially. With regards to education, it is vital that all employees are sufficiently informed of all the various risk types and the detail behind the various classification schemes. This will ensure the accurate classification, measurement and management of the various risk types. It is necessary for the operational risk function in a bank to ensure that employees involved in the credit risk related processes are adequately educated and trained in recognising operational losses. This will also assist in analysis processes as well as the proper recording of the operational risk component within these losses. The essence lies in considering whether, and to what extent, banks take cognisance of these factors (classification schemes, causal factors, education and controls) in their classification processes.

Regulatory guidance with respect to boundary events is extremely limited and the ORX approaches and views on the boundary events topic do assist in the thinking process regarding the classification process of boundary events. ORX provides specific examples to serve as guidance to banks in terms of boundary events that are to be included in reporting to ORX. Application fraud, for example, is included in the list that ORX reports. According to ORX, loans obtained in a fraudulent transaction are to be capitalised as credit risk, and flagged as operational risk. On the other hand, the Federal Deposit Insurance Corporation believes that the fraudulent use of credit cards or the fraudulent use of homeowner equity lines of credit via a check should be treated as operational risk losses. The truth is that the boundary between credit risk and operational risk is both accounting standard dependent, and firm specific. Therefore, it is acknowledged that the interpretation of specific events, such as, for example, fraudulent activity on credit cards and identity theft is not only specific to a bank or firm, but it is also dependent on accounting standards.

The IASB explicitly states in IAS39 that it would not be appropriate to recognise impairment for losses that are expected to occur in the future, because the necessary loss event (which might be, for example, the death of the borrower) has not yet occurred. A loss should therefore be recognised and written off in credit risk only once default has occurred, irrespective of any other events that might have occurred prior to the loss event. The reference that is made by the IASB to an event pre-recognition is not to determine any classification – it is to ensure that write-off does not occur when repayment still exists, or even where it might be likely. Banks should be vigilant to the fact that losses might be logged for capital purposes in the operational risk and the credit risk environment. This might lead to double-counting. It is therefore vital that the operational risk function in the bank ensures that employees that are involved in the credit risk related processes are adequately educated and trained in recognising operational losses.

The existence of a credit loss is proposed as the starting point for the identification of a possible boundary event. Subsequently, a possible element of operational risk surrounding the loss that took place can be identified. The ultimate consideration is the fact that the boundary between the two risk types (credit risk and operational risk) is both bank specific, and standard dependent. The decision tree presented in Figure 4.5 aimed at guiding a user through the boundary event classification process. It should also assist a user to identify the operational risk component of the total loss amount, as only the operational risk component is to be flagged as operational risk.

This chapter provided a detailed discussion on the topic of boundary events, specifically those related to credit risk. Chapter 4 is an essential component of this study, as the various elements involved in classification of risks and losses were discussed, together with the regulatory views and current relevance of the topic. In addition, a proposal to simplify the classification process was also provided. Now the consideration is whether – and to what extent – banks take cognisance of factors such as classification schemes and causal factors in their classification processes. In addition, the question still remains: *How do banks currently classify boundary events?* In order to consider these points, a questionnaire has been compiled, based mainly on the theoretical coverage of this chapter. The questionnaire, the compilation and content thereof, as well as the results, are discussed in the next chapter.

Chapter 5

Methodology and Analysis of Results

5.1. Introduction

In Chapters 2, 3 and 4, a literature overview was presented on the background to Basel II credit risk, Basel II operational risk and boundary events respectively. This knowledge provides the base for acquiring an overview of the approach that banks currently follow in the classification of boundary events. In order to obtain the current view of South African banks regarding boundary events, the following research methodology steps were followed:

- identification of the banks to participate in the study;
- identification of the information that is required from the banks;
- design of the questionnaires;
- programming of the questionnaires in Microsoft Excel Visual Basic for Applications (VBA);
- holding meetings with the stakeholders of the participating banks for purposes of creating an awareness of the research;
- distribution of questionnaires;
- receipt and review of questionnaires, including follow-up where required; and
- writing up of results and responses received.

Each of the above steps is discussed in more detail in the sections that follow.

5.2. Identification of the banks to participate in the study

During the process of identifying the banks to participate in this study, the decision has been made to limit the study to South African banks only. The locally controlled registered banks in South Africa currently include the following (South African Reserve Bank, 2011):

- Absa Bank Limited;
- African Bank Limited;
- Bidvest Bank Limited;
- Capitec Bank Limited;
- FirstRand Bank Limited;
- Grindrod bank Limited;
- Investec Bank Limited;
- Nedbank Limited;
- Regal Treasury Private Bank Limited (In liquidation);

- Sasfin Bank Limited;
- The Standard Bank of South Africa Limited; and
- UBANK Limited.

Five of the banks listed above have been identified to participate in this study. The decision as to the specific banks to include for this research was mainly based on how advanced the bank is in terms of Basel II implementation. The entire South African Banking industry has implemented Basel II (Scholtz & De Villiers, 2011). As the AMA approach of Basel II has specific requirements in terms of the classification and treatment of boundary events, only certain banks – being specifically those that are more advanced in the approaches that are followed with regards to the management and measurement of operational risk – were selected.

5.3. Identification of the information that is required from the banks

The information required from the banks and the information to be included in the questionnaires is based on the information in the literature overview in Chapters 2, 3 and 4. The following points were foundational to the discussions in Section 4.4, and were therefore included as questions in the questionnaires:

- whether banks make use of an approved incident management lifecycle for effectively managing incidents and loss events that might occur throughout the institution;
- whether proper and approved guidelines, decision trees, taxonomies and causal categories are utilised by the bank for assistance in the approach to classification of loss events;
- how accurately the bank believes their current approach to classification and capital treatment is in terms of the Basel II regulations and requirements regarding the classification and treatment of boundary events,
- how strongly the operational risk experts in each bank believe factors such as taxonomies, decision trees, guidelines, causal factors and knowledgeable, adequately trained staff contribute to the success of classifying boundary events;

Questions were also asked on the following topics:

- information pertaining to loss thresholds that might or might not be utilised by the bank;
- gross loss amounts for the Basel II Retail Banking and Commercial Banking business lines specifically, and also the amounts that were flagged as boundary events for the previous financial year; and
- number of losses for the Basel II Retail Banking and Commercial Banking business lines specifically and also the number of losses that were flagged as boundary events for the previous financial year.

In terms of the data-specific questions posed to respondents, a short time period of observations of only one year was required. The reason is that some of the banks only recently adapted the AMA for operational risk, and by excluding these banks, the number of respondents would have been too small to draw meaningful results.¹⁹

In terms of the classification of specific boundary events and typical risk scenarios pertaining to such events, and the approaches of various individual experts, the following information was identified to be included in the questionnaires:

- demographical information of each individual, such as qualification background, number of years' experience in operational risk and credit risk, and current position at the bank;
- the risk category into which each individual will classify a set of typical and commonly found loss events and description thereof. The risk categories include pure credit risk, pure operational risk, or boundary event. The approach to these loss-event descriptions set forth in the questionnaires is explained in the section that follows.

The specific questions contained within the questionnaires are set out in Appendix 2 and Appendix 3.

5.4. Design of the questionnaires

The approach to conducting research can be either quantitative in nature, qualitative, or a combination of the two (Creswell, 2003:23). Whilst considering the approach to be adopted for this study, it was kept in mind that limited research and literature on the boundary events topic currently exists. This point has become evident during the process of performing the research as contained in this study. When a concept should be grasped and understood because limited research has been conducted on it, then it would typically merit a qualitative approach (Creswell, 2003:23). In order to obtain an understanding of the current classification of boundary events, a qualitative research approach was thus followed.

Based on the high-level points of information set out in Section 5.4, two separate questionnaires were utilised. The first questionnaire – referred to as the “General Questionnaire” – was designed to research the various approaches that banks follow in the process of classifying loss events, and specifically operational loss events that relate to credit risk. Various qualitative types of questions were included in order to obtain an understanding of the tools and mechanisms that banks utilise and make available to employees who are responsible for classifying their loss events. In addition, data-specific questions were asked pertaining to the capture of boundary events, such as the utilisation of loss thresholds and actual gross loss amounts and frequency of losses. The General Questionnaire was

¹⁹ In Section 6.5 a recommendation is made that future research can be conducted by utilising data of at least five years.

to be completed by each participating bank; thus resulting in five respondents for the General Questionnaire. The questions contained in the General Questionnaire are set out in Appendix 2.

The second questionnaire – referred to as the “Boundary Event Scenarios Questionnaire” – was designed to obtain an understanding of how risk management specialists approach the classification of typical, and frequently found typical loss-event scenarios. These loss descriptions, or loss scenarios, were compiled based on the literature background that exists with regards to boundary events and the boundary event examples that are commonly found in literature. The boundary event examples presented by ORX, as discussed in Section 4.4 were specifically utilised. The researcher also made use of her knowledge and industry experience to compile the loss descriptions. These loss descriptions were reviewed for validity and relevancy by two experts in the field of operational risk. A total of 16 typical loss-event scenarios was compiled and included in the Boundary Event Scenarios Questionnaire. In addition to this, each individual respondent of the Boundary Event Scenarios Questionnaire was to answer nine demographical questions, pertaining generally to the knowledge and experience backgrounds of the individual respondents. The Boundary Event Scenarios Questionnaire was required to be completed by at least three respondents per bank. The respondents were chosen by the Group Operational Risk managers of each participating bank and were considered by them as risk management experts. Nineteen respondents were available for the Boundary Event Scenarios Questionnaire. The questions contained in the Boundary Event Scenarios Questionnaire are set out in Appendix 3.

5.5. Programming of the questionnaires in VBA

The questionnaires were compiled and programmed in Excel VBA. In order to simplify the completion process for respondents, thus ensuring that the questionnaires are user-friendly for completion, incorporated query form was created. The coding by means of VBA also ensured that the questionnaires were completed in full by all the respondents, and that a respondent could not continue to the next question, without completing the current question.

The first page of each questionnaire consisted of a covering letter from the researcher and the School of Economics at the North-West University, Potchefstroom Campus. This letter explained the objectives of the study. The standard statement of confidentiality of information was also included. The covering letter to the questionnaires is set out in Appendix 1.

In terms of the questions for the General Questionnaire, option buttons were mostly utilised for use of input by the respondent. Programming was done in such a way that a user could not submit the questionnaire as final, if all the questions had not been completed. For the Boundary Event Scenarios Questionnaire, the demographical questions were also programmed by mostly using option buttons. Text boxes were incorporated in which the user could specify details such as qualification and current

employment position. The 16 loss descriptions were programmed by giving the user the three options to choose from in terms of the categorisation of each loss, namely “Credit”, “Operational” and “Boundary”. Subsequently, and based on the category selected, the user had to provide the loss amount applicable to the category selected. Three text boxes were available, in which the respondent could specify the amount of the loss that was purely due to credit risk, operational risk, or the amount that was flagged as a boundary event. Programming was performed in such a way that if the respondent selected “credit” as the event type, then only the “portion classified as pure credit risk” text box would be enabled. In the event that the respondent selected “operational” as the event type, then only the “portion classified as pure operational risk” text box would be enabled. Finally, in the event that the respondent selected “boundary” as the event type, then all three the text boxes would be enabled, that is, “portion classified as pure credit risk”, “portion classified as pure operational risk” and “portion classified as boundary event”.

Furthermore, the user could not proceed to the next scenario or loss description if the current loss description had not been completed. By means of the programming in VBA, the respondents were guided through the process of navigating through the questionnaires and completing the questionnaires. It was thereby also ensured that all the questions are completed prior to final submission.

Figure 5.1 provides an example of the front-end to the design of the scenarios or loss descriptions.

SCENARIO 11

Client M approaches the bank in order to obtain a new credit account. Client M presents the required documents as requested. The client's details are inputted into the bank's scoring model and, even though Client M is a student that works part-time, the scoring model rates him good enough to obtain a facility of R120 000.

The credit manager does not realise that there might be a possible error, and the facility is approved by him.

Client M draws the facility to the amount of R10 000, and only then is it discovered by the bank that the scoring model was in error, and that Client M is unable to repay the bank the amount of R10 000.

Event Type

☐ Credit

☐ Operational

☒ Boundary

Regulatory Treatment

Portion Classified as Pure Credit Risk:

Portion Classified as Pure Operational Risk:

Portion Classified as Boundary Event:

Source: Compiled by the author

Figure 5.1: Example of the loss description front-end in the Boundary Event Scenarios Questionnaire.

5.6. Holding meetings with the stakeholders of the participating banks

In order to initiate the communication with the various banks, and to start creating an awareness of the study, key operational risk stakeholders within the operational risk areas of each bank were contacted telephonically. A high-level background and overview was provided of the research topic, objectives and the methodology, and subsequently a meeting was set up with the key stakeholders at each bank.

The meetings were held between May 2011 and July 2011, based on the availability of the banking staff at the participating banks. Meetings were conducted by firstly presenting the covering letter stating the objective of the research and explaining the confidentiality statement. More detailed background was provided in terms of the approach to the study, the methodology followed, and the information that would typically be required by each bank in each of the questionnaires.

5.7. Distribution of questionnaires

E-mail addresses of the stakeholders were obtained during the meetings that were held in order for the questionnaires to be distributed. Subsequent to each of the meetings, the questionnaires were distributed by e-mail on the same day, or the following day of the meetings. The questionnaires were password-protected in order to protect the sensitive information as provided by the various banks. Finally, each bank was given three weeks to complete and submit their final questionnaires and responses.

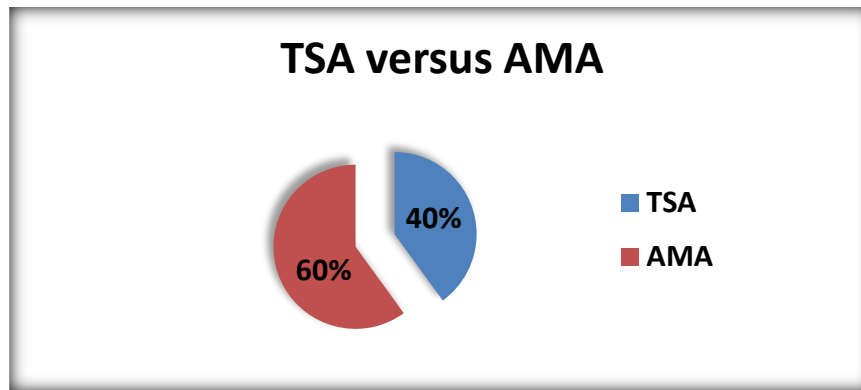
5.8. Receipt of questionnaires and writing up of results

On receipt of the questionnaires from the various banks, the information in each questionnaire could be employed to derive useful results. Firstly, the submitted data had to be captured in an acceptable format, useful for further data analysis.

5.9. Results – The General Questionnaire

Five respondents participated in the completion of the general questionnaire. As stated above, five banks in South Africa participated in this study, and the general questionnaire was to be completed by each bank.

Prior to starting the analysis of the results obtained, it was important to obtain an idea of the operational risk measurement approach that the respondents currently follow. There are 42% of respondents currently following TSA for operational risk; these banks are already in the early and final stages of implementing the AMA for operational risk. The remaining 60% of respondents are already utilising the AMA for operational risk. These results are represented in Figure 5.2 below.



Source: Compiled by the author

Figure 5.2: The measurement approach currently followed by the participating banks.

5.9.1. The use of tools to aid the classification process of loss events

As set out in Section 4.4, there are various tools and aiding mechanisms that banks can utilise for loss classification. The purpose of this section is to set forth the results that were obtained from the participating banks in terms of the tools that they currently utilise for the classification of boundary event losses specifically.

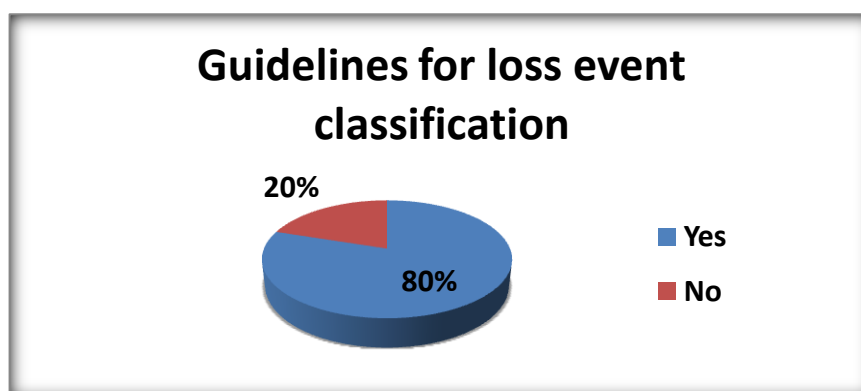
5.9.1.1. Incident management lifecycle

All the respondents currently utilise a documented and approved incident management lifecycle for the effective management of incidents that might occur throughout the organisation.

5.9.1.2. Guidelines for loss-event classification

The Basel II Framework does not provide any further guidelines as to what constitutes boundary events and as such, consistent guiding principles do not exist that banks can follow for accurately classifying and subsequently flagging such events. As far as the definition of an operational event is concerned, a bank could decide to adopt a stricter definition of operational risk; alternatively, appropriate definitions and guidelines should be instituted for other events or losses (Gallati, 2003:291).

Banks were asked to indicate whether proper, documented and approved guidelines are utilised for the classification of loss events, and specifically boundary events. Guidelines are utilised by 80% of banks. These results are indicated in Figure 5.3 below.



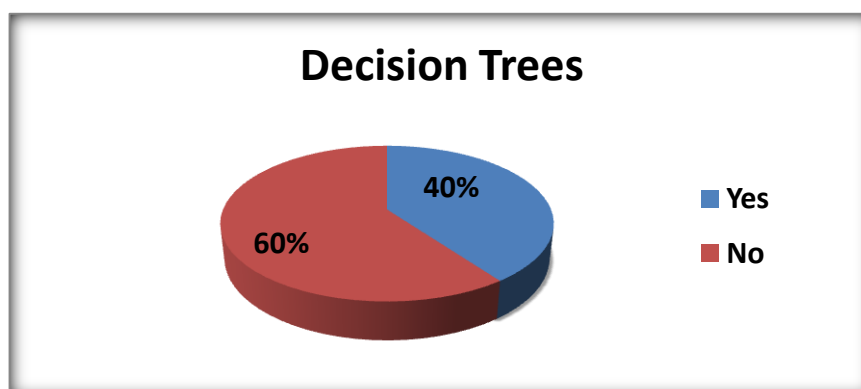
Source: Compiled by the author

Figure 5.3: The utilisation of documented and approved guidelines for loss classification.

5.9.1.3. Utilisation of decision trees for loss-event classification

A decision tree can play a positive part in the classification process of loss events, as the most important requirement that ORX sets out for event classification is consistency (ORX, 2007:22). Therefore, it is imperative that the classification takes place in accordance with agreed definitions and rules. Once a set of classification rules has been set, decision trees can be utilised for the automation of the classification process (ORX, 2007:22).

As set out in Figure 5.4, banks generally indicated that decision trees are mostly not utilised for assisting in the classification of losses and specifically boundary event losses. Decision trees are utilised by 40% of respondents to assist in their classification processes.



Source: Compiled by the author

Figure 5.4: Utilisation of decision tree for guidance in terms of loss classification.

5.9.1.4. Utilisation of a taxonomy of events for loss-event classification

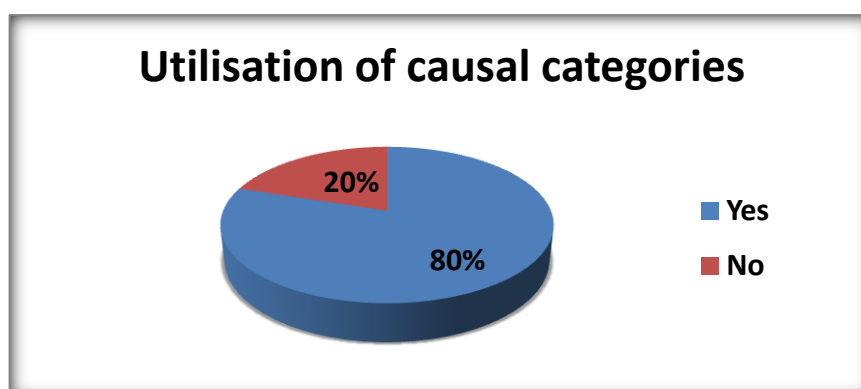
In order for a financial institution to manage operational risk structurally, it is important to have a mutually exclusive and exhaustive list of risk categories, in terms of the institution's risk universe (Samad-Kahn, 2008:28). Banks were therefore asked to indicate whether a taxonomy of events are

currently utilised to assist with loss classification. All the banks currently utilise a taxonomy of loss events. The taxonomies utilised will typically consist of a number of classes and subclasses in order to assist banks in their classification processes.

5.9.1.5. Utilisation of causal categories for loss-event classification

Causes are conditions that exist in or around processes and businesses. They generally increase the likelihood that an operational breakout can occur (Cech, 2007:39). It is therefore important to consider the fact that operational risk events might be the actual cause of credit risk events; that is, leading to a counterparty failing to meet the obligations per the agreed terms. Operational risk for any financial institution – and within any business line – arises from the influence and interaction of internal and external factors and events on the people, technology and processes utilised in business processes within that institution (Gallati, 2003:290).

In the light hereof, banks were asked to indicate whether they make use of causal categories to assist with the classification processes of their losses. Of all the respondents, 80% indicated that they do utilise causal categories in their loss-classification process. Figure 5.5 represents these results.



Source: Compiled by the author

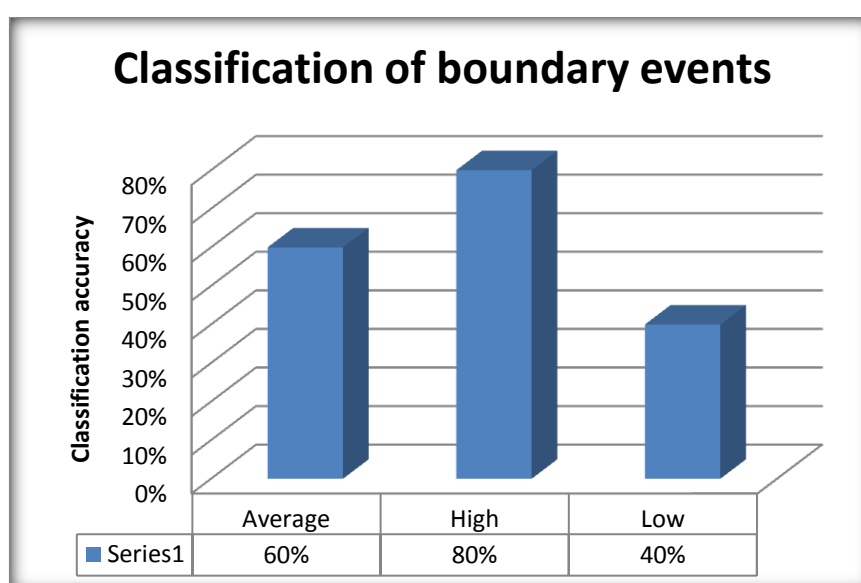
Figure 5.5: Utilisation of causal categories for guidance in terms of loss classification.

5.9.2. Accuracy of classification and capital treatment of boundary event losses

Banks were asked to indicate how accurate, they believe, their classification of boundary events is. They were required to provide a rating from 1 to 10, where 1 stipulates zero percent accurate and 10 stipulates one hundred percent accurate. The average rating of all the respondents was calculated, and in terms of the accuracy of boundary event classifications, banks feel that they perform such classifications 60% accurately. Also, the highest and lowest ratings were calculated. These are indicated in Figure 5.6 below.

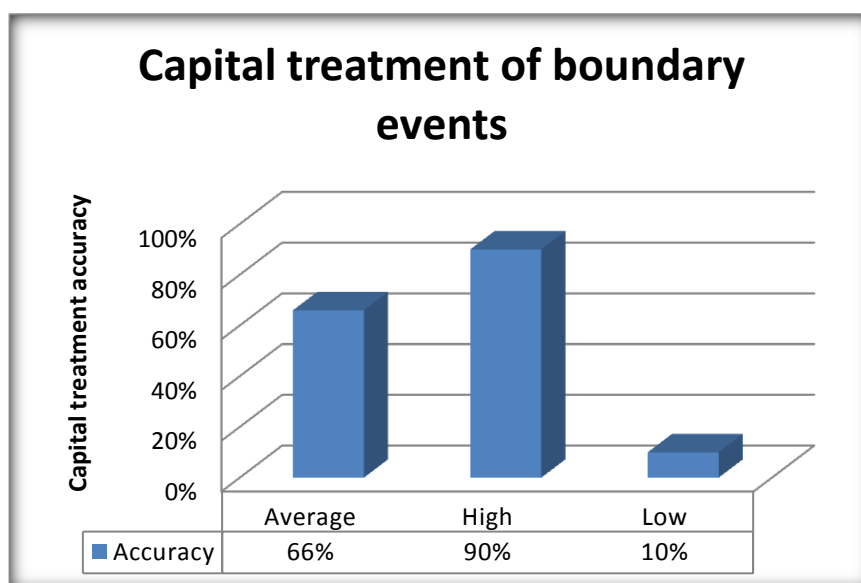
In terms of capital treatment of the various losses, the BCBS requires that boundary events should be treated as credit risk for the purposes of calculating minimum regulatory capital under the Basel II Framework (BIS, 2006a:153). Such losses will then not be subject to an operational risk capital charge but for the purposes of internal operational risk management, banks are required to identify all material operational risk losses. These material operational risk-related credit risk losses should be flagged separately within a bank's internal operational risk database (BIS, 2006a:153).

Similar to the calculation of results set out in Figure 5.6, the average rating was calculated for the responses to the treatment of boundary event losses from a capital perspective. Banks feel that they treat these losses on average, 66% accurately. The highest and lowest ratings were also calculated. These results are presented in Figure 5.7 below.



Source: Compiled by the author

Figure 5.6: Accuracy of boundary event classifications.

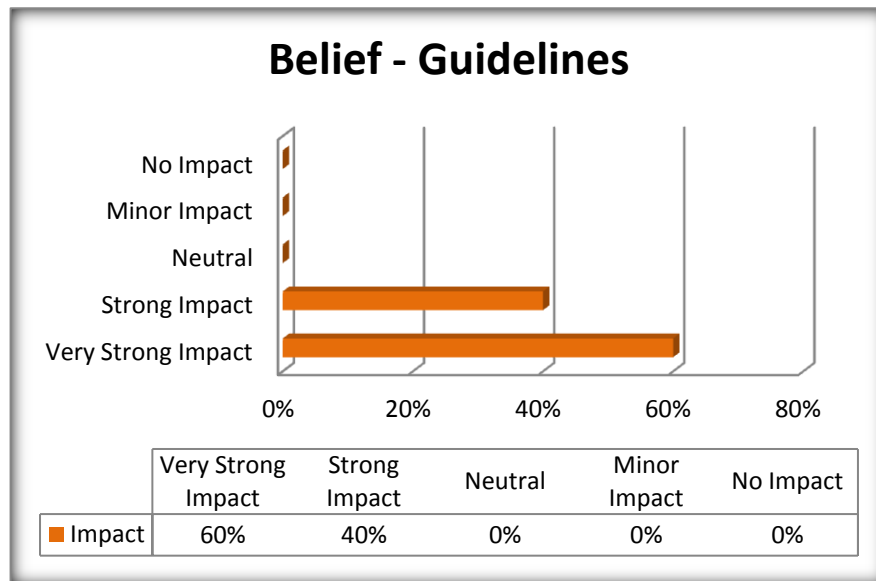


Source: Compiled by the author

Figure 5.7: Accuracy of boundary event capital treatment.

5.9.3. Contributing factors to accuracy of boundary event loss classifications

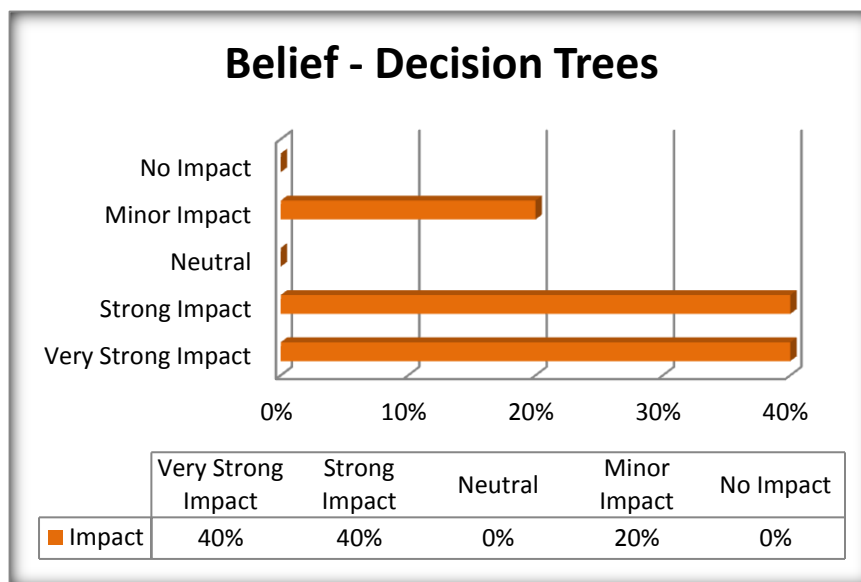
As noted before in this study, there are currently limited guidelines available – especially from a regulatory perspective – that banks can utilise to assist with the classification of boundary events. The five participating banks were asked to indicate how strongly they believe documented and approved guidelines impact the success or failure of boundary event classification and loss treatment within the organisation. As depicted in Figure 5.8, the stakeholders in the five banks believe that the use of documented and approved guidelines for the classification and treatment of boundary events definitely does contribute to the success and/or failure of such classifications.



Source: Compiled by the author

Figure 5.8: Belief that guidelines do/do not contribute to the success of classifications.

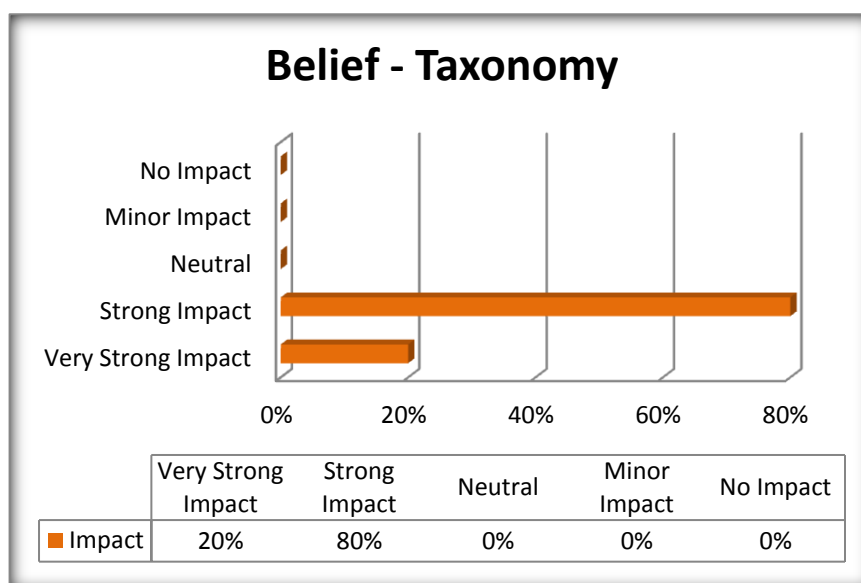
Furthermore, Figure 5.9 demonstrates that most of the banks believe that the usage of decision trees has a definite impact on the success of the accuracy of classifications. This is in contrast to the fact that 60% of the banks currently do not make use of decision tree as a mechanism to assist with classification processes, as was seen in Section 5.9.1.5.



Source: Compiled by the author

Figure 5.9: Belief that decision trees do/do not contribute to the success of classifications.

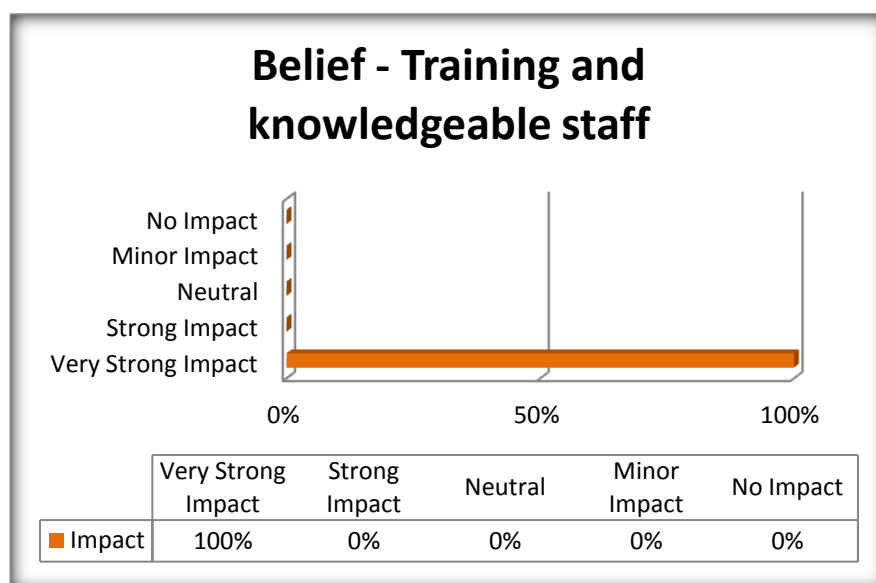
Most of the banks believe that a taxonomy of events has a definite impact on the success of loss-event classifications. This is illustrated in Figure 5.10 below.



Source: Compiled by the author

Figure 5.10: Belief that taxonomy of events does/does not contribute to the success of classifications.

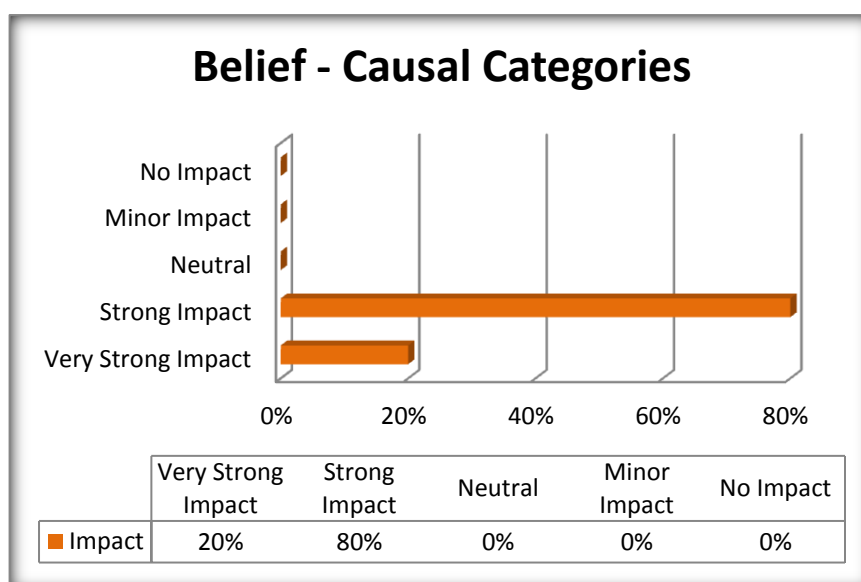
In terms of the knowledge and experience of staff members, it can be seen in Figure 5.11 that all the banks believe that knowledgeable, experienced and trained staff has a strong impact on the success or failure of the classification of loss events. It was discussed in Section 4.4.6 of Chapter 4 that it is important that all employees are completely informed of all the various risk types and the detail behind the various classification schemes. In order to ensure that staff is adequately informed regarding the various risk types, senior management should set the overall strategic direction and embed risk management philosophy across the business. This will ensure the accurate classification, measurement and management of the various risk types (KPMG, 2009:10).



Source: Compiled by the author

Figure 5.11: Belief that knowledgeable, experienced and trained staff contribute to the success of classifications.

All the banks believe that the use of documented and approved causal categories has a strong impact on the classification of losses related to boundary events. Only 80% of the banks, however, indicated that they currently make use of causal categories to assist in the categorisation processes.²⁰ This is illustrated in Figure 5.12.



Source: Compiled by the author

Figure 5.12: Belief that causal categories contribute to success/failure of classifications.

²⁰ Refer to section 5.9.1.5.

In summary, the results in Figure 5.9 and Figure 5.12 show that banks believe that the use of decision trees and causal categories have an impact on the accuracy of event classifications. It was, however, also clear that all the banks currently do not make use of these tools to assist them in their classification processes.

In this section, the banks' views on contributing factors to the accuracy of boundary event loss classifications were discussed. The following section uses the responses to the quantitative questions to provide some insight into how effectively boundary events are captured by the banks.

5.9.4. Operational risk data

A number of quantitative questions were put forth to the participating banks in the General Questionnaire to obtain an understanding of how effectively banks capture boundary events. In addition, the aim is also to see whether any consistency exists among the participating banks with regards to the number of boundary events currently captured throughout the participating banks.

5.9.4.1. Loss-reporting thresholds

One of the criteria that are put forth by Basel II is that banks must have an appropriate gross loss threshold for internal loss-data collection (BIS, 2006a:153). The BCBS recognises that an appropriate threshold might vary between banks, and also within a bank across the various business lines and/or event types (BIS, 2006a:153). It is, however, also true that the data collection threshold varies significantly across financial institutions. The choice of thresholds has an impact on operational risk capital computations (BIS, 2011:3).

For the sample of banks included in this study, not all the banks are currently on AMA for operational risk, and some banks are therefore still on TSA. Therefore, only 80% of the respondents participated in answering the questions on loss-reporting thresholds, as 20% of the respondents are still on TSA and are therefore not flagging boundary events in the operational risk system. The responses received from the AMA banks indicate that in general, 60% of the banks do utilise a loss threshold for loss reporting, whereas 40% of the banks do not utilise a loss threshold. The banks were, however, also asked to indicate their loss thresholds for the Basel II Retail Banking and Commercial Banking business lines respectively. The ORX operational risk report indicates that the Retail Banking and Commercial Banking business lines are the top two business lines in terms of the number of events that were reported for 2009 (ORX, 2010:11). These two business lines were responsible for about 70% of the total number of events. The top three event types have been reported to be Execution, Delivery and Process Management, External Fraud and Client Products and Business Practices (ORX, 2010:11). Refer to Figure 5.13 for the distribution of frequency of loss by business line, by event type.

Nos of Events	Internal Fraud	External Fraud	Employment Practices & Workplace Safety	Clients Products & Business Practices	Disasters & Public Safety	Technology & Infrastructure Failures	Execution, Delivery & Process Management	Malicious Damage	Total	% of Total
Corporate Finance	1	25	18	55	14	0	56	0	169	0.62%
Trading & Sales	11	142	105	135	3	114	1,874	0	2,384	8.81%
Retail Banking	692	7,233	2,395	1,672	203	170	3,764	56	16,185	59.83%
Commercial Banking	26	810	86	541	18	32	1,147	0	2,660	9.83%
Clearing	5	186	7	10	0	23	274	0	505	1.87%
Agency Services	10	231	13	60	1	13	1,158	0	1,486	5.49%
Asset Management	7	7	23	124	2	17	506	0	686	2.54%
Retail Brokerage	42	57	96	546	1	12	360	0	1,114	4.12%
Private Banking	28	84	30	423	1	26	668	0	1,260	4.66%
Corporate Items	5	36	229	53	29	36	149	1	538	1.99%
Multiple Lines	4	16	7	16	1	5	17	0	66	0.24%
Total	831	8,827	3,009	3,635	273	448	9,973	57	27,053	
% of Total	3.07%	32.63%	11.12%	13.44%	1.01%	1.66%	36.86%	0.21%		

1% - <5%

5% - 10%

>10%

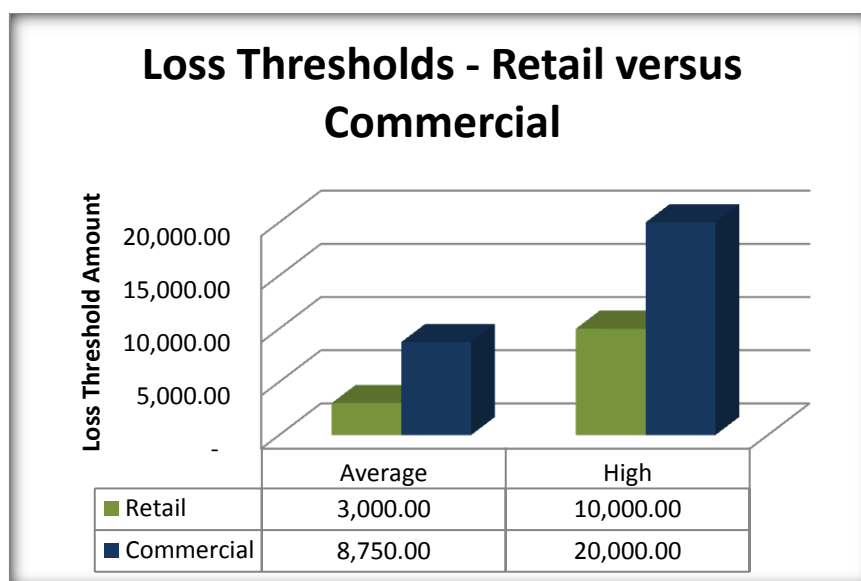
Source: ORX (2010:11)

Figure 5.13: Distribution of frequency of loss by business line by event type – 2009Q1-4.

The average loss threshold that is utilised for the Retail Banking business line is R3 750, whereas the average loss threshold for the Commercial Banking business line is R8 750. The maximum threshold reported for the Retail Banking business line is R10 000 and for the Commercial Banking business line, it is R20 000. The minimum loss thresholds applied are zero for both the business lines in question. These results are illustrated in Figure 5.14.

Of all the banks, 75% indicated the same threshold amount for the Retail Banking business line, as for the Commercial Banking business line. As motivation for using these numbers, some banks indicated that an internal loss data analysis has been performed in order to arrive at the utilised threshold amount. The banks utilising a zero loss threshold amount for both the business lines indicated that no threshold is utilised in order to accurately report on the loss events, and in order to ensure data completeness. Some banks utilise a lower loss threshold for the Retail Banking business line, and a higher loss threshold for the Commercial Banking threshold. The motivation provided for this is that Retail Banking traditionally has lower value, but higher volume incidents. These banks therefore feel that the data in terms of these losses need to be as complete as possible in order to effectively manage the risks. Commercial Banking has lower volumes of incidents with higher impacts. Banks feel that a higher threshold for these types of risks insures that the focus and attention of risk managers are placed on the correct and applicable areas.

Figure 5.14 illustrates the loss-reporting thresholds of banks for the Retail Banking and Commercial Banking business lines.



Source: Compiled by the author

Figure 5.14: Loss-reporting thresholds of banks – Retail Banking versus Commercial Banking.

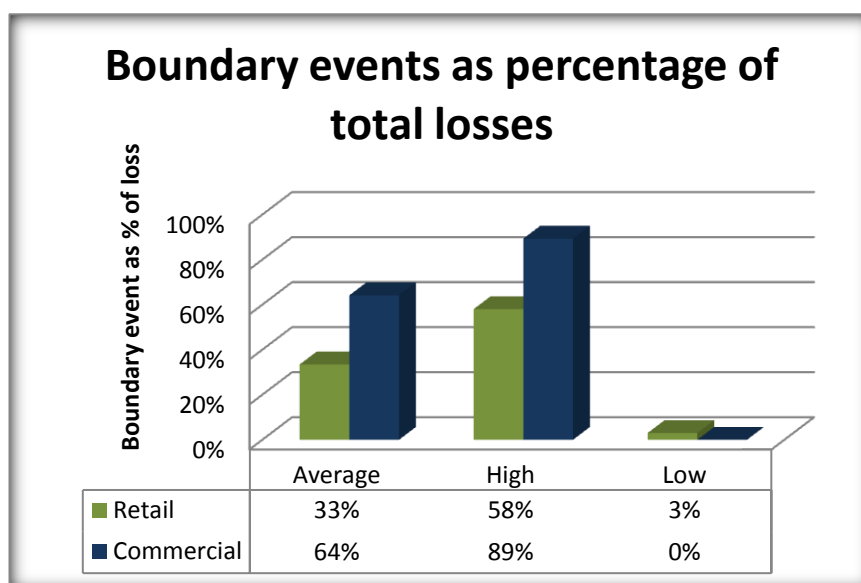
Banks were also asked to indicate whether different loss thresholds are utilised for boundary events for the Retail Banking and Commercial Banking business lines respectively. All the banks, however, utilise the same loss thresholds for boundary events, and at certain banks, it was indicated that a threshold amount for boundary events is investigated in order to ensure more accurate future classification of these types of losses.

5.9.4.2. Reported boundary events as percentage of total losses

Studies indicated that boundary event losses represent 30% of the total losses and in terms of the value of losses, this share rises to 40% in total (Sands, 2011a). This information is based on an internal study of the BCBS' standards implementation subgroup on operational risk (Sands, 2011a).²¹ Banks were asked to indicate the gross loss amounts for the previous financial year²² for the Retail Banking and Commercial Banking business lines respectively. In addition, the loss amounts for these losses that were flagged as boundary events also had to be indicated. By utilising this information, it was found that the average boundary event losses in Rand amounts comprise 33% for Retail Banking and 64% for Commercial Banking. The maximum boundary event losses relative to gross losses are 58% for Retail Banking and 89% for Commercial Banking, whereas the minimum indications were 3% and 0% for Retail Banking and Commercial Banking respectively. These figures are illustrated in Figure 5.15 below.

²¹ Refer to Section 4.2 for more detail.

²² The previous financial year was 2010.

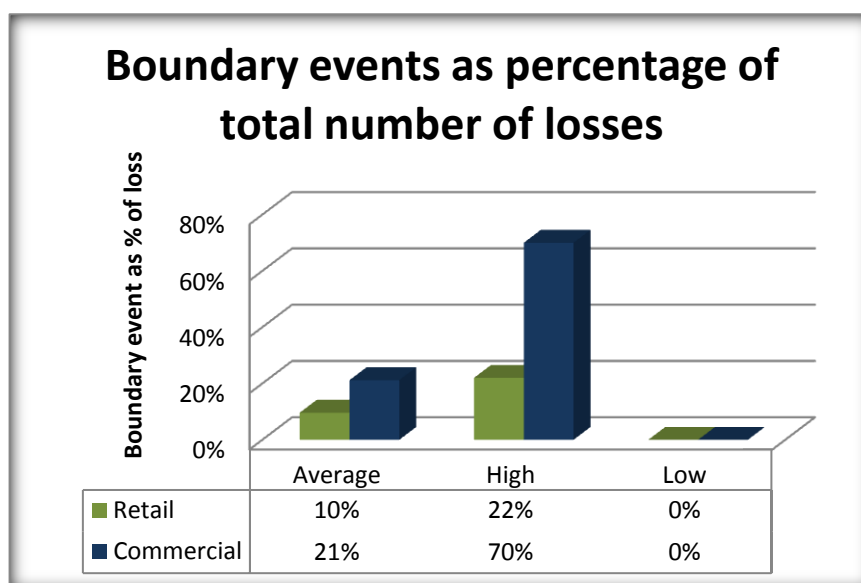


Source: Compiled by the author

Figure 5.15: Boundary event losses as percentage of total losses.

Banks were also asked to indicate the frequency of losses for the previous financial year²³, for the Retail Banking and Commercial Banking business lines respectively. In addition, the frequency of losses that were flagged as boundary events also had to be indicated. By utilising this information, it was found that the average boundary event losses comprise 10% for Retail Banking and 21% for Commercial Banking. The maximum boundary event losses relative to gross losses are 22% for Retail Banking and 70% for Commercial Banking, whereas the minimum indications were 0% for both Retail Banking and Commercial Banking. This is illustrated in Figure 5.16 below.

²³ The previous financial year was 2010.



Source: Compiled by the author

Figure 5.16: Boundary event loss frequencies as percentage of total loss frequencies.

In the sample observed and the period under observation, there have been outliers in the responses received. Various reasons for this observation can be noted. Firstly, 50% of the banks responding to these questions have only adopted the AMA during the past year, and the observation period applicable is for the previous financial year. Secondly, the remaining 50% of the banks also only adopted AMA during the past four years. Even though a proposal here could be to increase the observation period so that at least five years are utilised, in order to smooth out any outliers, this might still prove to be challenging as enough data would not be available from which to analyse more meaningful results. Also, as this study focuses only on South African banks, the sample size of 5 is small.

In Section 5.9.4.1, a view was obtained of the loss-reporting thresholds that banks currently apply. The loss-reporting threshold applied by banks can undeniably have an impact on the volume and value of losses captured, and therefore also on the boundary events that are flagged – or not flagged – in the process. The loss threshold is a regulatory requirement that might have a significant impact on both the management and measurement of operational risk. The Range of Practice Paper by the BCBS indicated that data collection thresholds show wide diversity across banks (BIS, 2011:25). Some financial institutions apply higher thresholds in order to avoid cluttering their operational risk databases with events that are deemed to be immaterial; other institutions choose lower thresholds with the view that they will obtain more information on their loss events for management purposes (BIS, 2011:25).

Another point to be considered is that banks might, or might not include provisions in their gross loss reporting. This fact will have a significant influence on the results being observed. The BCBS states in their latest supervisory guidelines on the AMA that provisions, or “reserves”, being the potential

operational loss impact, should be taken into account in the gross loss amount (BIS, 2011:21). In the sample observed, 25% of banks currently include provisions in their gross loss reporting. This fact can therefore also skew the responses observed.

Finally, it is true that banks currently follow different approaches with regards to their loss event classification processes, and therefore also for the classification and capitalisation of boundary events. This fact is clearly reflected in the responses obtained from banks in terms of the tools they currently utilise for classification as set out in Section 5.9.1. There are clear differences in whether banks utilise proper and approved guidelines for the classification of boundary events, causal categorisations and decision trees. In addition, it should also be kept in mind that even though banks might make use of these tools, the approaches followed by the banks in the utilisation of such tools can also be significantly different. This has also been identified in the 2006 Observed Range of Practice document of the BCBS (BIS, 2011:11). Here it has been found that a wide range of practice was emerging during the implementation of banks' AMA frameworks. Also, the diversity in practice is consistent with the evolutionary nature of operational risk management as an emerging risk management discipline (BIS, 2011:1).

Keeping these challenges in mind, the aim of this section in the research is to obtain a broad idea of how prudent banks are in the capturing of boundary events, mainly based on the indication provided by Sands (2011a), stating that boundary event losses should represent about 30% of the total losses. In terms of the value of losses, this share should rise to about 40% in total. Therefore, if the average of the responses received is observed based on the loss amounts, being 33% and 64% for Retail Banking and Commercial Banking business lines respectively, these numbers seem to be in the range of the 40% as indicated by Sands (2011a). In terms of the number of losses, the averages observed were 10% and 21% for Retail Banking and Commercial Banking business lines respectively. In this instance, significant outliers were also present, but nevertheless, based on the average, these indications are significantly less than the 30% indication provided by Sands (2011a).

The conclusion that is reached at this point is first of all, that there is significant disparity in the degree to which boundary event losses are captured in the Retail Banking and Commercial Banking business lines (at the different banks included in this study). There are numerous underlying factors responsible for the variance, and as discussed above, amongst others, the diversity in terms of the use of classification tools also plays a significant role (apart from the other factors that include loss-reporting thresholds and the inclusion or exclusion of provisions in gross losses). In order to observe and investigate the approach to classification in more detail, the responses obtained in terms of the Boundary Event Scenarios Questionnaire are explained and discussed in detail in the section that follows.

5.10. Results – the Boundary Event Scenarios Questionnaire

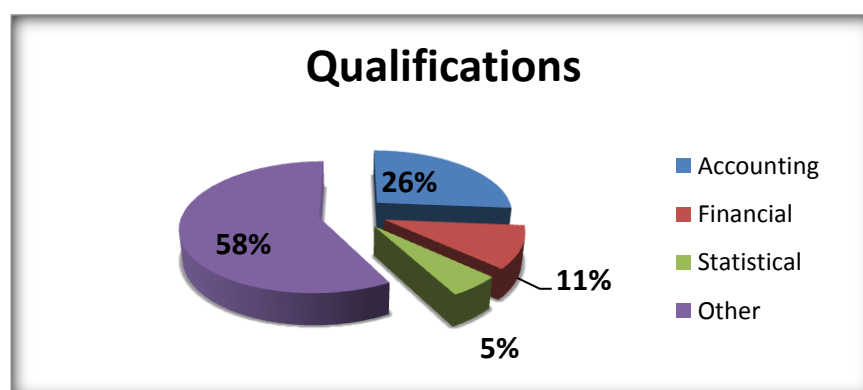
As stated previously, the five participating banks were requested to distribute the scenarios questionnaire to at least three operational risk experts within the operational risk areas of the bank. The purpose of this questionnaire was to obtain an understanding of how risk experts currently view typical boundary event risk scenarios, and also how they approach the classification thereof.

5.10.1. Demographics

It is imperative to provide background as to the demographics of the respondents to these questionnaires. This information will not be utilised in performing comparative analysis between demographics (for example knowledge, experience and qualification) and the responses received in the boundary event scenarios questions. The reason for this is that an approach, or approaches, to the classifications of the various boundary event scenarios are merely set forth. At no point is a correct or incorrect answer provided.

5.10.1.1. Qualifications

The respondents to the Boundary Event Scenarios Questionnaire comprise of a diverse and wide variety of qualifications. Of all the respondents, 5% indicated that they have a statistical qualification. There were 11% of the respondents who have a financial qualification. Qualifications here include Baccalaureus Commericii (B.Com) Financial Management and Masters in Business Administration (MBA) in Financial and Strategic Management. A further 26% of respondents have an accounting background, specifically being Chartered Accountants (CA) and the remaining 58% of respondents have other types of qualifications. These include broadly degrees in mathematics, computer science, risk management, law and human movement studies. Refer to Figure 5.17 for an illustration of the qualification demographics of the respondents.

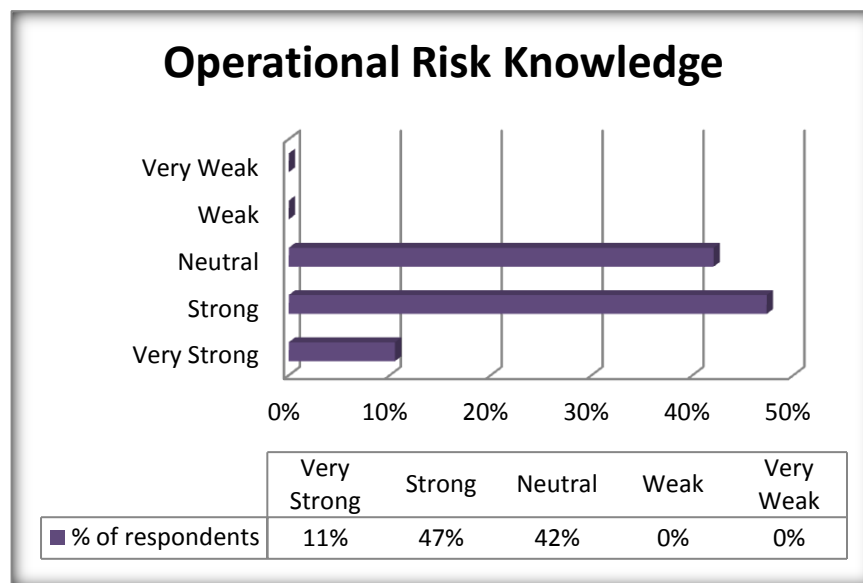


Source: Compiled by the author

Figure 5.17: Qualifications of respondents.

5.10.1.2. Knowledge and experience

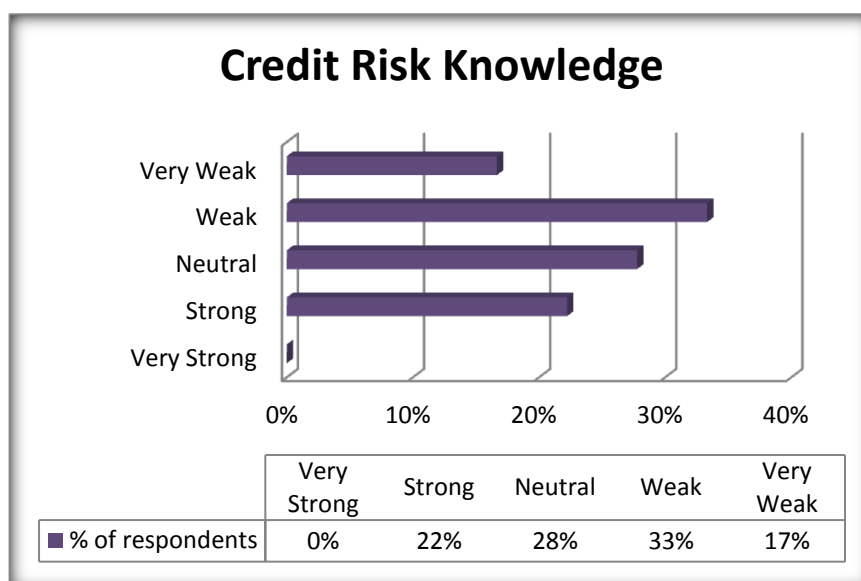
Banks participating in this study were requested to distribute the Boundary Events Scenarios Questionnaire to key operational risk stakeholders within the organisation. Each respondent had to provide information on how well they would rate their level of knowledge in Basel II operational risk, and Basel II credit risk respectively. Of all the respondents, 47% indicated that they have a strong level of knowledge in Basel II operational risk. A further 11% believe that their knowledge in Basel II is very strong, whereas 42% believe that they have a neutral knowledge and understanding of Basel II operational risk. This is illustrated in Figure 5.18.



Source: Compiled by the author

Figure 5.18: Operational risk knowledge of respondents.

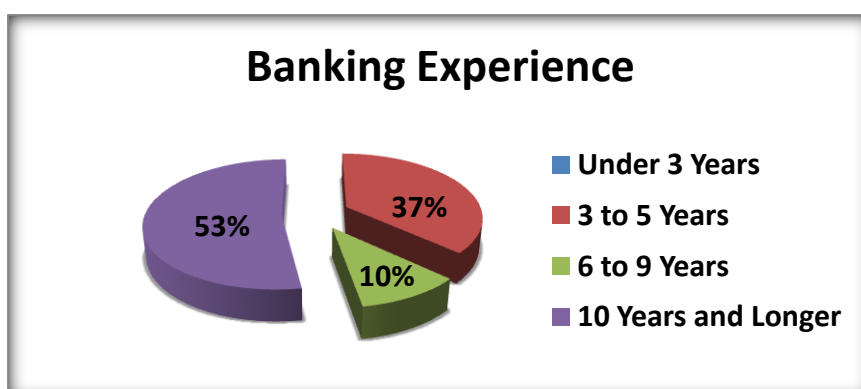
As illustrated in Figure 5.19, in terms of Basel II credit risk knowledge, none of the respondents believe that they have a very strong level of knowledge and experience. There were 22% who feel they have a strong level of knowledge of Basel II credit risk, whereas 28% of respondents believe they have a neutral understanding. Of all the respondents, 33% indicated that they have weak Basel II credit risk knowledge, and 17% have a very weak Basel II credit risk knowledge.



Source: Compiled by the author

Figure 5.19: Credit risk knowledge of respondents.

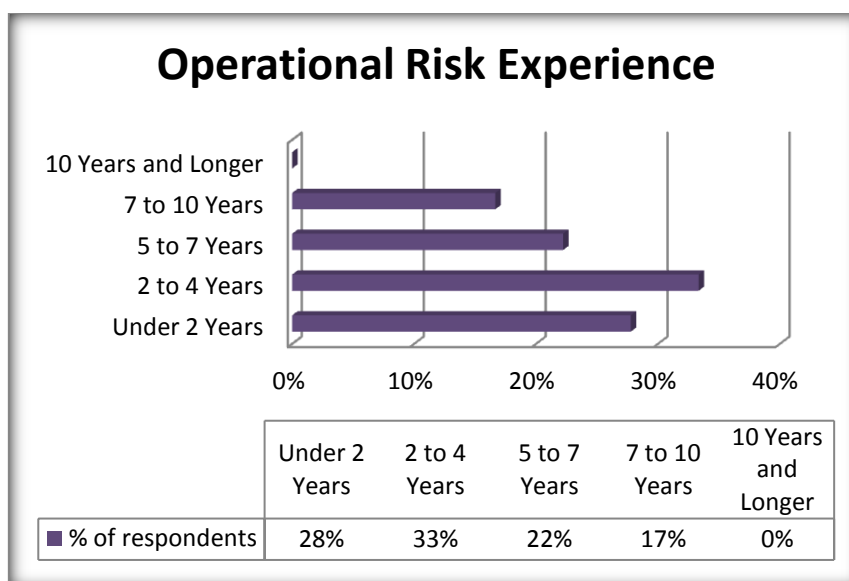
Respondents were also asked to indicate the total number of year's employment and experience in the banking industry. More than half of the respondents have more than 10 years of experience in the banking industry. There were 37% of respondents who have three to five years' experience, and the remaining 10% of respondents have six to nine years of experience in the banking industry. Refer to Figure 5.20 for a depiction of these results.



Source: Compiled by the author

Figure 5.20: Banking employment and experience of respondents.

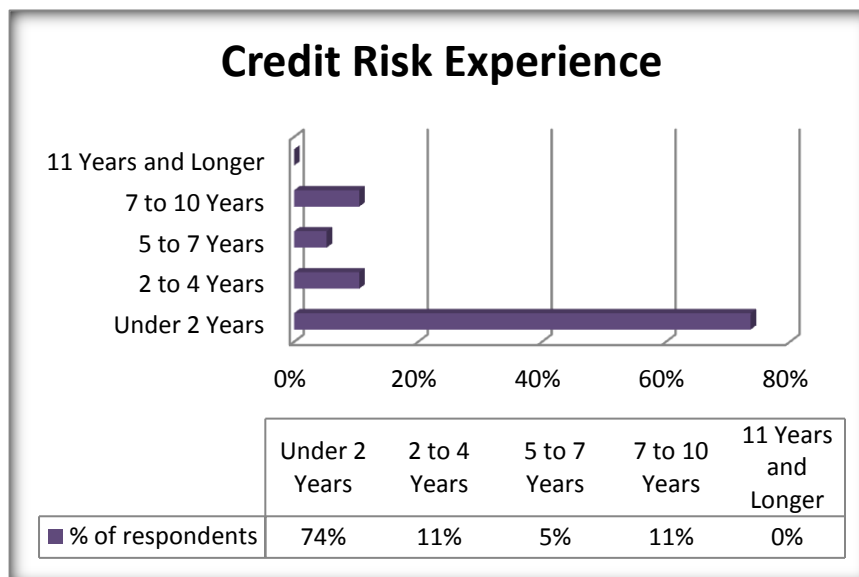
In terms of the level of operational risk experience of the respondents, most of the respondents have two to four years' experience in operational risk, being 33%. A further 28% of respondents have less than two years' experience in this risk type. Also, 22% of respondents have five to seven years' experience; 17% of the respondents have the longest time of experience, being seven to ten years. Figure 5.21 illustrates the operational risk experience of the respondents.



Source: Compiled by the author

Figure 5.21: Operational risk experience of respondents.

As per the illustration in Figure 5.22, most of the respondents do not have a high level of experience in credit risk. Of all the respondents, 74% have less than two years of experience, whereas 11% of respondents have two to four years and seven to ten years of experience in credit risk respectively. A further 5% of the respondents have five to seven years' experience in credit risk.



Source: Compiled by the author

Figure 5.22: Credit risk experience of respondents.

The operational risk managers were asked to submit the questionnaires to employees in their environment that they view as experts in risk management. Based on the results, respondents to the questionnaires feel that they have a strong level of knowledge of Basel II operational risk. There were respondents that believe their level of knowledge of Basel II credit risk is strong, but they mostly feel

their Basel II credit risk knowledge is neutral or weak. More than half of the respondents have more than 10 years of experience in the banking industry. Most of the respondents have two to four years experience in operational risk and less than two years experience in credit risk.

5.10.2. Boundary event scenarios

As discussed earlier, the purpose of the Boundary Event Scenarios Questionnaire was to obtain an understanding of how risk management specialists approach the classification of typical, and frequently found typical loss-event scenarios. A total of 16 typical loss-event scenarios are put forth. The results obtained in this section of the Boundary Event Scenarios Questionnaire are discussed in the sections that follow.

5.10.2.1. Boundary event scenarios – consistency of responses

In order to test the consistency and reliability of the responses to the categorisation of the 16 scenarios in the Boundary Event Scenarios Questionnaire, Cronbach's α values were calculated. Cronbach's α , a coefficient of internal consistency, is utilised for measuring the degree to which the questions in a questionnaire reflect the same underlying constructs; it also measures the degree to which the questions are homogeneous (Cooper & Emory, 1995:155).

Cronbach's α coefficient varies between 0 and 1. An $\alpha > 0.7$ indicates an acceptable level of reliability of the data, and the internal consistency thereof (Santos, 1999). This value for the 16 scenarios is 0.81. It can therefore be concluded that the risk descriptions and scenarios posed to the respondents effectively analyse the approach of the operational risk experts to risk classifications.

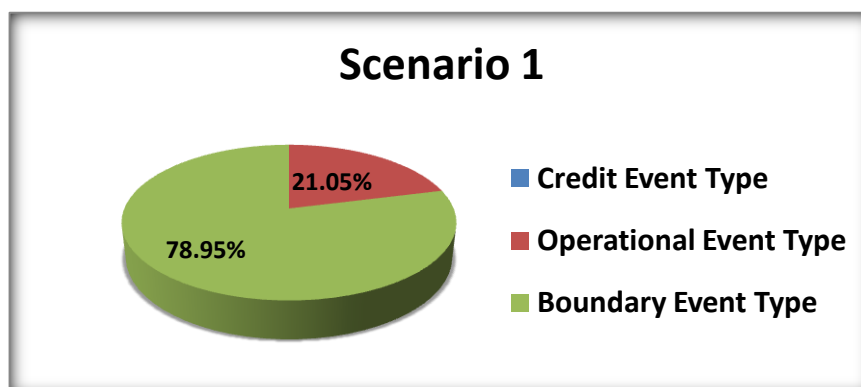
In the sections that follow, each boundary event scenario, as set out in the questionnaire, is set out together with the results obtained for each scenario. A pie chart is presented for each scenario in order to provide the classifications that were obtained from all the respondents. Thereafter, a breakdown is provided for each classification category (that is, for credit risk, operational risk and boundary event separately), that shows how the respondents logged the losses for each instance of classification. These breakdowns should ultimately amount to 100% of all the responses obtained. Subsequently, losses in the boundary event scenarios are categorised and classified by utilising the decision tree proposed in Section 4.4. The raw data of responses received for the sixteen scenarios are set out in Appendix 4.

5.10.2.2. Scenario 1

The bank has granted Client A a credit card facility of R10 000. This overdraft facility has been approved by the bank's application scorecard, and has been sanctioned adequately and properly. Client A goes to the ATM to withdraw money. The exposure of R10 000 to the client on the credit card has already been reached, and the client attempts to withdraw R4 000 from the ATM. The system

should automatically reject this request, but due to an error, Client A receives the R4 000 and the account is overdrawn above the agreed limit. Credit staff at the bank does not follow up on this overdrawn facility and Client A defaults on his exposure to the bank.

Figure 5.23 illustrates the responses received for scenario one.



Source: Compiled by the author

Figure 5.23: Scenario one - classification responses.

Boundary event type. The 78.95% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 36.84% classified this event as a boundary event type and said that the boundary event portion of the loss is R4 000 and the credit risk portion of the loss is R10 000. These respondents made up the majority of the respondents. It can be assumed that the respondents attributed the R10 000 to purely credit risk; these respondents might feel that the R10 000 portion of the loss contained no element of operational risk. The R4 000 was seen as the portion that is classified as the boundary event, whereas an operational element, namely a system breakdown, was responsible for this portion of the loss. This amounts to a total loss of R14 000.

Of all the respondents, 10.53% of the respondents said that the full loss of R14 000 is classified as the boundary event portion. These respondents might have felt that – as the client defaulted – and there was an operational risk element involved in the loss to this specific entity, the total loss amount of R14 000 should be classified as a boundary event.

Some respondents said that R4 000 of the full loss is attributable to operational risk whereas R10 000 is attributable to credit risk. These respondents amounted to 10.53% of all the respondents. The respondents saw the R4 000 loss as an operational risk loss, as this is the portion of the loss where the operational element was involved. The R10 000 was seen as a pure credit risk loss.

There were 10.53% of the respondents who viewed R4 000 as the boundary event portion, and did not attribute any other losses to credit risk or operational risk.

Of all the respondents that classified this loss as a boundary event type, 5.26% said that the R14 000 loss is attributable to credit risk, whereas the boundary event portion is R4 000. The respondents here viewed the complete loss as a credit risk loss, whilst attributing R4 000 to the boundary portion, where the operational element was involved.

5.26% of the respondents viewed R10 000 as the boundary event portion. The respondents in this category did not attribute any other portion of the total loss to another risk type.

Operational event type. The portion of respondents that classified this event type as a boundary event type was 78.95%. The specific loss indications of the 78.95% of respondents were set out above. The remaining portion, which is 21.05%, felt that this loss is purely due to operational risk. These respondents attributed R4 000 of the loss to operational risk. The full loss was not logged by these respondents, but they did attribute the R4 000 loss portion to operational risk – that is, the portion of the loss where the operational element of a system breakdown was involved.

In terms of the decision tree that was proposed in Section 4.4.8, an approach to the classification of this type of loss event can be suggested. Note that no “right” or “wrong” answer is provided. This is merely a guideline and suggestion in terms of the research conducted and the decision tree proposed in Table 4.10. As per the decision tree, the steps (in Table 4.10) can be followed for guidance through the decision process. Refer to Table 5.1.

Table 5.1: Decision tree steps for scenario one.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R14 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Partially.	R10 000	Client failing to meet obligations.	CREDIT RISK
			R4 000	System failure of the ATM.	OPERATIONAL RISK ²⁴
F	Was an operational factor responsible for the entire loss?	No. The operational factor was responsible for R4 000 of the total loss.	R4 000		
H	- The total loss amount of R14 000 should be captured and capitalised as a credit risk loss. - The portion of the loss attributable to the operational risk element – in this instance, R4 000 – should be flagged as a boundary event in the operational risk system of the bank. - Depending on the policy of the bank, the entire loss of R14 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

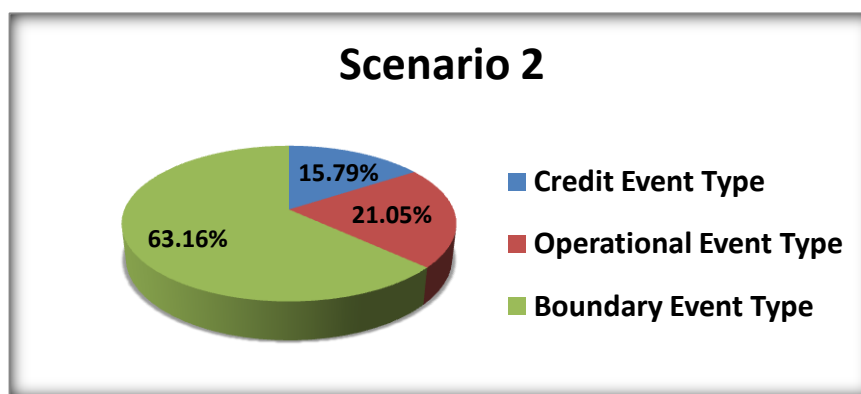
²⁴ The “operational risk” highlighted in red, indicates a boundary event.

Source: Compiled by the author

5.10.2.3. Scenario 2

Client B has been granted an overdraft facility of R40 000. This overdraft facility has been approved by the bank's appropriate application scorecard, and has been adequately and properly sanctioned. Client B overdraws this facility to R60 000 and Client B is therefore R20 000 over his approved and agreed limit. Credit staff at the bank aims to follow up on the overdrawn facility and Client B cannot be reached due to insufficient client details on the system. The client defaults on the amount of R60 000.

Figure 5.24 provides the results received in terms of the classification for scenario two.



Source: Compiled by the author

Figure 5.24: Scenario two - classification responses.

Boundary event type. The 63.16% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 31.58% said that R40 000 of the loss is due to credit risk, whilst R20 000 is a boundary event portion. The view can be that the R40 000 would have been a credit loss anyway, should the client not have overdrawn his facility. The R20 000 could have been prevented had the staff followed up on this overdrawn facility, and had the client's details on the system been sufficient for follow-up.

There were 26.32% of respondents that said that the full loss of R60 000 is classified as the boundary event portion. These respondents might have felt that, as the client defaulted, and there was an operational risk element involved in the loss, the whole loss amount of R60 000 should be classified as a boundary event.

Finally, the remaining 5.26% of all the respondents that classified the loss as a boundary event type, said that R20 000 of the full loss is attributable to operational risk whereas R40 000 is attributable to credit risk. These respondents saw the R20 000 loss as an operational risk loss, as this is the portion of the loss where the operational element was involved.

Credit event type. There were 15.79% of respondents that said that this loss is a credit risk loss. Of all the respondents, 10.53% attributed the whole loss of R60 000 to pure credit risk. As this is a client default, the respondents felt that this is a credit risk loss event. The remaining 5.26% of these respondents felt that R20 000 of the total loss is due to credit risk.

Operational event type. There were 21.05% of the respondents who felt that this loss is due to operational risk. Of all the respondents, 15.79% attributed only the R20 000 to operational risk. The additional loss of R20 000 was due to operational failure, and therefore these respondents might have felt it appropriate to classify this portion as operational risk. The remaining 5.26% of the respondents said that the event is purely an operational risk event type, but classified the R60 000 loss as a boundary event loss.

The steps for the decision process are stipulated in Table 5.2.

Table 5.2: Decision tree steps for scenario two.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R60 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Partially.	R40 000	Client failing to meet obligations.	CREDIT RISK
			R20 000	Inadequate client information.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	No. The operational factor was responsible for R20 000 loss of the R60 000 loss.	R20 000		
H	- The total loss amount of R60 000 should be captured and capitalised as a credit risk loss. - The portion of the loss attributable to the operational risk element (R20 000) should be flagged as a boundary event in the operational risk system of the bank. - Depending on the policy of the bank, the entire loss of R60 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

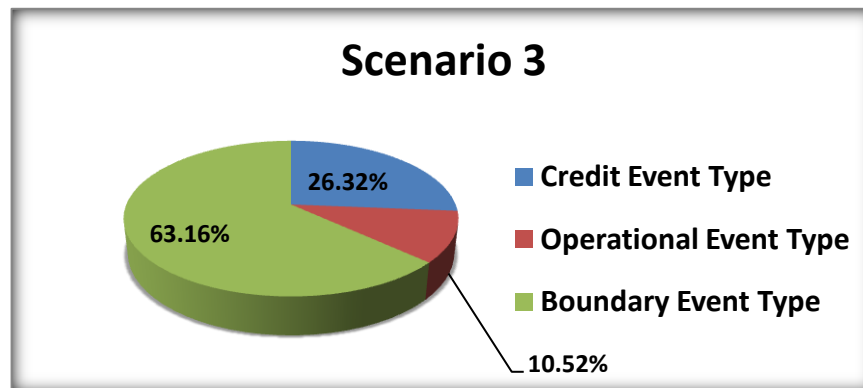
Source: Compiled by the author

There is, however, another interpretation of the loss description for this loss scenario. The description of this loss event states that the client's details on the system were not sufficient. Should the credit staff have been able to reach the client, the total loss of R60 000 might have been recovered. In light of this interpretation, the total loss amount of R60 000 can be viewed as containing an operational risk element.

5.10.2.4. Scenario 3

Client C has been granted an overdraft facility of R50 000. The facility has gone through proper and adequate approval processes. During the 5th month, the R50 000 facility is overdrawn to an amount of R90 000. The credit team failed to report the account as overdrawn, and at the end of the 6th month, no risk triggers were identified. In the 9th month, the facility is overdrawn to R120 000. A liquidator was appointed, and only then was the position realised by the credit team.

In Figure 5.25, the respondents' approach to the risk classification of scenario three is illustrated.



Source: Compiled by the author

Figure 5.25: Scenario three - classification responses.

Boundary event type. The 63.16% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 36.84% believe that R50 000 of the total loss of R120 000 is due to pure credit risk, and R70 000 of the total loss is a boundary event. These respondents might believe that the client would have defaulted on the R50 000 anyway – therefore being a pure credit risk loss event – while the R70 000 could have been recovered, had credit staff at the bank reported the account and investigated the overdrawn facility.

Furthermore, 10.53% believe that the total loss of R120 000 was due to a boundary event that took place. These respondents therefore believe that the full loss was due to the fact that credit staff did not follow up on the overdrawn facility.

Of all the respondents, 5.26% believe that the total loss of R120 000 was due to pure credit risk, whereas R70 000 of the loss is due to a boundary event. These respondents might have recognised the fact that the complete loss of R120 000 is a credit risk event, whereas the R70 000 portion was exacerbated by an operational risk element, and therefore should be flagged as a boundary event.

A total of 5.26% of all the respondents attributed R70 000 of the loss to a boundary event taking place. Finally, the remaining 5.26% of respondents that classified this event as a boundary event type,

classified R30 000 of the loss as an operational risk loss, R40 000 of the total loss as a credit risk loss, and R70 000 as a boundary event.

Credit event type. The 26.32% of respondents that believe that this is a credit risk loss believe that the total loss of R120 000 was due to pure credit risk. The respondents might feel that an operational element was not responsible in the loss event that took place, and therefore attributed the full loss to pure credit risk.

Operational event type. The 10.52% of respondents that believe that this is an operational risk loss indicated the losses as follows. Of all the respondents, 5.26% believe that the total loss of R120 000 is due to operational risk and the remaining 5.26% of the respondents believe that R70 000 is due to operational risk.

Table 5.3 presents the steps that can be followed through the decision process.

Table 5.3: Decision tree steps for scenario three.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R120 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Partially.	R50 000	Client failing to meet obligations.	CREDIT RISK
			R70 000	Credit staff failing to follow up on overdrawn facility.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	No. The operational factor was responsible for R70 000 loss of the R120 000 loss.	R70 000		
H	- The total loss amount of R120 000 should be captured and capitalised as a credit risk loss. - The portion of the loss attributable to the operational risk element (R70 000) should be flagged as a boundary event in the operational risk system of the bank. - Depending on the policy of the bank, the entire loss of R120 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

Source: Compiled by the author

Here, the assumption is made that the client would have defaulted anyway, and that R50 000 of the R120 000 loss was due to the client failing to meet obligations, and the additional R20 000 loss was due to the inadequate staff practices. Once again in this risk scenario, appropriate and sufficient detail

is required in order to draw accurate conclusions of the loss event, and what occurred. Only then, can one be sure that an accurate conclusion is reached with regards to the loss event and its classification.

5.10.2.5. Scenario 4

Client D is granted an overdraft facility of R25 000, which has been approved by the application scorecard and adequately and properly sanctioned. The facility of R25 000 is fully drawn. Credit staff follows up on the drawn facility, and it is discovered that Client D is not able to repay the R25 000 that has been granted.

All the respondents believe that this loss is purely due to credit risk.

Table 5.4 provides guidance through the risk classification decision process.

Table 5.4: Decision tree steps for scenario four.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R25 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	No element of operational risk is mentioned.			
E	The total loss amount of R25 000 should be captured and capitalised as a credit risk loss.				

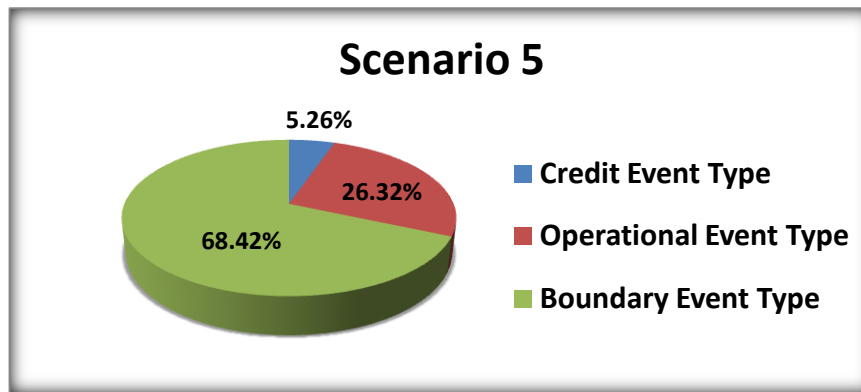
Source: Compiled by the author

Once again, adequate and appropriate information regarding the loss event is required. The capturer of the losses should ensure that no element of operational risk is involved in this event, in which instance an amount should be flagged as boundary.

5.10.2.6. Scenario 5

Client E owes the bank an amount of R200 000, and subsequent to investigations, the client is not able to repay the amount. The credit risk officer responsible for this client is aware of sufficient collateral supplied by the client, as this has been discussed with the client, and also mentioned on the sanctioning documents. This documentation is, however, missing and therefore it is impossible for the bank to take advantage of the collateral.

Figure 5.26 illustrates the responses received for scenario five.



Source: Compiled by the author

Figure 5.26: Scenario five - classification responses.

Boundary event type. The 68.42% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 57.89% believe that the total loss of R200 000 is attributable to a boundary event. These respondents therefore believe that the full loss is a credit risk loss, caused by an element of operational risk.

Also, 10.53% of all the respondents believe that R200 000 is due to pure credit risk, and that R200 000 is attributable to a boundary event. These respondents might recognise the fact that R200 000 is a credit risk loss, whilst also keeping in mind that an operational element was involved, leading to the R200 000 also being flagged as a boundary event in the operational risk system.

Operational event type. The 26.32% of respondents that believe that this is an operational risk loss event indicated that the full loss of R200 000 is due to pure operational risk. These respondents therefore do not recognise any element of credit in the loss, and feel that the full loss is purely due to operational risk.

Credit event type. The 5.26% of respondents that believe that this is a credit risk loss, said that the R200 000 is a pure credit risk loss. These respondents therefore did not recognise any element of operational risk in this loss event.

Table 5.5 provides guidance in terms of the decision process for scenario five.

Table 5.5: Decision tree steps for scenario five.

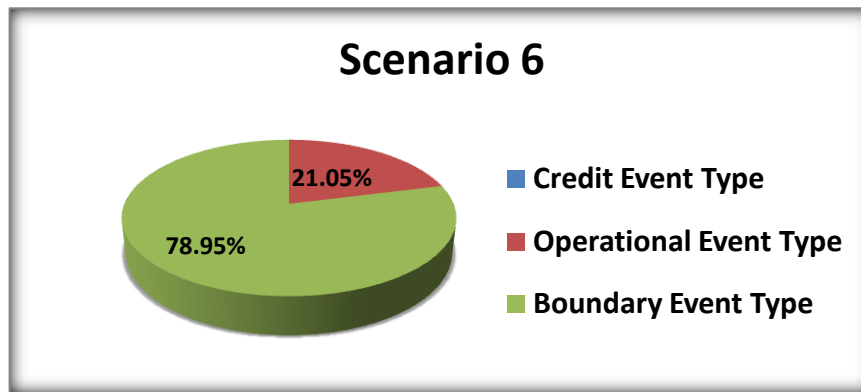
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R200 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R200 000	Collateral documentation was missing.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	Yes. The operational factor was responsible for the R200 000 loss.	R200 000		
H	- The total loss amount of R200 000 should be captured and capitalised as a credit risk loss. - The portion of the loss attributable to the operational risk element (which is the full loss of R200 000) should be flagged as a boundary event in the operational risk system of the bank. - Depending on the policy of the bank, the entire loss of R200 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

Source: Compiled by the author

5.10.2.7. Scenario 6

Client F is granted an overdraft facility of R10 000. The facility has been approved by the application scorecard and adequately sanctioned. When the facility amount was however captured, it was captured incorrectly as R100 000. The client does not qualify for this incorrectly captured limit. The limit of R100 000 is fully drawn, and Client F has defaulted on this amount as she is unable to repay the amount.

Figure 5.27 illustrates the approach of the respondents to the classification of scenario six.



Source: Compiled by the author

Figure 5.27: Scenario six - classification responses.

Boundary event type. The 78.95% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 42.11% believe that R90 000 of the total loss is a boundary event, whereas R10 000 is due to pure credit risk. These respondents might feel that the client might have defaulted on the R10 000 loss due to pure credit, and that the R90 000 additional loss was due to the operational element of the incorrectly captured amount.

A further 21.05% of all respondents believe that the full loss of R100 000 is attributable to a boundary event. These respondents might feel that an operational element was responsible for the full loss amount of R100 000. In addition, 5.26% of all the respondents view the R100 000 as a credit risk loss, but also as a boundary event type, whereas another 5.26% believe that R100 000 is an operational risk loss, but also a boundary event type. Finally, there were 5.26% of respondents that felt that R100 000 is a pure operational risk loss.

Operational event type. The 21.05% of respondents that believe that this is an operational risk loss event indicated the losses as follows. Of all the respondents, 15.79% feel that the full loss of R100 000 is due to pure operational risk. These respondents therefore did not recognise the line of credit risk in this loss event. The remaining 5.26% of respondents viewed the amount of R90 000 as pure operational risk, therefore also not recognising an element of operational risk involved in this event.

As per the decision tree presented earlier in this paper, Table 5.6 proposes steps that can be followed to assist in the decision process for classifying the loss in scenario six.

Table 5.6: Decision tree steps for scenario six.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R100 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Partially.	R10 000	Client failing to meet obligations.	CREDIT RISK
			R90 000	Human error.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	No. The operational factor was responsible for R90 000 loss of the R100 000 loss.	R90 000		
H	- The total loss amount of R100 000 should be captured and capitalised as a credit risk loss. - The portion of the loss attributable to the operational risk element (R90 000) should be flagged as a boundary event in the operational risk system of the bank. - Depending on the policy of the bank, the entire loss of R100 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

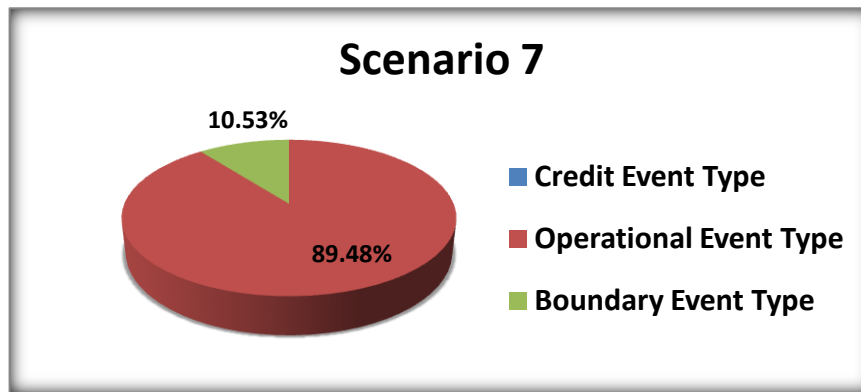
Source: Compiled by the author

Once again, it should be ensured that adequate information is available prior to making decisions or assumptions on loss classifications. The assumption was made here that the client would have defaulted on the original R10 000 anyway, in which case the R10 000 loss is pure credit risk. Another option might be that the bank would have been able to recover the R10 000 loss from the client. Part of the R10 000 might also have been recovered. This would have caused the loss classification and loss amounts captured to be significantly different. Accurate and adequate information is therefore of importance.

5.10.2.8. Scenario 7

Client G is a good customer of the bank, and deposits a cheque of R300 000 into his account. The cheque is returned unpaid as fraud. It turns out that this is a stolen Zimbabwean cheque. The cheque was also wrongly cleared by the bank. Client G is not aware or responsible for the fraud, but the bank is however facing a loss. The client used all of the funds and subsequently the bank had to take legal action in order to recover the loss/part of the loss. Subsequently, appropriate recovery procedures were followed and an amount of R220 000 was recovered.

Figure 5.28 presents the responses received for scenario seven.



Source: Compiled by the author

Figure 5.28: Scenario seven - classification responses.

Operational event type. The 89.48% of respondents that believe that this is an operational risk loss event indicated the losses as follows:

Of all the respondents, 63.16% of all the respondents feel that the R80 000 loss is due to pure operational risk. These respondents therefore did not recognise an element of credit risk in this loss event.

A further 15.79% of all the respondents feel that R300 000 is due to pure operational risk, while 10.53% of the respondents feel that R220 000 is due to pure operational risk.

Boundary event type. The 10.53% of respondents that believe that this is a boundary event loss indicated that the full loss of R80 000 is attributable to a boundary event. These respondents might therefore feel that this is a credit-related loss that was caused by an operational risk element.

Table 5.7 provides guidance in terms of the decision process for this scenario.

Table 5.7: Decision tree steps for scenario seven.

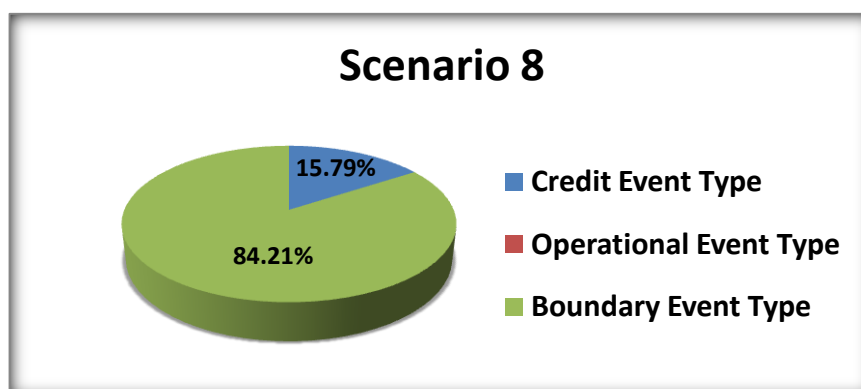
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	No.			
B	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R300 000, of which R220 000 was recovered, therefore amounting to R80 000.	Human error.	OPERATIONAL RISK ²⁵
D	The total loss amount of R80 000 should be captured and capitalised as an operational risk loss.				

Source: Compiled by the author

5.10.2.9. Scenario 8

Within the last few months the bank has faced several legal issues and challenges, which were of a similar nature. Subsequent to several investigations, it was discovered that the standard security documentation, which has been updated recently, contained vague and ambiguous terms regarding the security and collateral required for facilities. Consequently, this led to numerous facilities – granted subsequent to the documentation being updated – having in place security that could not be taken up as and when required by the bank. The bank suffered losses on a number of drawn and overdrawn facilities that were avoidable. One such incident is where Client K, who has drawn his full facility of R600 000, defaulted on the amount and even though the credit officer was certain of the correct procedures being followed with regards to the collateral for the facility, the full collateral could not be taken up, and covered only R450 000 of the amount owed.

Figure 5.29 serves as an illustration for the responses received for scenario eight.



Source: Compiled by the author

Figure 5.29: Scenario eight - classification responses.

²⁵ As the client did not default, this is not indicated as a boundary event.

Boundary event type. The 84.21% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 47.37% feel that the total loss of R150 000 is a boundary event. These respondents therefore might feel that even though this is a credit-related event, an operational risk element – being inadequate security documentation – was causing the loss.

A further 15.79% of all the respondents feel that a R600 000 loss is due to operational risk, while 10.53% of all respondents feel that a R450 000 loss is due to operational risk. There were 5.26% who feel that the R150 000 loss is due to pure credit risk, and that R150 000 is a boundary event. These respondents might have recognised the fact that the R150 000 loss should be indicated – and therefore capitalised – as credit, but that R150 000 should also be flagged as a boundary event, as the operational element namely inadequate security documentation was involved in the credit loss. Finally, an additional 5.26% of all respondents feel that a R450 000 loss is due to pure credit risk, and R150 000 is a boundary event.

Credit event type. The 15.79% of respondents that believe that this is a credit risk loss indicated the losses as follows:

Of all the respondents, 10.53% feel that the loss of R150 000 is due to pure credit risk. These respondents did not recognise any operational risk element in the loss. The remaining 5.26% of all the respondents feel that a loss of R450 000 is due to pure credit risk.

Refer to Table 5.8 for guidance on the decision process for this scenario.

Table 5.8: Decision tree steps for scenario eight.

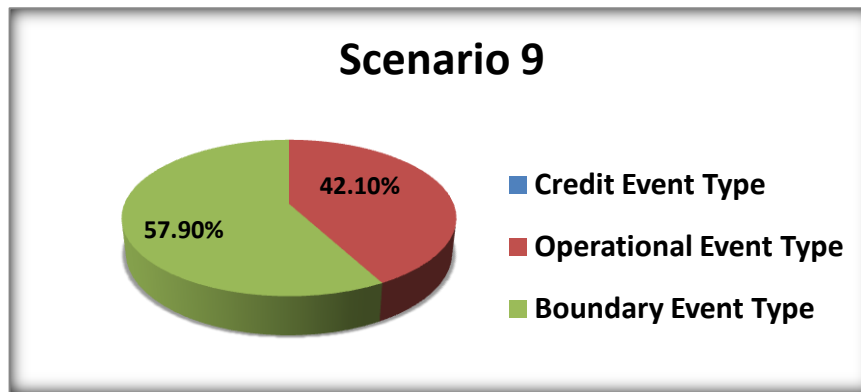
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	The client defaulted on the amount of R600 000, whereof R450 000 was recovered.		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R150 000	Inadequate documentation.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	Yes.	R150 000		
G	- The total loss amount of R150 000 should be captured and capitalised as a credit risk loss. - The R150 000 should be flagged as a boundary event in the operational risk system of the bank, as this loss is attributable to the operational risk element. - Depending on the policy of the bank, the entire loss of R150 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

Source: Compiled by the author

5.10.2.10. Scenario 9

A potential new client, Client H, wishes to open an account at the Sandton City branch. He claims to be representing a well-known company in Sandton. Fraudulent documents are presented, and the credit officer at the branch approves the new account for Client H, together with an overdraft facility of R180 000. It was only discovered after several months that the application by Client H was fraudulent. The credit officer at the Sandton City branch was negligent in the approval of the application, as he assumed the client to represent the well-reputed company and did not go through the appropriate checks and authorisation with regards to the documents presented. Client H has fully drawn the amount of R180 000. The bank managed to possess assets from Client H amounting to R90 000. The remaining R90 000 could not be recovered.

Refer to Figure 5.30 for the responses received for scenario nine.



Source: Compiled by the author

Figure 5.30: Scenario nine - classification responses.

Boundary event type. The 57.90% of respondents that believe that this is a boundary event loss indicated the losses as follows:

Of all the respondents, 47.37% feel that the R90 000 loss is attributable to a boundary event. These respondents therefore might believe that the loss was credit related, but ultimately caused by an operational element, being inappropriate documentation authorisation and checks. Furthermore, 10.53% of all the respondents feel that the amount of R180 000 is attributable to a boundary event.

Operational event type. The 42.10% of respondents that believe that this is an operational risk loss event indicated the losses as follows:

Of all the respondents, 36.84% feel that the R90 000 loss is due to pure operational risk, while 5.26% feel that a R180 000 loss is due to pure operational risk. These respondents did not recognise any credit risk element in the loss event.

Refer to Table 5.9 for guidance through the decision process of classifying the loss in scenario nine.

Table 5.9: Decision tree steps for scenario nine.

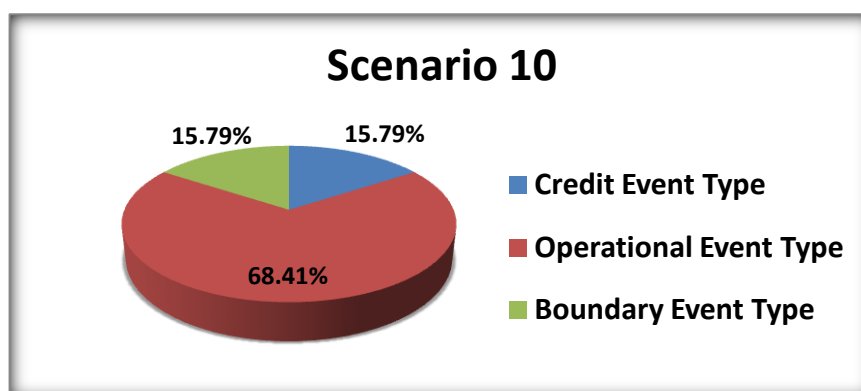
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	The client defaulted on the amount of R180 000, whereof R90 000 was recovered.		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R90 000	Negligent staff.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	Yes.	R90 000		
G	- The total loss amount of R90 000 should be captured and capitalised as a credit risk loss. - The R90 000 should be flagged as a boundary event in the operational risk system of the bank, as this loss is attributable to the operational risk element. - Depending on the policy of the bank, the entire loss of R90 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

Source: Compiled by the author

5.10.2.11. Scenario 10

An employee of a big client of the bank, ABS (Pty) Ltd, forged cheques and a letter of authority. The company was defrauded of R5 000 000. The employee has left the company, and ABS (Pty) Ltd only became aware of these fraudulent activities one year later. ABS (Pty) Ltd now claims the full amount of R5 000 000 from the bank. Subsequent to lengthy investigations, the bank's legal advisors and/or Legal Department advise that the bank would certainly be successful in court, as there was no sign of proof of negligence from the bank's side. Subsequent to numerous debates, the Corporate Credit Department decides that, because ABS (Pty) Ltd is a highly reputable company and client of the bank, the bank should protect the highly valuable client relationship. Together with the legal team, the bank decides to pay ABS (Pty) Ltd a goodwill payment that equals 50% of the claimed amount.

Figure 5.31 illustrates the responses that were received for this scenario.



Source: Compiled by the author

Figure 5.31: Scenario ten - classification responses.

Operational event type. The 68.41% of respondents that believe that this is an operational risk loss event indicated the losses as follows:

Of all the respondents, 57.89% believe that the loss of R2 500 000 is due to pure operational risk. No credit risk element has been recognised by these respondents, and they might believe that the external fraud element causes this loss to be viewed as pure operational in nature. There were 5.26% of all the respondents who believe that this loss is not a boundary event, neither operational risk or credit risk related.

The remaining 5.26% of all the respondents believe that a R5 000 000 loss is due to pure operational risk.

Boundary event type. The 15.79% of respondents that are of the opinion that this is a boundary event believe that the total loss of R2 500 000 is a boundary event. These respondents therefore do recognise an operational element together with a credit risk element in this loss event.

Credit event type. 15.79% of respondents that are of the opinion that this loss is purely categorised as a credit risk loss and attribute the R2 500 000 loss to pure credit risk and these respondents therefore do not recognise any operational risk element in this loss.

Table 5.10 provides an approach to the classification of this type of loss event.

Table 5.10: Decision tree steps for scenario ten.

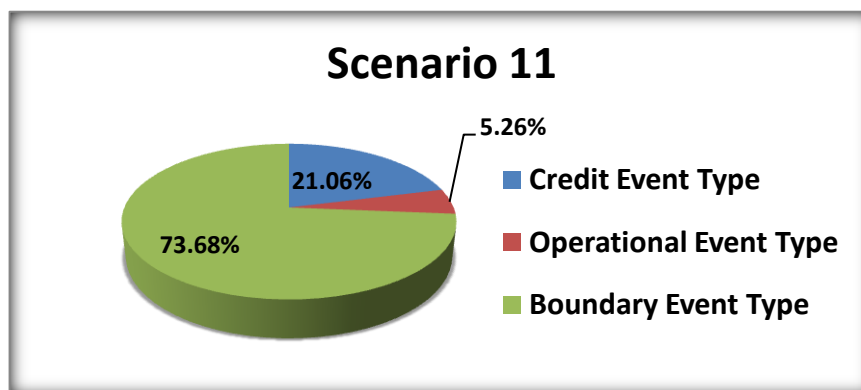
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	No.			
B	Was the loss partially or wholly caused by an operational risk element?	An operational risk element was responsible for the client claiming an amount of R5 000 000 from the bank. The bank paid a goodwill amount of R2 500 000 to the client.	R2 500 000	External fraud.	OPERATIONAL RISK
D	The total loss amount of R2 500 000 should be captured and capitalised as an operational risk loss.				

Source: Compiled by the author

5.10.2.12. Scenario 11

Client M approaches the bank in order to obtain a new credit account. Client M presents the required documents as requested. The client's details are inputted into the bank's scoring model and, even though Client M is a student that works part-time, the scoring model rates him good enough to obtain a facility of R120 000. The credit manager does not realise that there might be a possible error, and the facility is approved by him. Client M draws the facility to the amount of R10 000, and only then is it discovered by the bank that the scoring model was in error, and that Client M is unable to repay the bank the amount of R10 000.

Refer to Figure 5.32 for a representation of the responses received for scenario 11.



Source: Compiled by the author

Figure 5.32: Scenario 11 - classification responses.

Boundary event type. The 73.68% of respondents that believe that this is a boundary event indicated that the R10 000 loss is a boundary event. These respondents might believe that this is a default event,

with an operational element causing the loss. The operational element involved here is a system error by way of the model providing an inappropriate facility; inadequate staff might also be considered as an operational element being responsible for this loss.

Credit event type. The 21.06% of respondents that believe that this is a credit risk loss event indicated that the R10 000 loss is purely attributable to credit risk. These respondents therefore did not recognise an operational risk element in this risk scenario.

Operational event type. The 5.26% of respondents that believe that this is an operational risk loss event indicated that the R10 000 loss is purely due to operational risk. The respondents in this category therefore did not view this loss as containing any element of credit risk.

The steps, as set out in Table 5.11, can be followed for guidance through the decision process.

Table 5.11: Decision tree steps for scenario 11

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R10 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R10 000	Model / system error.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	Yes.	R10 000		
G	- The total loss amount of R10 000 should be captured and capitalised as a credit risk loss. - The R10 000 should be flagged as a boundary event in the operational risk system of the bank, as this loss is attributable to the operational risk element. - Depending on the policy of the bank, the entire loss of R10 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

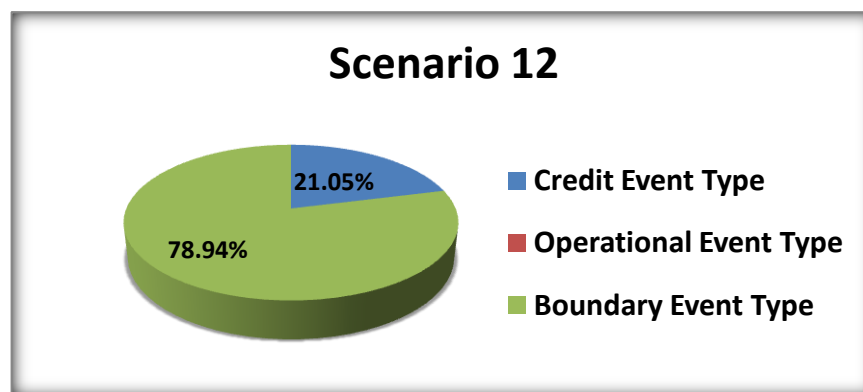
Source: Compiled by the author

In this scenario, it is once again emphasised that adequate information is required in order to adequately and correctly decide on the loss classification. The assumption was made here that the bank was not supposed to grant the facility to the client at all. Another option might be that the appropriate amount that should have been granted, was R2 000. In such an event, R2 000 of the R10 000 would be pure credit risk related, whereas R8 000 would have been due to the operational risk element.

5.10.2.13. Scenario 12

Client P has always had a good relationship with the bank. He has a current facility of R1 000 000. Client P has sufficient collateral and his payments are always up to date. The bank decides to increase Client P's facility to R1 400 000. Due to negligence on the credit manager's side, the client's collateral information is not updated. In the wake of the economic crisis, Client P suffers losses and has to close down his business. His facility was drawn to R1 300 000 and he is able to repay only R1 100 000.

Figure 5.33 provides the feedback obtained in terms of the classification of scenario 12.



Source: Compiled by the author

Figure 5.33: Scenario 12 - classification responses.

Boundary event type. The 78.94% of respondents that believe that this is a boundary event indicated the losses as follows:

Of all the respondents, 68.42% believe that the R200 000 loss is a boundary event. These respondents therefore noted that there was both an operational risk element and a credit risk element involved with this loss event.

Also, 5.26% of all the respondents believe that R200 000 is a boundary event, and R200 000 is attributable to pure credit risk. These respondents also recognised both an operational risk element and a credit risk element involved with this loss event.

The remaining 5.26% of respondents believe that R100 000 is a boundary event, and R100 000 is attributable to pure credit risk.

Credit event type. The 21.05% of respondents that believe that this is a credit risk loss event indicated that the R200 000 loss is attributable to pure credit risk. No element of operational risk was therefore recognised by these respondents.

As per the decision tree, certain steps can be followed for guidance through the decision process. Refer to Table 5.12.

Table 5.12: Decision tree steps for scenario 12.

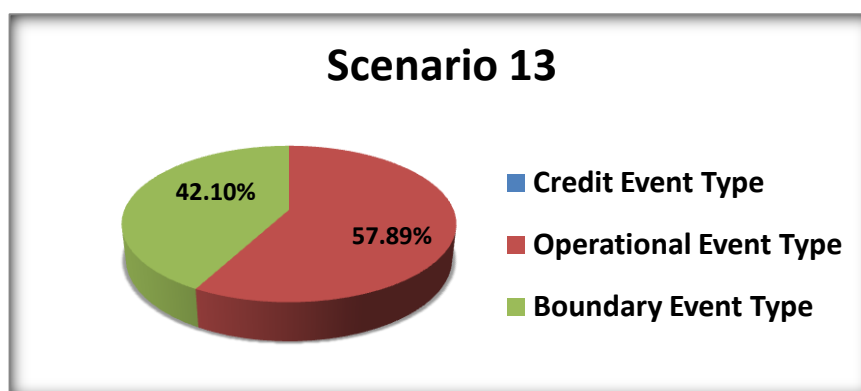
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes	R200 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R200 000	Staff negligence.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	Yes.	R200 000		
G	- The total loss amount of R200 000 should be captured and capitalised as a credit risk loss. - The R200 000 should be flagged as a boundary event in the operational risk system of the bank, as this loss is attributable to the operational risk element. - Depending on the policy of the bank, the entire loss of R200 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

Source: Compiled by the author

5.10.2.14. Scenario 13

Mr X is an employee of the credit division within the bank. A close relative of Mr X, Mr A, applies for a credit card at the Nelspruit branch. Mr A's application for a credit card is successful. Mr X is responsible for capturing Mr A's details on the credit risk system that calculates the approved overdraft facility. Mr A promises to pay Mr X an amount of money for an increased facility on his credit card. Mr X agrees, and by inputting incorrect details, Mr A is granted an overdraft facility of R100 000, which is far above his means and ability to repay. Mr X's manager authorises the facility, and does not pick up on the fraudulent activity and incorrect information entered. A few months later, Mr A defaults on an amount of R80 000.

Refer to Figure 5.34 for the results obtained for scenario 13.



Source: Compiled by the author

Figure 5.34: Scenario 13 - classification responses.

Operational event type. The 57.89% of respondents that believe that this is an operational risk loss event indicated that the R80 000 loss is purely due to operational risk. Therefore, these respondents did not recognise a credit risk element in this loss event.

Boundary event type. The 42.10% of respondents that believe that this is a boundary event indicated the losses as follows:

There were 31.58% respondents who believe that the R80 000 loss is attributable to a boundary event. These respondents recognised the credit risk in this loss event as the client defaulted, but also recognised the operational element, being fraudulent activity. An additional 5.26% of all the respondents believe that R80 000 is attributable to pure credit risk, and R80 000 is attributable to a boundary event. These respondents noted the credit risk in this loss event as a client default was involved; furthermore, an operational element was also recognised. Finally, the remaining 5.26% of all the respondents said that R80 000 is a boundary event loss, but the credit portion is not clear as the original facility was not stated in the risk description.

Table 5.13 illustrates steps that can be utilised to classify the loss in scenario 13.

Table 5.13: Decision tree steps for scenario 13.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R80 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	Wholly.	R80 000	Fraudulent activity.	OPERATIONAL RISK
F	Was the operational factor responsible for the entire loss?	Yes.	R80 000		
G	- The total loss amount of R80 000 should be captured and capitalised as a credit risk loss. - The R80 000 should be flagged as a boundary event in the operational risk system of the bank, as this loss is attributable to the operational risk element. - Depending on the policy of the bank, the entire loss of R80 000 might be reported in the operational risk system of the bank. But this should be merely for reporting purposes, and not for purposes of capitalising the loss amount as operational risk.				

Source: Compiled by the author

Once again, an assumption has been made in this loss scenario, the assumption was that the bank would not have granted this client any facility. Therefore, once again, adequate factual information surrounding the actual events and occurrences of this loss event should be utilised in the classification process.

5.10.2.15. Scenario 14

Client Z is granted a properly approved and sanctioned overdraft facility of R20 000. After several months, the account is highlighted on the system as “dormant”. On further investigation, the credit officer determines that the client is unable to repay the amount of R20 000.

All the respondents believed that this loss is attributable to a pure credit risk event.

Table 5.14 serves as an illustration of the steps that can be utilised to classify the loss in scenario 13.

Table 5.14: Decision tree steps for scenario 14.

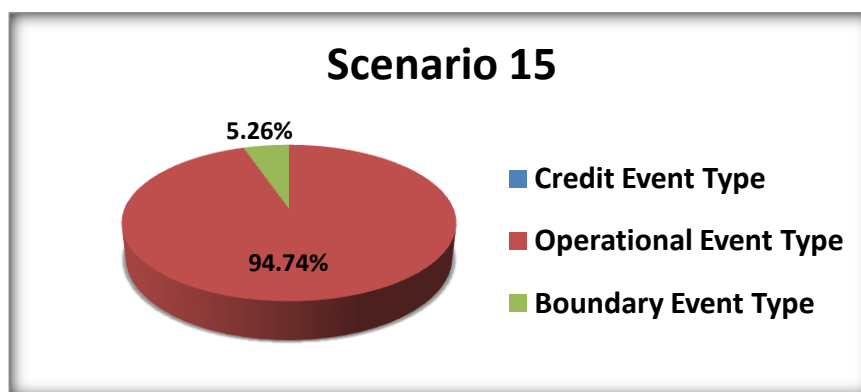
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	Yes.	R20 000		CREDIT RISK
C	Was the loss partially or wholly caused by an operational risk element?	No element of operational risk is mentioned.			
E	The total loss amount of R20 000 should be captured and capitalised as a credit risk loss.				

Source: Compiled by the author

5.10.2.16. Scenario 15

Mrs H is an employee of the bank, and works at the Northgate branch. Mrs H has handled several credit card applications for the day and mistakenly, a number of documents relating to the applications are misplaced between her personal documents and these are packed in her briefcase on her way home. Mrs H becomes a victim of a hijacking that afternoon on her way home, and consequently, her vehicle with her briefcase is stolen. The hijackers got hold of the confidential documents and managed to use the information to withdraw money from two clients' new credit accounts. Subsequently the respective amounts of R10 000 and R3 000 were withdrawn from the clients' accounts.

Refer to Figure 5.35 for a representation of the results received for scenario 15.



Source: Compiled by the author

Figure 5.35: Scenario 15 - classification responses.

Operational event type. The 94.74% of respondents that believe that this loss is due to pure operational risk said that the R13 000 loss is purely classified as operational risk. These respondents therefore did not recognise any element of credit risk in this loss scenario.

Boundary event type. The remaining 5.26% of respondents that classified the loss as a boundary event type, said that the full loss of R13 000 is a boundary event. These respondents therefore recognised credit risk as well as operational risk elements in this loss scenario.

In Table 5.15, the steps to be followed for the decision process are illustrated.

Table 5.15: Decision tree steps for scenario 15.

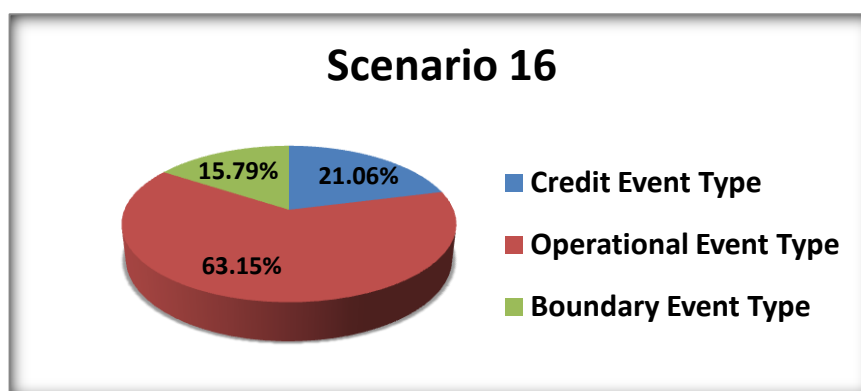
Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	No.			
B	What caused this loss event?	The operational element in this loss event is an external event, namely the hijacking that took place.	R13 000	External event namely hijacking	OPERATIONAL RISK
D	The total loss amount of R13 000 should be captured and capitalised as an operational risk loss.				

Source: Compiled by the author

5.10.2.17. Scenario 16

Unknowingly, Client Q deposited a fraudulent Zimbabwean cheque of R700 000 into his account. The cheque was returned unpaid, with reason: “Stolen cheque”. The client was not part of the fraud. The client also used all the funds. Legal action therefore had to be taken by the bank to recover the loss suffered. R300 000 of the total amount was recovered. The loss subsequent to recovery therefore amounted to R400 000.

Refer to Figure 5.36 for the risk-classification results obtained for this scenario.



Source: Compiled by the author

Figure 5.36: Scenario 16 - classification responses.

Operational event type. The 63.15% of respondents that believe that this is an operational risk loss event indicated that the loss of R400 000 is purely due to operational risk. These respondents did not recognise any element of credit risk in this loss event.

Credit event type. The 21.06% of respondents that believe that this is a credit risk loss event indicated the losses as follows:

There were 10.53% of respondents who attributed the R400 000 loss to pure credit risk, whilst the remaining 10.53% attributed R700 000 to pure credit risk.

Boundary event type. The 15.79% of respondents that believe that this is a boundary event indicated that the loss of R400 000 is a boundary event. These respondents therefore recognised an element of credit risk, as well as operational risk involved in this loss event.

As per the decision tree discussed in Chapter 4, the following steps can be followed for guidance through the decision process. Refer to Table 5.16.

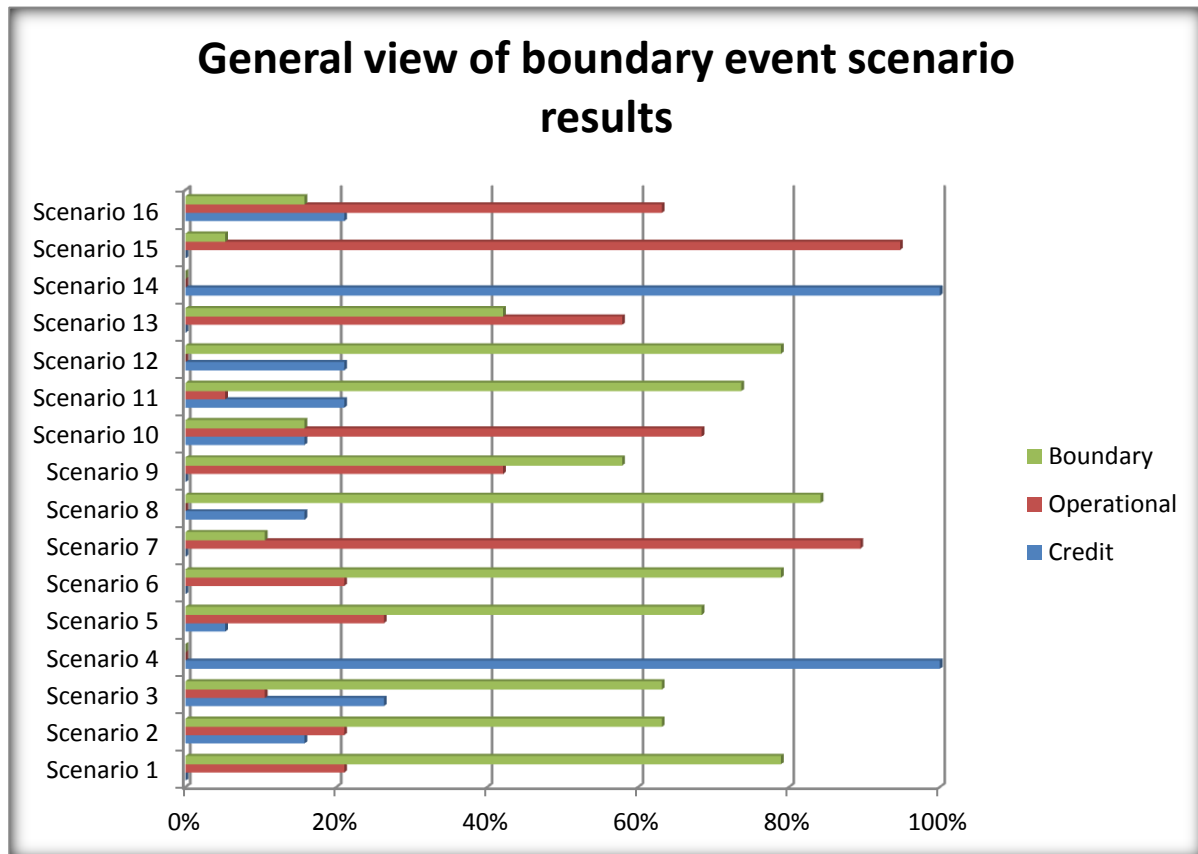
Table 5.16: Decision tree steps for scenario 16.

Step	Question	Response	Loss	Due to	Attributable to
A	Did the client fail to meet obligations?	No.			
B	What caused this loss event?	The operational element in this loss event is an external event, namely fraudulent activity.	R400 000	External event namely fraudulent activity.	OPERATIONAL RISK
D	The total loss amount of R400 000 should be captured and capitalised as an operational risk loss.				

Source: Compiled by the author

5.10.2.18. Boundary event scenarios – uniformity of respondents

In order to obtain a view of the uniformity of respondents with regards to responses received on the risk-type classifications of the boundary event scenarios, the graph in Figure 5.37 can be utilised. Uniform results were only obtained for scenario 4 and scenario 14. For the rest of the results, the views were significantly disparate. The results in Figure 5.38 show the classifications.



Source: Compiled by the author

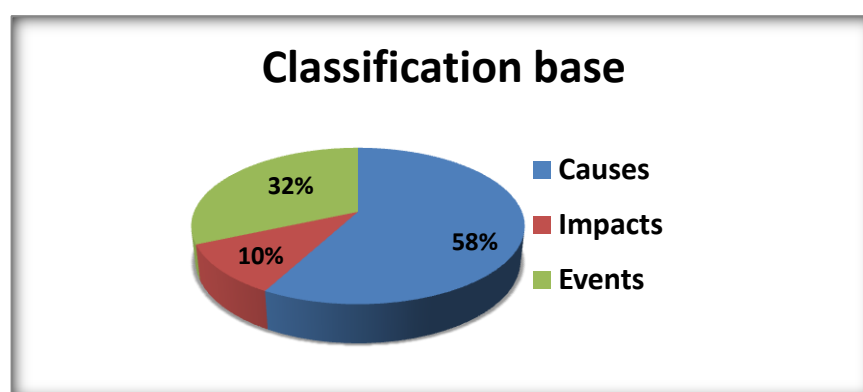
Figure 5.37: Overall view of boundary event scenario responses.

For both scenario 4 and 14, all the respondents indicated a credit risk loss event type. For all the other scenarios, there were different views as to what risk type the loss event was. Within all the classifications, respondents also indicated differing loss amounts as captured and attributed to the various risk types. This has been reported in the tables throughout this chapter.

5.10.2.19. Classification base

There are four attributes, namely *causes*, *events*, *impacts* and *controls* that can be utilised to analyse risks. The question can be asked: Which is the best for classification (Cech, 2007:39)?

The final question was for respondents to indicate which “classification base” was utilised in the classification of the events. 58% of respondents indicated that they utilised causal categorisation as the classification base. 32% indicated that they utilised events, whereas 10% indicated that impacts were used to classify the losses. None of the respondents indicated using controls as a classification base. These results are provided in Figure 5.38.



Source: Compiled by the author

Figure 5.38: Classification base applied for classification.

It is therefore concluded that the majority of respondents utilised causal analysis to approach the boundary event scenarios, and the classification thereof.

5.11. Summary of results

Five South African banks were included in the study to obtain an understanding of banks’ approaches to boundary events. There is some disparity in the tools and/or mechanisms that banks utilise for assisting them in boundary event loss classification. There is, however, uniformity with regards to the use of an incident management lifecycle and a taxonomy of events, in which events all the participating banks indicated that they do utilise these tools. With regards to the use of guidelines, causal categories and decision trees, a greater measure of disparity was observed.

There is extreme disparity in the percentage of gross losses and number of losses that are flagged as boundary. As benchmark, the studies referred to by Adachi in the OpRisk North America Conference in March 2011 were utilised.²⁶ It was stated that boundary losses represent about 30% of total losses, whereas in terms of the value of losses, this share should rise to an amount of about 40% in total. For the purpose of this study, this test was performed for the Retail Banking and Commercial Banking Basel business lines only, and it was found that the average of the responses received (for gross loss amounts) is 33% and 64% for retail banking and commercial banking business lines respectively. For frequency of events, the averages observed were 10% and 21% for retail banking and commercial banking business lines respectively. Together with significant outliers being present, these results are

²⁶ Refer to Section 4.2 for more detail.

not completely in line with the indication provided. In addition, for the retail banking business line, the minimum observation of flagged boundary events in terms of gross losses was 3%, with the maximum being 58%. For the commercial banking business line, the observations were a minimum of 0% and a maximum of 89%. In terms of the frequency of losses, these observations were 0% and 22% for retail banking, and 0 % and 70% for commercial banking.

There are various reasons and considerations as to why the sample specifically, and the time over which the study was conducted, pose some challenges. These include the role that the loss-reporting thresholds play. It was also noted that the banks use different loss-reporting thresholds, with the average being R3 750 for retail banking and R8 750 for commercial banking. The minimum observed thresholds for both these business lines were zero, and the maximum observed thresholds were R10 000 and R20 000 for retail banking and commercial banking respectively. The inclusion or exclusion of provisions in loss reporting can also skew responses observed. In the sample, 25% of banks currently include provisions in their gross loss reporting. The short period over which the study was conducted also has an impact on the observations noted. There might be significant outliers in the data, and the utilisation of a longer period of observation will smooth out the adverse effect of outliers on the data. Most importantly, the tools and mechanisms utilised – or not utilised – by the participating banks play a significant role, and also the extent to and way in which these are implemented and followed.

At least three respondents per bank (and in total, 19 respondents) participated in the boundary events risk scenarios questionnaires. These respondents comprised of a diverse and wide variety of qualifications. There were respondents with, amongst others, statistical, financial and accounting qualifications. There were 47% of respondents that believe they have a strong level of knowledge in Basel II operational risk, and 11% that believe that their knowledge in Basel II operational risk is very strong. None of the respondents believe that they have a very strong level of knowledge and experience in Basel II credit risk, while 22% felt they have a strong level knowledge in Basel II credit risk. More than half of the respondents have more than 10 years of experience in the banking industry. In terms of the level of operational risk experience of the respondents, 33% of the respondents have two to four years' experience in operational risk. Also, 17% of the respondents have seven to ten years' experience. Most of the respondents do not have a high level of experience in credit risk and 74% of respondents have less than two years of experience. These results show that the respondents have a large amount of banking experience, even though all the experience is not necessarily within operational risk.

The results obtained for the boundary event scenarios, as responded to by the operational risk experts, were extremely disparate. The only scenarios that indicated uniform results were scenario four and scenario 14. In addition, within these classifications, respondents also indicated different and disparate loss amounts as captured and attributed to the various risk types. This indicates that there are

significantly different views with regards to the interpretation of the approach to be followed in the classification of boundary events.

Cognisance is taken of the fact that most of the boundary event scenarios put forth in the questionnaire are open to interpretation in various ways, and this can therefore be viewed as a limitation to the study. A great variety of assumptions can be made for most of the boundary event scenarios. The respondents therefore had to make certain assumptions whilst deciding on the risk classifications and loss capturing.

5.12. Conclusion

What approaches do banks currently follow, and which tools and mechanisms do banks utilise to assist them in the classification of boundary events? Banks mostly utilise a taxonomy of events, and an incident management lifecycle is also followed for occurring losses. Some banks utilise causal categorisation, decision trees and approved guidelines. Even though only the AMA banks were included in the data-specific study on the recorded and flagged boundary events, there was extreme disparity in the percentage of gross losses and number of losses that are flagged as boundary events.

It was clear that the respondents to the boundary events scenarios questionnaire have relatively high levels of experience in the banking industry, and in operational risk specifically. The respondents also rated their knowledge in Basel II operational risk as relatively strong, and there was also a big variety of qualification backgrounds. There was, however, still a very high level of disparity with regards to how losses are classified, and where the losses are ultimately recorded within these classifications.

From the significant differences that were noted in the responses received, it can be concluded that banks and individuals are not fully clear and definite about the classification of losses specific to boundary event risk types. The limited guidance put forth by Basel II can also be responsible for uncertainties in this area. Specifically with regards to the boundary event risk scenario descriptions that were put forth, cognisance is taken of the fact that most of the boundary event scenarios in the questionnaire are open to interpretation in various ways. The respondents therefore had to make certain assumptions whilst deciding on the risk classifications and loss capturing. This point emphasises the fact that adequate risk descriptions, loss descriptions and loss event background is required prior to a risk manager capturing information on boundary events.

Proper classification procedures and guidelines for loss events and boundary events specifically, are imperative, as the classification of losses is the final step to the categorisation of the losses for capital purposes. Incorrect classification of losses will lead to incorrect inputs into the capital model. In turn, the calculated capital requirements of the bank will therefore not be a true reflection of the bank's capital cushion in terms of the risks it is facing.

With the results of this study discussed, final conclusions can be drawn and recommendations can be made for banks and financial institutions, and also recommendations for future research. These points are discussed in the next and final chapter.

Chapter 6

Conclusion and Recommendations

6.1. Introduction

Chapter 6 begins with an overview and brief review of the aim of this research project. Thereafter, all the relevant information that was discussed in the previous chapters, is concluded. Firstly, there is an overview of what constitutes credit risk and operational risk respectively, as well as the approaches set forth by Basel II that banks can follow for measuring these risks. Secondly, boundary events are summarised, and the requirements of Basel II and ORX are provided. The various tools and mechanisms that banks can utilise for classifying boundary events are summarised, and a decision tree is proposed for assisting in the process of classifying operational risk losses, credit risk losses or boundary event losses. Thirdly, a view is provided of the various approaches, tools and mechanisms that banks currently utilise to assist them in their classification processes. Fourthly, an idea is put forth of how effectively banks currently classify and capture boundary events. Finally, the measure of uniformity or disparity that currently exists with regards to how operational risk experts approach the classification of typical boundary event losses is given.

6.2. Aim of research project

The aim of this research project was to provide a clear definition of what constitutes credit risk losses and operational risk losses, and to utilise these as a basis for providing a conceptual approach to boundary event losses. As there is currently limited guidance on the issue of boundary events, suitable guidelines were to be provided for banks to classify boundary events. Subsequently, an understanding was to be established of the approach, tools and mechanisms that South African banks currently utilise in their classification processes. An idea was to be obtained as to how effectively banks currently classify boundary events and flag the operational risks existent in these loss events, in their operational risk databases. By utilising general risk scenario descriptions, an overview was to be obtained of the measure of disparity or uniformity that currently exists with regards to how operational risk experts and bank stakeholders approach the classification of boundary events.

6.3. Study review – Credit risk

The concept of capital and the definition thereof, are important considerations when it comes to the concept of the various risks that banks face. Banks mainly have to hold capital for the absorption of the financial risks that they face. Capital serves as a buffer against future, unidentified and unexpected losses. As the classification of losses has an impact on regulatory capital, it is at the core of this study. There are two approaches prescribed by the BCBS for credit risk measurement namely the TSA and AIRB, with the AIRB approach intended for banks that meet more rigorous reporting standards. The

AIRB provides banks with the flexibility of utilising their own estimates for both the risk-weight functions, and credit risk mitigation.

6.4. Study review – Operational risk

This paper focuses on regulatory requirements in terms of boundary events specifically, where the BCBS definition of operational risk is core. The requirement of the BCBS is that unless a bank can demonstrate to the supervisor that it adequately captures expected losses as part of its internal business practices, it will be required to calculate its regulatory capital requirement as the sum of unexpected loss and expected loss. The various approaches that the BCBS makes available for the calculation of operational risk capital include the BIA, TSA and the AMA. There are general criteria and standards in the Basel II Framework for the implementation of the AMA specifically. There is an approach, consisting of two steps out of which a bank can construct an operational risk framework under the AMA. The first phase is where a foundation is developed for the future use of AMAs, and the second phase entails the modelling of the losses.

6.5. Study review – Boundary events

Literature, as well as guidance from the BCBS on the topic of boundary events is extremely limited. This topic is relevant, as boundary events between credit risk and operational risk are a great source of concern for the industry and for regulators. For the purposes of firm-wide risk management, financial institutions are to identify material boundary event types of losses, and to utilise this information for their overall risk management improvement. The BCBS requires that operational risk losses that are related to credit risk should be treated as credit risk for the purposes of calculating minimum regulatory capital under the Basel II Framework. Such losses will not be subject to any operational risk capital charges. However, for the purposes of internal operational risk management, banks should identify all these material operational risk losses. Such material operational risk-related credit risk losses should be flagged separately within a bank's internal operational risk database. The ORX requirements relating to the classification of boundary events include a list of boundary event examples that can be included in the boundary event reporting processes. The ORX view includes all defaults, whether through process issues, external fraud or modelling errors. According to ORX, fraudulent loans obtained in a fraudulent transaction should be capitalised as credit risk and flagged as an operational risk. A credit default is therefore at the crux of a boundary event, whether it is as a result of a client of the bank failing to meet obligations, or a fraudulent client misrepresenting herself, and then also failing to meet obligations. There are, however, various views on which of these fraud-related events are to be logged as boundary events. The boundary defining credit losses may be decided on differently in financial institutions for the same type of loss. Therefore, the interpretation of specific events, such as, for example, fraudulent activity on credit cards and identity theft, is not only specific to a bank or firm, but it is also accounting standard dependent. This is clear in the

guidance provided by the IASB: when considering the accounting standards, a loss should be recognised and written off as credit risk only once the loss event has occurred, irrespective of any other events that might have occurred prior to the loss event.

There are various aspects to consider when performing risk classifications. These include, amongst others, loss or risk frameworks (or taxonomies), causal categories, and controls. Through consideration of these aspects, a decision tree is proposed that a financial institution can utilise to simplify the thought process and the approach to the boundary event loss classification process.²⁷ As stated above, the existence of a credit default is core to the identification of a possible boundary event, and the proposed decision tree is based on this view.

6.6. Study review – The approaches that banks currently utilise for classification

The various tools or mechanisms that can be utilised for classification (for purposes of this study), include classification schemes (or taxonomies); causes; education of relevant staff members; controls and the use of an incident management lifecycle. The essence lies in considering whether – and to what extent – banks and financial institutions take cognisance of factors such as classification schemes, causal factors and other tools and mechanisms listed above. Importantly, the question still remains: *How do banks currently classify boundary events?* A research methodology was conducted, which enabled an overview of the approach that South African banks currently follow in the classification of boundary events. The research methodology followed entailed the compilation of questionnaires and the distribution thereof to five AMA banks in South Africa. Questions posed to respondents included a number of general qualitative questions pertaining to tools that banks utilise for classification.

There appears to be a wide range of practices applied by South African banks when classifying boundary events. It was noted that not all the banks consistently utilise the following to assist with consistent classification of boundary events:

- formalised and approved guidelines;
- decision trees;
- causal analysis and categorisation.

The key stakeholders in the organisations involved in this study do believe that formalised and approved guidelines have a strong impact on the success or failure of the accuracy of classifications. The majority of respondents believe that decision trees have a strong impact on the success or failure of classification processes, and that the utilisation of causal categorisation has a positive impact on classifications. A point that came through clearly, is that all these respondents believe that trained,

²⁷ A decision tree is discussed and proposed in Section 4.4.7, and the decision tree is set out in Figure 4.5.

knowledgeable and educated staff has a strong impact on the success or failure of the accurate classification of banks' boundary events.

6.7. Study review – The effectiveness of boundary event classification

Questions posed in the questionnaires²⁸ included data-specific questions, the purpose of which was to obtain an understanding of how prudent banks are in the capturing of boundary events. This is mainly based on the indication provided by Sands (2011a), stating that boundary event losses should represent approximately 30% of the total losses. In terms of the value of losses, this proportion should rise to approximately 40% in total. Numerous factors were at play, which had an impact on how meaningfully the results obtained, could be analysed. These factors included, amongst other, the inclusion or exclusion of provisions in loss reporting, the loss-reporting thresholds utilised by the banks, and the extent to which tools and mechanisms are utilised for classification process. Finally, as mentioned above, the training and levels of staff knowledge also plays a strong role. Keeping these challenges in mind, outliers were noted in the responses received, and on average (South African Rand amount), the amount of boundary event losses comprised 33% for retail banking and 64% for Commercial banking. The maximum boundary event losses relative to gross losses were 58% for Retail banking and 89% for Commercial banking, whereas the minimum indications were 3% and 0% for Retail banking and Commercial banking respectively. For the frequency of losses, the average boundary event losses comprise 10% for Retail banking and 21% for Commercial banking. The maximum boundary event losses relative to gross losses are 22% for Retail banking and 70% for Commercial banking, whereas the minimum indications were 0% for both Retail banking and Commercial banking.

If the average of the responses received is observed based on the loss amounts (being 33% and 64% for Retail banking and Commercial banking business lines respectively) these values appear to be in the range of the 40% as indicated by Sands (2011a). In terms of the number of losses, the averages observed were 10% and 21% for Retail banking and Commercial banking business lines respectively. In this instance, significant outliers were also present, but nevertheless, based on the average, these indications are significantly less than the 30% indication provided by Sands (2011a). Significant disparity exists in the measure to which boundary events are flagged.

6.8. Study review – Uniformity/disparity in the classification of boundary events

As part of the questionnaires, operational risk experts were provided with sixteen typical boundary event loss descriptions, and the respondents were required to classify the losses according to pure operational risk, pure credit risk, or boundary event risks. Respondents were also requested to include

²⁸ Two questionnaires were used in this study.

the loss values, that is, where they would view the losses that took place (that is, as pure credit risk loss, as pure operational risk loss or as boundary event type loss). The purpose of the Boundary Event Scenarios Questionnaire was therefore to obtain an understanding of how risk management specialists approach the classification of typical and frequent loss-event scenarios.

The respondents mostly have strong operational risk knowledge, and relatively neutral to strong credit risk knowledge. More than half of the respondents have more than ten years' experience in the banking industry. Most of the respondents have between two to four years' experience in operational risk. Cronbach's α value for the sixteen scenarios was tested to be 0.81. It can therefore be concluded that the risk descriptions and scenarios posed to the respondents effectively analyse the approach of the operational risk experts to risk classifications.

Uniform results – in terms of whether respondents classified risks as operational, credit, or boundary – were obtained for only 13% of the scenarios (two out of the sixteen scenarios). For the remainder of the results, the views were significantly variant. In addition, within the different categorisations (credit, operational or boundary), there were also numerous different approaches to where respondents felt the losses should be captured, for instance, some respondents captured a full loss amount as a boundary, whereas others would perform a split on loss amounts, stating that a portion of the loss amount was pure credit risk, and the rest of the loss amount was a boundary event.

There are significantly different views with regards to the interpretation of the approach to be followed in the classification of boundary events. Cognisance was also taken of the fact that most of the boundary event scenarios in the questionnaire were open to interpretation in some ways, and that a great variety of assumptions could be made for most of the boundary event scenarios. The respondents therefore had to make certain assumptions whilst deciding on the risk classifications and loss capturing. This point emphasises the fact that adequate risk descriptions, loss descriptions and understanding of the background of the loss event is required prior to a risk manager capturing information for a boundary event. Finally, the conclusion was drawn from the results that the majority of the respondents used causal analysis to draw conclusions for the classification of the boundary events.

6.9. Conclusion

The topic of boundary events – specifically those related to credit risk – is a relevant issue in the risk and financial industry. The topic leads to numerous debates, the amount of supporting literature and research in this area is limited, and no standardised guidelines exist, which banks can utilise to assist them during the classification processes. An important point to note is that operational risk may materialise either directly or indirectly through credit risk, and therefore, despite the distinction existing between credit risk and operational risk, it might sometimes still appear difficult to distinguish among loss events that are attributed to the different risk types.

A few years ago when the banking industry was confronted with the issue of boundary events, the BCBS ruled that credit losses which are driven by operational failure, should be treated as credit losses for the purposes of capital adequacy. This is the only guidance provided by the BCBS in terms of the treatment of boundary events. The root of the problem lies in the classification of these loss events, and once more clarity is provided on an effective approach to classification, it would be easier for banks to more accurately adhere to this regulatory requirement. The issue lies in the fact that the potential exists that actual boundary events might be classified as purely credit risk, and correctly be included in the credit risk capital charge, but not be flagged separately within the bank's internal operational risk database. Also, boundary events might be classified as operational risk and therefore be subject to the operational risk capital charge, instead of the credit risk capital charge. The first instance might give rise to an operational risk manager not being completely cognisant of the operational risks that the business is facing. The emphasis should always be on the management of risks and for this reason it is important that a financial institution indicates and flags all boundary events in its operational risk system. In addition, there is also the possibility of regulatory capital arbitrage in the event that losses are not classified correctly.

Currently, there is very little uniformity on how the classification of boundary events is performed. This is an indication of the lack of guidance that currently exists with regards to this issue. Also, it is clear that all banks are not effective enough when it comes to the flagging of boundary events. As these losses are not flagged as boundary events, they are therefore either indicated as pure credit risk losses, or pure operational risk losses.

Based on these results obtained, recommendations are put forth for banks with regards to the classification processes of boundary events.

6.10. Recommendations for financial institutions

With regards to boundary events and the classification thereof, the following recommendations can be made based on the research conducted and conclusions made in this study.

The identification of a credit default should be the first step to considering a boundary event. When going through the process of classifying boundary events, banks are advised to follow an approach whereby a credit default is considered to be central to the initial thought process of risk and loss classification. Therefore, the first trigger to the possible existence of a boundary event is the occurrence of a credit default – that is, a client of the bank failing to meet obligations according to agreed terms. A credit default, as stated earlier, is the crux of a boundary event, whether it is as a result of a client failing to meet obligations, or fraudulent activity combined with the failure to meet obligations. It is therefore advised that banks comply with the requirement of the BCBS by considering operational risk and credit risk in boundary events according to their specific definitions, and not exclude any specific events – such as, for example fraud – from the defined processes and

standards to meet the regulatory requirements. The use of a decision tree is proposed, as set out in Section 4.4.8 of Chapter 4. It is firstly necessary to consider whether a client default is involved in the loss event, and then, consideration can be given to the operational elements.

Adequate education, knowledge and experience of loss-event classification personnel. It is clear that the process of accurately and adequately classifying boundary event risks and losses requires a sufficient amount of education, knowledge and experience. This was also noted in the responses obtained from respondents who all indicated that education has a strong impact on the success or failure of accurate classification. Ernst and Young conducted a recent risk management study on 62 member firms of the Institute of International Finance (IIF). The writer supports the recommendations made by this study, namely that financial institutions are to ensure that their risk management functions have a sufficient amount and quality of resources to fulfil the specific required roles. Most importantly, risk management personnel should possess sufficient qualifications, experience and status to facilitate control responsibilities (Ernst and Young, 2011:38). Credibility requires a mastery of risk disciplines (Ernst and Young, 2011:38). A mastery of the credit risk and operational risk disciplines are imperative to the entities in the institutions that are responsible for making the decisions as to the classifications of the boundary event types. Finally, it is recommended that firms consider the establishment of a bi-directional career crossover between risk and line roles. This will serve as a significant and direct contribution to the improvement of mutual understanding, and it will also strengthen the risk management function (Ernst and Young, 2011:39).

Centralised risk management function should exist to utilise detailed information and to perform loss classification. Together with the use of knowledgeable and educated staff members, a centralised function should be established in key segments or business units, which is made responsible for the decision-making and classification processes of losses. This can be attained by requiring that business or operational personnel provide detailed supporting information on the loss event, in a standard format, to the key risk management stakeholder in the segment or business unit. As was noted during the analysis of the boundary event scenarios, adequate information is imperative to the process of classifying losses. The risk management expert will then have the ability to classify risks and losses efficiently and consistently throughout the segment or business unit through the use of adequate information. This will prevent uninformed entities, and uneducated personnel in the risk management subject to make decisions on areas that might have a significant impact on the financial institution itself – not only from a regulatory perspective, but also from a risk management perspective.

There should be adequate and efficient cooperation between operational risk and credit risk functions. ORX recommends that the operational risk function should be made responsible for ensuring that employees involved in the credit risk related processes of the institution are trained in recognising operational losses. This will assist in establishing processes for risk management analysis,

and the adequate and efficient reporting of the operational risk component within these losses (ORX, 2011:22). A specific team within credit risk can be involved in the determination of whether part of a credit loss is driven by the materialisation of an operational risk event. According to ORX, some of the members utilise their credit risk impairment teams for these purposes (ORX, 2011:22). Proper communication between the credit risk and operational risk teams is important, as credit risk losses might be captured as credit risk without any further consideration being given to whether an operational risk element was involved in the event. The recognition of these operational risk elements in the credit losses is imperative for proper and complete operational risk management. The operational risk management function should therefore liaise with its credit risk counterparts in order to promote consistent approaches on the implementation of the operational risk element identification and boundary event flags (ORX, 2011:22).

Banks can take cognisance of accounting standards and how boundary events have been treated historically. The interpretation of specific events, such as, for example, fraudulent activity on credit cards and identity theft, is not only specific to a bank or firm, but it is also accounting standard dependent (ORX, 2011:22). The IASB explicitly states that it would not be appropriate to recognise an impairment for losses that are expected to occur in a future period, because the necessary loss event (which might be, for example, the death of the borrower) has not yet occurred. Therefore, it can be concluded that only once a default occurs, can the loss be accounted for. As such, banks adhering to account standards will impair all defaults, irrespective of whether they take place through fraudulent activities. Banks should therefore be vigilant to the fact that losses might be logged for capital purposes in the operational risk databases for capital purposes as well. This might lead to double-counting. Losses in credit risk are mostly either embedded in trading profit P&L, or booked on specific accounts. As such losses are accounted for in credit risk, and therefore logged for credit risk capital purposes, these losses should merely be flagged in the operational risk system for management purposes.

Furthermore, Basel II states that operational risk losses relating to credit risk and that have historically been included in banks' credit risk databases should still be treated as credit risk for regulatory capital purposes. These losses will therefore not be subject to the operational risk capital charge (BIS, 2006a:153).

6.11. Regulatory recommendations

According to the Bank Supervision Department of the South African Reserve Bank (SARB), the purpose of the BA410 return, which is the annual operational risk return to be completed by South African banks for submission to the SARB, is for the regulator to obtain from a bank that has adopted the AMA the bank's loss-event types, recorded losses and loss recoveries. This information is based

on the specified business lines and loss-event types (South African Reserve Bank, 2008:545). An example of the BA410 is included in Appendix 5.

In terms of the disparity and lack of uniformity noted in terms of the measure in which banks currently flag their boundary events, it is recommended that the regulator adds an additional requirement to the BA410 return. This should entail that two additional lines be added to each business line section. Therefore, in addition to the “Number of events” and “Gross loss amount” information, the “Number of boundary events” and “Boundary events gross loss amount” should be added to the BA410 for each business line. This will ensure that the regulator has more certainty with regards to how prudently banks identify operational risk elements in their credit risk losses. In addition, banks will be required to incorporate all the necessary policies, procedures, guidelines and mechanisms to adequately identify these risks. Ultimately, this will have the desired effect on operational risk management: operational risk managers will have a complete view of all the operational risks being faced in the financial institution. Operational risk will become a more transparent risk type in the bank, and even those operational risks that are not so evident to operational risk managers will be identified and managed more efficiently and effectively.

6.12. Recommendations for further research

With reference to Section 5.9.4.2, where boundary events as percentage of total losses of the participating banks were investigated, future research can be conducted on data of at least five years. This will ensure that outliers can be smoothed out, as certain large events and losses in one specific year might be present or absent; including an additional number of years, and therefore data points, will neutralise the effect of outliers.

With regards to the questions posed in the General Questionnaire, future research can be conducted on more banks by including a number of international banks as well.

In terms of the boundary event scenarios approach that was followed in this study, future research can be to perform this research by conducting unstructured interviews with the participants. In this study, the respondents had to make assumptions when analysing the risk types. By conducting unstructured interviews, the analysis of boundary events can be assisted to a much greater extent than the thought processes of operational risk experts, and the assumptions they make, and can be properly noted and recorded. This will, in turn, ensure that more accurate conclusions can be formed regarding the approach that operational risk experts currently follow when analysing risk events and classifying losses.

Bibliography

BADEA, L. & SOCOL, A. 2010. Characteristics of managing operational banking risk. *Theoretical and applied economics*, 2010:39-60. [online] Available at: <http://store.ectap.ro/articole/354.pdf>. [Date of access: 09 February 2011].

BAGCHI, S.K. 2005. Credit risk mitigation – implications of Basel II prescriptions in Indian banking. [online] Available at: <http://220.227.161.86/10415549-553.pdf>. [Date of access: 20 July 2011].

BENEDEK, G. & HOMOLYA, D. 2007. *Analysis of operational risk of banks – catastrophe modelling*. [online] Available at: http://web.uni-corvinus.hu/matkg/working_papers/wp_2007_8_benedek_homolya.pdf. [Date of access: 09 February 2010].

BERNANKE, S. 2006. *Modern risk management and banking supervision: At the Stonier Graduate School of Banking*, Washington, D.C. June 12. [online] Available at: <http://www.federalreserve.gov/newsevents/speech/Bernanke20060612a.htm>. [Date of access: 06 June 2010].

BESSIS, J. 2010. *Risk management in banking*. 3rd ed. Chichester, UK: Wiley. 821 p.

BESSIS, J. 2002. *Risk management in banking*. 2nd ed. Chichester, UK: Wiley. 780 p. BIES, S. 2005. *Remarks by Governor Susan Schmidt Bies: At the International Center for Business Information's Risk Management Conference*. Basel Summit, Geneva, Switzerland. December 6. [online] Available at: <http://www.federalreserve.gov/boarddocs/speeches/2005/20051206/default.htm>. [Date of access: 06 June 2010].

BIS, Basel Committee on Banking Supervision. 2011. *Operational risk – supervisory guidelines for the advanced measurement approach*. [online] Available at: <http://www.bis.org/publ/bcbs196.pdf>. [Date of access: 21 July 2011].

BIS, Basel Committee on Banking Supervision. 2009. *History of the Basel committee and its membership*. [online] Available at: <http://www.bis.org/bcbs/history.pdf>. [Date of access: 05 January 2010].

BIS, Basel Committee on Banking Supervision. 2006a. *International convergence of capital measurement and capital standards*. [online] Available at: <http://www.bis.org/publ/bcbs128.htm>. [Date of access: 20 August 2009].

BIS, Basel Committee on Banking Supervision. 2006b. Goals and strategies of the Basel committee. *BIS Review* 122/2006. [online] Available at: www.bis.org/review/r061214a.pdf. [Date of access: 13 June 2010].

BIS, Basel Committee on Banking Supervision. 2005. *The treatment of expected losses by banks using the AMA under the Basel II Framework*. [online] Available at: http://www.bis.org/publ/bcbs_n17.pdf. [Date of access: 06 July 2010].

BIS, Basel Committee on Banking Supervision. 2003. *Consultative document – the new Basel capital accord*. [online] Available at: <http://www.bis.org/bcbs/bcbscp3.htm>. [Date of access: 06 January 2010].

BIS, Basel Committee on Banking Supervision. 2001a. *Overview of the new Basel capital accord*. [online] Available at: <http://www.bis.org/publ/bcbsca02.pdf>. [Date of access: 28 October 2009].

BIS, Basel Committee on Banking Supervision. 2001b. *The internal ratings-based approach to credit risk*. [online] Available at: <http://www.bis.org/publ/bcbsca05.pdf>. [Date of access: 06 November 2009].

BIS, Basel Committee on Banking Supervision. 2001c. *Consultative document – operational risk*. [online] Available at: <http://www.bis.org/publ/bcbsca07.pdf>. [Date of access: 12 January 2010].

BIS, Basel Committee on Banking Supervision. 2000. *Principles for the management of credit risk*. [online] Available at: <http://www.bis.org/publ/bcbs54.pdf?noframes=1>. [Date of access: 26 August 2009]. BUCHELT, R & UNTEREGGER, S. 2004. Cultural risk and risk culture: operational risk after Basel II. *Financial Stability Report* 6: 86-97. [online]: Available at: http://www.oenb.at/en/img/fsr_06_cultural_risk_tcm16-9495.pdf. [Date of access: 15 September 2010].

CAGAN, P. 2009. Managing operational risk through the credit crisis. *Compliance, Risk & Opportunity*. [online] Available at: <http://www.algorithmics.com/EN/media/pdfs/Algo-RA0209-CRO-PCagen.pdf>. [Date of access: 16 September 2010].

CECH, R. 2007. Event horizon. *Oprisk and compliance*, February 2007:35-39. [online] Available at: <https://subscriber.riskbusiness.com/InterestingReading/RC%20Event%20Horizon.pdf>. [Date of access: 10 May 2011].

CHAPELLE, A., CRAMA, Y., HUBNET, G., & PETERS, J.P. 2006. *Practical methods for measuring and managing operational risk in the financial sector: A clinical study*. [online] Available at: http://www.google.co.za/url?sa=t&source=web&cd=5&ved=0CD4QFjAE&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.86.1340%26rep%3Drep1%26type%3Dpdf&rct=j&q=Practical%20methods%20for%20measuring%20and%20managing%20operational%20risk%20in%20the%20financial%20sector&ei=w_DVTebE8anhAfv_ry1CQ&usg=AFQjCNEuDEacmFYnoolud66esDPvslg. [Date of access: 12 July 2010].

CHAUDHARY, D, SINGH, P & PRABHAT, P. 2005. *Basel II: the Duckworth-Lewis of banking*. [online] Available at: <http://www.thehindubusinessline.com/iw/2005/02/06/stories/2005020600621300.htm>. [Date of access: 05 June 2010].

COOPER, D.R. & EMORY, C.W. 1995. *Business research methods*. 5th ed. Chicago: Irwin.

COSMA, S., GABBI, G. & SALVADORI, G. 2009. *Are small banks discriminated by the new operational risk rules? A clinical paper for the Italian case*. [online] Available at: <http://69.175.2.130/~finman/Reno/Papers/AreSmallBanksdiscriminatedbytheNewOperationalRiskRules.pdf>. [Date of access: 17 September 2010].

CREDITFLUX. 2010. *Glossary*. [online] Available at: <http://www.creditflux.com/Glossary/Credit-event/>. [Date of access: 17 September 2010].

CRESWELL, J.W. 2003. *Research design – qualitative, quantitative, and mixed methods approaches*. 2nd ed. Sage Publications, Inc. 246 p.

CROUHY, C., GALAI, D. & MARK, R. 2001. *Risk management*. New York: McGraw-Hill. 717 p.

DE SERVIGNY, A. & RENAULT, O. 2004. *Measuring and managing credit risk*. New York: McGraw-Hill. 466 p.

ELIZALDE, A. & REPULLO, R. 2007. Economic and regulatory capital in banking: what is the difference? *International journal of central banking*, 3(3):87-117, September.

ERNST & YOUNG. 2011. *Making strides in financial services risk management*. [online] Available at: [http://www.ey.com/Publication/vwLUAssets/Making_strides_in_financial_services_risk_management/\\$FILE/Making%20strides%20in%20financial%20services%20risk%20management.pdf](http://www.ey.com/Publication/vwLUAssets/Making_strides_in_financial_services_risk_management/$FILE/Making%20strides%20in%20financial%20services%20risk%20management.pdf). [Date of access: 27 July 2011].

ESTERHUYSEN, J.T. 2006. *The management of operational value at risk in banks*. Potchefstroom: North-West University. (Thesis – PhD). 301 p.

Federal Deposit Insurance Corporation. 2003. *Supervisory guidance on operational risk advanced measurement approaches for regulatory capital*. [online] Available at: <http://www.fdic.gov/regulations/laws/publiccomments/basel/oprisk.pdf>. [Date of access: 30 August 2011].

FERGUSON, R.W. 2003. Basel II: *Before the Committee on Banking, Housing and Urban Affairs. Testimony of Vice Chairman*, 18 June. [online] Available at: <http://www.thehindubusinessline.com/iw/2005/02/06/stories/2005020600621300.htm>. [Date of access: 06 June 2010].

GALLATI, R. 2003. *Risk management and capital adequacy*. New York: McGraw-Hill. 555 p.

HEINRICH, J. 2004. *Goodness-of-fit*. [online] Available at: <http://www-cdf.fnal.gov/physics/statistics/recommendations/goodnessoffit.html>. [Date of access: 12 April 2012].

HOFFMAN, D.G. 2002. *Managing operational risk: 20 firm-wide best practice strategies*. New York: Wiley. 534 p.

INTERNATIONAL ACCOUNTING STANDARDS BOARD. 2009. International accounting standards 39.

IZHAR, H. 2010. *Identifying operational risks in Islamic banks*. [online] Available at: <http://www.newhorizon-islamicbanking.com/index.cfm?action=view&id=10802§ion=features>. [Date of access: 08 April 2011].

JONES, C. & SHIEKH, A. 1999. Developing and implementing risk management systems. *Financial Technology*, June: p48-52.

KING, J.L. 2001. *Operational risk: measurement and modelling*. Chichester: Wiley. 261 p.

KOCH, T.W. & MACDONALD, S.S. 2003. *Bank management*. 4th ed. Orlando, USA: Dryden Press. 968 p.

KPMG. 2009. *Operational risk framework for advanced measurement approach*. [online] Available at: http://www.kpmg.pl/dbfetch/52616e646f6d49561246763afdc2bea90ab12d605bf7eb913ccbf5e50f172878/f_ulotka_oprisk_en_online.pdf. [Date of access: 18 July 2010].

KPMG. 2005. *Basel II: a closer look*. [online:] Available at: <http://us.kpmg.com/microsite/FSLibraryDotCom/docs/211-412%20Basel%20II%20-%20A%20Closer%20look%20-%20WEB%20VERSION.pdf>. [Date of access: 20 November 2009].

KPMG. 2003. *Basel II: a worldwide challenge for the banking business*. [online] Available at: www.kpmg.com.co/...Banking/Basel%20a%20World%20Wide%20Challenge.pdf. [Date of access: 17 June 2010]. LUBBE, J. & SNYMAN, F. 2009. *Advanced measurement approach for banks*. [online] Available at: <http://www.statssa.gov.za/isi2009/ScientificProgramme/IPMS/0256.pdf>. [Date of access: 15 July 2010].

MACLENAGHEN, T. 2007. The data puddle challenge. *Oprisk and compliance*. August 2007:24-31. [online] Available at: <https://subscriber.riskbusiness.com/InterestingReading/TmL%20Puddles%20July%2024%202007.pdf>. [Date of access: 10 May 2011].

MATTEN, C. 2000. *Managing bank capital: capital allocation and performance measurement*. 2nd ed. New York: Wiley. 341 p.

MATTEN, C. 1999. *Risk and capital management – an overview*. [online] Available at: http://www.apra.gov.au/RePEc/RePEcDocs/Archive/conference_papers1/risk_capital_management.pdf. [Date of access: 20 August 2009]. MATTHEWS, K. 1996. *Capital adequacy ratios for banks*. [online] Available at: http://www.rbnz.govt.nz/research/bulletin/1992_1996/1996jun59_2matthews.pdf. [Date of access: 20 January 2010].

MERRIAM-WEBSTER. 2012. Learner's dictionary. [online] Available at: www.learnersdictionary.com. [Date of access: 10 April 2012].

MOOSA, I.A. 2006. Misconceptions about operational risk. *Journal of operational risk*, 1(4):97-104, Winter

ORX. 2007. *ORX reporting standards: an ORX members' guide to operational risk event/loss reporting*. [online] Available at: http://www.orx.org/lib/uploads/public_folder/ORRS-Feb-07.pdf. [Date of access: 07 February 2011].

ORX. 2011. *Operational risk reporting standards* (edition 2011). [online] Available at: <http://www.orx.org/standards>. [Date of access: 15 June 2011].

ORX. 2010. *ORX operational risk report*. [online] Available at: <http://www.orx.org/orx-data>. [Date of access: 13 July 2011]. OSTROWSKI, J. 1997. *Titanic interesting facts*. [online] Available at: <http://www.titanicstory.com/interest.htm>. [Date of access: 15 September 2010].

PALISADE. 2012. *Monte Carlo simulation: what is it and how does it work?* [online] Available at: http://www.palisade.com/risk/monte_carlo_simulation.asp. [Date of access: 10 April 2012].

PETERS, G & TERAUDS, V. 2007. *Quantifying bank operational risk*. School of Mathematics and Statistics, University of New South Wales, Sydney.

PLESNER, S. 2007. *Operational risk management*. [online] Available at: http://www.nordiccapitalmarkets.org/UserFiles/File/Operational_Risk_Management_-_Soren_Plesner.pps. [Date of access: 21 February 2011].

RAGHAVAN, R.S. 2003. *Risk management in banks*. [online] Available at: http://icai.org/resource_file/11490p841-851.pdf. [Date of access: 20 September 2010].

RIPPEL, M. & TEPLY, P. 2008. *Operational risk – scenario analysis*. [online] Available at: <http://ies.fsv.cuni.cz/default/file/download/id/10246>. [Date of access: 06 July 2010].

SAITA, F. 2007. *Value at risk and bank capital management*. Amsterdam: Academic Press. 259 p.

SAMAD-KHAN, A. 2008. *Modern operational risk management*. [online] Available at: <http://www.opriskadvisory.com/docs/Modern%20Operational%20Risk%20Management.pdf>. [Date of access: 03 March 2011].

SANDS, M. 2011a. *Oprisk North America: risk appetite, supermodels and reform*. [online] Available at: <http://www.risk.net/operational-risk-and-regulation/news/2039135/oprisk-north-america-risk-appetite-supermodels-and-reform>. [Date of access: 10 May 2011].

SANDS, M. 2011b. *Citi's Wertheim: operational risk function must detect to protect*. [online] Available at <http://www.risk.net/operational-risk-and-regulation/profile/2069010/citis-wertheim-operational-risk-function-detect-protect/page/2>. [Date of access: 30 May 2011].

SANTOS, J.R.A. 1999. Cronbach's alpha: a tool for assessing the reliability of scales. *Journal of Extension*, 37(2), Apr. [online] Available at: <http://www.joe.org/joe/1999april/index.html>. [Date of access: 12 July 2011].

SCHOLTZ, J. & DE VILLIERS, D. 2011. *Banking regulation and supervision in South Africa*. [online] Available at: http://www.webberwentzel.com/wwb/action/media/downloadFile?media_fileid=6150. [Date of access: 28 June 2011].

SMIT, W. 2009. *Determining the fair level of economic capital for credit- and market risk in commercial banks*. Potchefstroom: North-West University. (Thesis – M.Com). 195 p.

SOUTH AFRICAN RESERVE BANK. 2011. *South African registered banks and representative offices*. [online] Available at: <http://www.resbank.co.za/RegulationAndSupervision/BankSupervision/Pages/SouthAfricanRegisteredBanksAndRepresentativeOffices.aspx>. [Date of access: 28 June 2011].

SOUTH AFRICAN RESERVE BANK. 2008. *Regulations relating to banks*. [online] Available at: <http://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/52/19%20BA400,%20BA410.pdf>. [Date of access: 30 March 2011]STEIN, H. 2010. *Clear and present danger*. [online] Available at: <http://www.risk.net/operational-risk-and-regulation/feature/1696813/clear-danger>. [Date of access: 30 March 2011].

STOLZ, S. 2002. *The relationship between bank capital, risk-taking, and capital regulation: a review of the literature*. [online] Available at: <http://econpapers.repec.org/paper/kielkielw/1105.htm>. [Date of access: 31 August 2009].

STRAHAN, P.E. 2003. *The real effects of U.S. banking deregulation*. [online] Available at: <http://research.stlouisfed.org/publications/review/03/07/Strahan.pdf>. [Date of access: 31 August 2009].

SUNGARD. 2010. *Credit risk*. [online] Available at: <http://www.erisk.com/learning/jigsaw/creditrisk.asp>. [Date of access: 17 September 2010].

TOZER-PENNINGTON, V. 2011. *Time to shine*. [online] Available at: <http://www.risk.net/operational-risk-and-regulation/opinion/2039022/shine>. [Date of access: 10 May 2011].

TOZER-PENNINGTON, V. 2010. *Oprisk Europe: the slow drive for change*. [online] Available at: <http://www.risk.net/operational-risk-and-regulation/feature/1724768/oprisk-europe-the-slow-drive-change>. [Date of access: 10 May 2011].United Nations Conference on Trade and Development. 2006. *Basel 2: the new Basel capital accord and its impact on commodity financing in developing countries*.

[online] Available at: <http://www.docstoc.com/docs/16141211/United-Nations-Conference-on-Trade-and-Development-BASEL-2> [Date of access: 05 January 2010].

YEH, A., TWADDLE, J. & FRITH, M. 2005. *Basel II: a new capital framework*. [online] Available at: http://www.rbnz.govt.nz/research/bulletin/2002_2006/2005sep68_3yehtwaddlefrith.pdf. [Date of access: 10 January 2010].

Appendix 1

The Cover Letter to Each Questionnaire



NORTH-WEST UNIVERSITY
YUNIBESITHI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT
POTCHEFSTROOM CAMPUS

Private Bag X6001, Potchefstroom
South Africa 2520

Tel: +27(18) 299-1111/2222
Web: <http://www.nwu.ac.za>

School of Economics
Tel: +27(18) 2991352
Fax: +27(18) 2991398
Email: andre.heyman@nwu.ac.za

3 May 2011

Dear Sir/Madame,

The survey you received studies the approach that South African banks follow in the classification of operational risk losses relating to credit risk, or "boundary events".

By completing this survey, you agree that the information you provide may be used for research purposes. Know that you are free to decide not to complete the survey, although your data cannot be replaced by anyone else's. The survey is, however, completed anonymously, and I, as researcher, will in no way connect the information you provide to you personally, or to your company.

I foresee that you are unlikely to experience any negative consequences due to completing this questionnaire. Even so, I, the researcher, undertake to keep the individual information provided herein confidential, not to let it out of my possession, and to analyse results only at an aggregated level.

I do hope that the information I gain from this survey will assist me in analysing the approach that South African banks follow for the classification of boundary events.

The survey consists of two separate questionnaires. The first questionnaire covers fourteen general questions relating - amongst others - to the bank's approach to the classification of losses, and some data-specific questions relating to losses and boundary events. Only one respondent per bank is required to complete this questionnaire.

The second questionnaire covers nine demographical questions, and a description of sixteen scenarios, on which the respondent should indicate the classification of the loss, and the loss amounts that are treated as a credit risk, operational risk or boundary event. Three respondents per bank are required to complete this questionnaire.

If you do, however, have further questions or concerns, please feel free to contact the principal investigator, Jolene Steenkamp:

Mobile: 082 4311 133
E-mail: jolene.steenkamp@gmail.com

Your time and cooperation is greatly appreciated.

Yours Sincerely
Jolene Steenkamp

Appendix 2

The layout of the General Questionnaire

Question 1

Does the bank have a documented and approved Incident Management Lifecycle for Operational Risk events that might occur throughout the various divisions and/or segments within the bank?

- Yes
- No

Question 2

In terms of the classification of an incident, and specifically boundary events, are proper, documented and approved guidelines utilised for accurate classification?

- Yes
- No

Question 3

In terms of the classification of an incident, and specifically boundary events are documented and approved decision trees utilised for accurate classification?

- Yes
- No

Question 4

Does the bank utilise a taxonomy of events that comprises of a number of levels and subclasses?

- Yes
- No

Question 5

The Bank for International Settlements ("BIS") (BIS, 2006a: 153) requires that operational risk losses that are related to credit risk, that is, credit risk/operational risk boundary events should be treated as credit risk for the purposes of calculating minimum regulatory capital under the Basel II Framework. Such losses will, therefore, not be subject to any operational risk capital charges. However, for the purposes of internal operational risk management, banks are required to identify all material operational risk losses. Such material operational risk-related credit risk losses – or credit risk/operational risk boundary events – should be flagged separately within a bank's internal operational risk database (BIS, 2006a: 153).

In your opinion, how accurately - in terms of the regulations - does the bank classify boundary events? Please give a rating from 1 to 10, where 1 stipulates zero percent accurate, and 10 stipulates one hundred percent accurate.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

Question 6

The Bank for International Settlements ("BIS") (BIS, 2006a: 153) requires that operational risk losses that are related to credit risk, that is, credit risk/operational risk boundary events should be treated as credit risk for the purposes of calculating minimum regulatory capital under the Basel II Framework. Such losses will, therefore, not be subject to any operational risk capital charges. However, for the purposes of internal operational risk management, banks are required to identify all material operational risk losses. Such material operational risk-related credit risk losses – or credit risk/operational risk boundary events – should be flagged separately within a bank's internal operational risk database (BIS, 2006a: 153).

In your opinion, how accurately - in terms of the regulations - does the bank treat the losses associated to boundary events, from a capital perspective? Please give a rating from 1 to 10, where 1 stipulates zero percent accurate, and 10 stipulates one hundred percent accurate.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9

- 10

Question 7

How strongly do you believe does each of the factors listed below, impact the success/failure of the boundary event classification and loss treatment within your organisation?

- a. The use of documented and approved guidelines for the classification and treatment of boundary events.*
- b. The use of documented and approved decision trees for the classification and treatment of boundary events.*
- c. The use of a taxonomy of events.*
- d. The utilisation of adequately trained, knowledgeable and experienced staff responsible for classification and treatment of boundary events.*
- e. The use of documented and approved causal categories for the classification of boundary events.*
- Very Strong Impact
- Strong Impact
- Minor Impact
- No Impact

Question 8

In terms of the classification of an incident, and specifically boundary events, are documented and approved causal categories utilised by the bank for accurate classification?

- Yes
- No

Question 9

Does the bank apply a threshold for internal data collection?

- Yes
- No
- a. Please specify the threshold amount for the "Retail banking" Business Line.*
- b. Please provide the reasoning behind the utilisation of the specific threshold amount for the data collection of losses for the "Retail banking" Business Line. Otherwise, provide the reason for the bank not utilising a threshold.*
- c. Please specify the threshold amount for the "Commercial banking" Business Line:*
- d. Please provide the reasoning behind the utilisation of the specific threshold amount for the data collection of losses for the "Commercial" Business Line. Otherwise, provide the reason for the bank not utilising a threshold.*

Question 10

Specifically for internal losses relating to boundary events, does the bank apply a threshold for the data collection of these events?

- Yes
- No
- a. *Please specify the boundary events threshold amount for the "Retail banking" Business Line.*
- b. *Please provide the reasoning behind the utilisation of the specific threshold amount for the data collection of losses relating to boundary events, for the "Retail banking" Business Line. Otherwise, provide the reason for the bank not utilising a threshold.*
- c. *Please specify the boundary events threshold amount for the "Commercial" Business Line.*
- d. *Please provide the reasoning behind the utilisation of the specific threshold amount for the data collection of losses relating to boundary events, for the "Retail banking" Business Line. Otherwise, provide the reason for the bank not utilising a threshold.*

Question 11

- a. *Please provide the gross loss amount that the bank reported for the previous financial year, for the "Retail banking" Business Line.*
- b. *For the "Retail banking" Business Line, please provide the gross loss amount that was flagged as "boundary" for credit, for the previous financial year.*

Question 12

- a. *Please provide the gross loss amount that the bank reported for the previous financial year, for the "Commercial" Business Line.*
- b. *For the "Commercial" Business Line, please provide the gross loss amount that was flagged as "boundary" for credit, for the previous financial year.*

Question 13

- a. *Please provide the number of losses that the bank reported for the previous financial year, for the "Retail banking" Business Line.*
- b. *For the "Retail banking" Business Line, please provide the number of losses that were flagged as "boundary" for credit, for the previous financial year.*

Question 14

- a. *Please provide the number of losses that the bank reported for the previous financial year, for the "Commercial" Business Line.*
- b. *For the "Commercial" Business Line, please provide the number of losses that were flagged as "boundary" for credit, for the previous financial year*

Appendix 3

The layout of the Boundary Events Scenarios Questionnaire

a. Demographical questions

The following questions are included in the section of demographical questions:

Question A

How many years of employment and experience do you have in the banking industry?

- Under 3 Years
- 3 to 5 Years
- 6 to 9 Years
- Years and Longer

Question B

In which area or division of the Bank do you work?

Question C

What is your current position at the bank, in this specific division specified?

Question D

What position/job description did you fulfil prior to this current position?

Question E

Please specify your educational or qualificational background.

- Financial
- Accounting
- Statistical
- Other

Please specify your educational or qualificational background:

Question F

How many years of experience do you have in operational risk?

- Under 2 Years
- 2 to 4 Years
- 5 to 7 Years
- 7 to 10 Years

- 11 Years and Longer

Question G

How many years of experience do you have in credit risk?

- Under 2 Years
- 2 to 4 Years
- 5 to 7 Years
- 7 to 10 Years
- 11 Years and Longer

Question H

How strong would you rate your knowledge and understanding of the Basel II Regulations relating to operational risk?

- Very Strong
- Strong
- Neutral
- Weak
- Very Weak

Question I

How strong would you rate your knowledge and understanding of the Basel II Regulations relating to credit risk?

- Very Strong
- Strong
- Neutral
- Weak
- Very Weak

b. Scenario Descriptions

Scenario 1

The bank has granted Client A a credit card facility of R10 000. This overdraft facility has been approved by the bank's application scorecard, and has been sanctioned adequately and properly. Client A goes to the ATM to withdraw money. The exposure of R10 000 to the client on the credit card has already been reached, and the client attempts to withdraw R4 000 from the ATM. The system should automatically reject this request, but due to an error, Client A receives the R4 000 and the

account is overdrawn above the agreed limit. Credit staff at the bank does not follow up on this overdrawn facility and Client A defaults on his exposure to the bank.

Scenario 2

Client B has been granted an overdraft facility of R40 000. This overdraft facility has been approved by bank's appropriate application scorecard, and has been adequately and properly sanctioned. Client B overdraws this facility to R60 000, and Client B is therefore R20 000 over his approved and agreed limit. Credit staff at the bank aims to follow up on the overdrawn facility and Client B cannot be reached due to insufficient client details on the system. The client defaults on the amount of R60 000.

Scenario 3

Client C has been granted an overdraft facility of R50 000. The facility has gone through proper and adequate approval processes. During the 5th month, the R50 000 facility is overdrawn to an amount of R90 000. The credit team failed to report the account as overdrawn, and at the end of the 6th month, no risk triggers were identified. In the 9th month, the facility is overdrawn to R120 000. A liquidator was appointed, and only then was the position realised by the credit team.

Scenario 4

Client D is granted an overdraft facility of R25 000, which has been approved by the application scorecard and adequately and properly sanctioned. The facility of R25 000 is fully drawn. Credit staff follows up on the drawn facility, and it is discovered that Client D is not able to repay the R25 000 that has been granted.

Scenario 5

Client E owes the bank an amount of R200 000, and subsequent to investigations, the client is not able to repay the amount. The credit risk officer responsible for this client is aware of sufficient collateral supplied by the client, as this has been discussed with the client, and also mentioned on the sanctioning documents. This documentation is however missing, and therefore is it impossible for the bank to take advantage of the collateral.

Scenario 6

Client F is granted an overdraft facility of R10 000. The facility has been approved by the application scorecard and adequately sanctioned. When the facility amount was however captured, it was captured incorrectly as R100 000. The client does not qualify for this incorrectly captured limit. The limit of R100 000 is fully drawn, and Client F has defaulted on this amount as she is unable to repay the amount.

Scenario 7

Client G is a good customer of the bank, and deposits a cheque of R300 000 into his account. The cheque is returned unpaid as fraud. It turns out that this is a Zimbabwean stolen cheque. The cheque was also wrongly cleared by the bank. Client G is not aware or responsible for the fraud, but the bank is however facing a loss. The client used all of the funds and subsequently the bank had to call in legal action in order to recover the loss/part of the loss. Subsequently, appropriate recovery procedures were followed and an amount of R220 000 was recovered.

Scenario 8

The bank has faced several legal issues and challenges within the last few months, which were of a similar nature. Subsequent to several investigations, it was discovered that the standard security documentation, which has been updated recently, contained vague and ambiguous terms regarding the security and collateral required for facilities. Consequently, this led to numerous facilities – granted subsequent to the documentation being updated – having in place security that could not be taken up as and when required by the bank. The bank suffered losses on a number of drawn and overdrawn facilities that were avoidable. One such incident is where Client K, who has drawn his full facility of R600 000, defaulted on the amount and even though the credit officer was certain of the correct procedures being followed with regards to the collateral for the facility, the full collateral could not be taken up, and covered only R450 000 of the amount owed.

Scenario 9

A potential new client, Client H, wishes to open an account at the Sandton City branch. He claims to be representing a well known company in Sandton. Fraudulent documents are presented, and the credit officer at the branch approves the new account for Client H, together with an overdraft facility of R180 000. It was only discovered after several months that the application by Client H was fraudulent. The credit officer at the Sandton City branch was negligent in the approval of the application, as he assumed the client to represent the well-reputed company and did not go through the appropriate checks and authorisation with regards to the documents presented. Client H has fully drawn the amount of R180 000. The bank managed to possess assets from Client H amounting to R90 000. The remaining R90 000 could not be recovered.

Scenario 10

An employee of a big client of the bank, ABS (Pty) Ltd, forged cheques and a letter of authority. The company was defrauded of R5 000 000. The employee has left the company, and ABS (Pty) Ltd only became aware of these fraudulent activities 1 year later. ABS (Pty) Ltd now claims the full amount of R5 000 000 from the bank. Subsequent to lengthy investigations, the bank's legal advisors and/or Legal Department advise that the bank would certainly be successful in court, as there was no sign of proof of negligence from the bank's side. Subsequent to numerous debates, the Corporate Credit Department decides that, because ABS (Pty) Ltd is a highly reputable company and client of the bank,

the bank should protect the highly valuable client relationship. Together with the Legal team, the bank decides to pay ABS (Pty) Ltd a goodwill payment that equals 50% of the claimed amount.

Scenario 11

Client M approaches the bank in order to obtain a new credit account. Client M presents the required documents as requested. The client's details are inputted into the bank's scoring model and, even though Client M is a student that works part-time, the scoring model rates him good enough to obtain a facility of R120 000. The credit manager does not realise that there might be a possible error, and the facility is approved by him. Client M draws the facility to the amount of R10 000, and only then is it discovered by the bank that the scoring model was in error, and that Client M is unable to repay the bank the amount of R10 000.

Scenario 12

Client P has always had a good relationship with the bank. He has a current facility of R1 000 000. Client P has sufficient collateral and his payments are always up to date. The bank decides to increase Client P's facility to R1 400 000. Due to negligence on the credit manager's side, the client's collateral information is not updated. In the wake of the economic crisis, Client P suffers losses and has to close down his business. His facility was drawn to R1 300 000 and he is able to repay only R1 100 000.

Scenario 13

Mr. X is an employee of the credit division within the bank. A close relative of Mr. X, Mr. A, applies for a credit card at the Nelspruit branch. Mr. A's application for a credit card is successful. Mr. X is responsible for capturing Mr. A's details on the credit risk system that calculates the approved overdraft facility. Mr. A promises to pay Mr. X an amount of money, for an increased facility on his credit card. Mr. X agrees, and by inputting incorrect details, Mr. A is granted an overdraft facility of R100 000, which is far above his means and ability to repay. Mr. X's manager authorises the facility, and does not pick up on the fraudulent activity and incorrect information entered. A few months later, Mr. A defaults on an amount of R80 000.

Scenario 14

Client Z is granted a properly approved and sanctioned overdraft facility of R20 000. After several months, the account is highlighted on the system as "dormant". On further investigation, the credit officer determines that the client is unable to repay the amount of R20 000.

Scenario 15

Mrs. H is an employee of the bank, and works at the Northgate branch. Mrs. H has handled several credit card applications for the day and mistakenly, a number of documents relating to the

applications are misplaced between her personal documents and these are packed in her briefcase on her way home. Mrs. H becomes a victim of a hijacking that afternoon on her way home, and consequently, her vehicle with her briefcase is stolen. The hijackers got hold of the confidential documents and managed to use the information to withdraw money from two clients' new credit accounts. Subsequently the respective amounts of R10 000 and R3 000 were withdrawn from the clients' accounts.

Scenario 16

Unknowningly, Client Q deposited a fraudulent Zimbabwean cheque of R700 000 into his account. The cheque was returned unpaid, with reason: "Stolen cheque". The client was not part of the fraud. The client also used all the funds. Legal action therefore had to be taken by the bank to recover the loss suffered. R300 000 of the total amount was recovered. The loss subsequent to recovery therefore amounted to R400 000.

Final Question

During your completion of this questionnaire and the sixteen scenarios that were presented, what "classification base" did you apply most frequently to classify the various loss events:

Contributing factors / or causes: that is, the pre-existing condition that made the event more likely to happen.
Asking the question: WHY DID IT HAPPEN?
Events: that is, the actual occurrence that took place and that was recorded.
Asking the question: WHAT HAPPENED?
Controls: that is, the "extra steps" in the business process that were designed to detect or prevent the loss events.
Asking the question: WHY WAS IT NOT PREVENTED?
Impacts / or effects: that is, the difference between the expected outcome of the operational process and its actual outcome. There might be multiple impacts per incident.
Asking the question: WHAT WAS THE RESULT?

Appendix 4

Boundary Event Scenario Questionnaire – Responses

Responses to scenario 1

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	4,000		
2	Boundary Event Type			14,000
3	Boundary Event Type		10,000	4,000
4	Boundary Event Type	4,000	10,000	
5	Boundary Event Type			14,000
6	Boundary Event Type		14,000	4,000
7	Boundary Event Type		10,000	4,000
8	Operational Event Type	4,000		
9	Boundary Event Type		10,000	4,000
10	Boundary Event Type		10,000	4,000
11	Boundary Event Type		10,000	4,000
12	Boundary Event Type	4,000	10,000	
13	Boundary Event Type			4,000
14	Boundary Event Type			4,000
15	Boundary Event Type		10,000	4,000
16	Boundary Event Type		10,000	4,000
17	Operational Event Type	4,000		
18	Operational Event Type	4,000		
19	Boundary Event Type			10,000

Responses to scenario 2

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	20,000		
2	Boundary Event Type			60,000
3	Boundary Event Type		40,000	20,000
4	Credit Event Type		60,000	
5	Boundary Event Type			60,000
6	Boundary Event Type		40,000	20,000
7	Boundary Event Type		40,000	20,000
8	Boundary Event Type		40,000	20,000
9	Boundary Event Type	20,000	40,000	
10	Boundary Event Type			60,000
11	Boundary Event Type		40,000	20,000
12	Operational Event Type			60,000
13	Credit Event Type		20,000	
14	Boundary Event Type			60,000
15	Boundary Event Type			60,000
16	Boundary Event Type		40,000	20,000
17	Operational Event Type	20,000		

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
18	Operational Event Type	20,000		
19	Credit Event Type		60,000	

Responses to scenario 3

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Boundary Event Type			70,000
2	Boundary Event Type			120,000
3	Boundary Event Type		50,000	70,000
4	Credit Event Type		120,000	
5	Boundary Event Type			120,000
6	Boundary Event Type		120,000	70,000
7	Boundary Event Type		50,000	70,000
8	Operational Event Type	120,000		
9	Boundary Event Type		50,000	70,000
10	Boundary Event Type		50,000	70,000
11	Boundary Event Type		50,000	70,000
12	Credit Event Type		120,000	
13	Credit Event Type		120,000	
14	Credit Event Type		120,000	
15	Boundary Event Type		50,000	70,000
16	Boundary Event Type		50,000	70,000
17	Operational Event Type	70,000		
18	Boundary Event Type	30,000	40,000	70,000
19	Credit Event Type		120,000	

Responses to scenario 4

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Credit Event Type		25,000.00	
2	Credit Event Type		25,000.00	
3	Credit Event Type		25,000.00	
4	Credit Event Type		25,000.00	
5	Credit Event Type		25,000.00	
6	Credit Event Type		25,000.00	
7	Credit Event Type		25,000.00	
8	Credit Event Type		25,000.00	
9	Credit Event Type		25,000.00	
10	Credit Event Type		25,000.00	
11	Credit Event Type		25,000.00	
12	Credit Event Type		25,000.00	
13	Credit Event Type		25,000.00	
14	Credit Event Type		25,000.00	
15	Credit Event Type		25,000.00	

16	Credit Event Type		25,000.00	
17	Credit Event Type		25,000.00	
18	Credit Event Type		25,000.00	
19	Credit Event Type		25,000.00	

Responses to scenario 5

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	200,000		
2	Boundary Event Type			200,000
3	Boundary Event Type		200,000	200,000
4	Boundary Event Type			200,000
5	Boundary Event Type			200,000
6	Boundary Event Type		200,000	200,000
7	Boundary Event Type			200,000
8	Operational Event Type	200,000		
9	Operational Event Type	200,000		
10	Boundary Event Type			200,000
11	Boundary Event Type			200,000
12	Operational Event Type	200,000		
13	Operational Event Type	200,000		
14	Credit Event Type		200,000	
15	Boundary Event Type			200,000
16	Boundary Event Type			200,000
17	Boundary Event Type			200,000
18	Boundary Event Type			200,000
19	Boundary Event Type			200,000

Responses to scenario 6

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	90,000		
2	Boundary Event Type			100,000
3	Boundary Event Type		10,000	90,000
4	Boundary Event Type		10,000	90,000
5	Boundary Event Type			100,000
6	Boundary Event Type		100,000	100,000
7	Boundary Event Type		10,000	90,000
8	Operational Event Type	100,000		
9	Operational Event Type	100,000		
10	Boundary Event Type		10,000	90,000
11	Boundary Event Type		10,000	90,000
12	Boundary Event Type	100,000		
13	Boundary Event Type	100,000		100,000
14	Boundary Event Type			
15	Boundary Event Type		10,000	90,000
16	Boundary Event Type		10,000	90,000

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
17	Boundary Event Type			100,000
18	Operational Event Type	100,000		
19	Boundary Event Type			100,000

Responses to scenario 7

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	300,000		
2	Operational Event Type	220,000		
3	Operational Event Type	80,000		
4	Operational Event Type	80,000		
5	Operational Event Type	300,000		
6	Operational Event Type	80,000		
7	Operational Event Type	80,000		
8	Operational Event Type	80,000		
9	Operational Event Type	80,000		
10	Boundary Event Type			80,000
11	Operational Event Type	80,000		
12	Operational Event Type	80,000		
13	Operational Event Type	300,000		
14	Operational Event Type	80,000		
15	Operational Event Type	80,000		
16	Operational Event Type	80,000		
17	Boundary Event Type			80,000
18	Operational Event Type	80,000		
19	Operational Event Type	220,000		

Responses to scenario 8

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Boundary Event Type			600,000
2	Boundary Event Type			450,000
3	Boundary Event Type			150,000
4	Boundary Event Type			150,000
5	Boundary Event Type			600,000
6	Boundary Event Type		150,000	150,000
7	Boundary Event Type		450,000	150,000
8	Credit Event Type		150,000	
9	Credit Event Type		450,000	
10	Boundary Event Type			150,000
11	Boundary Event Type			150,000
12	Boundary Event Type			150,000
13	Boundary Event Type			600,000
14	Credit Event Type		150,000	
15	Boundary Event Type			150,000
16	Boundary Event Type			150,000

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
17	Boundary Event Type			150,000
18	Boundary Event Type			150,000
19	Boundary Event Type			450,000

Responses to scenario 9

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Boundary Event Type			180,000
2	Boundary Event Type			90,000
3	Operational Event Type	90,000		
4	Boundary Event Type			90,000
5	Boundary Event Type			180,000
6	Operational Event Type	90,000		
7	Boundary Event Type			90,000
8	Operational Event Type	90,000		
9	Operational Event Type	90,000		
10	Boundary Event Type			90,000
11	Operational Event Type	90,000		
12	Operational Event Type	90,000		
13	Operational Event Type		180,000	
14	Boundary Event Type			90,000
15	Operational Event Type	90,000		
16	Boundary Event Type	-	-	90,000
17	Boundary Event Type			90,000
18	Boundary Event Type			90,000
19	Boundary Event Type			90,000

Responses to scenario 10

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	2,500,000		
2	Operational Event Type	2,500,000		
3	Operational Event Type	N/A	N/A	N/A
4	Operational Event Type	2,500,000		
5	Operational Event Type	2,500,000		
6	Operational Event Type	2,500,000		
7	Operational Event Type	2,500,000		
8	Operational Event Type	2,500,000		
9	Operational Event Type			
10	Credit Event Type		2,500,000	
11	Operational Event Type	2,500,000		
12	Operational Event Type	2,500,000		
13	Operational Event Type	5,000,000		
14	Credit Event Type		2,500,000	
15	Boundary Event Type			2,500,000
16	Credit Event Type		2,500,000	

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
17	Boundary Event Type			2,500,000
18	Boundary Event Type			2,500,000
19	Operational Event Type	2,500,000		

Responses to scenario 11

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Boundary Event Type			10,000
2	Boundary Event Type			10,000
3	Boundary Event Type			10,000
4	Operational Event Type	10,000		
5	Boundary Event Type			10,000
6	Credit Event Type		10,000	
7	Boundary Event Type			10,000
8	Credit Event Type		10,000	
9	Boundary Event Type			10,000
10	Boundary Event Type			10,000
11	Boundary Event Type			10,000
12	Credit Event Type		10,000	
13	Credit Event Type		10,000	
14	Boundary Event Type			10,000
15	Boundary Event Type			10,000
16	Boundary Event Type			10,000
17	Boundary Event Type			10,000
18	Boundary Event Type			10,000
19	Boundary Event Type			10,000

Responses to scenario 12

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Credit Event Type		200,000	
2	Boundary Event Type			200,000
3	Boundary Event Type			200,000
4	Boundary Event Type			200,000
5	Boundary Event Type			200,000
6	Boundary Event Type		200,000	200,000
7	Boundary Event Type			200,000
8	Boundary Event Type		100,000	100,000
9	Boundary Event Type			200,000
10	Boundary Event Type			200,000
11	Boundary Event Type			200,000
12	Credit Event Type		200,000	
13	Credit Event Type		200,000	
14	Credit Event Type		200,000	
15	Boundary Event Type			200,000
16	Boundary Event Type			200,000

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
17	Boundary Event Type			200,000
18	Boundary Event Type			200,000
19	Boundary Event Type			200,000

Responses to scenario 13

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	80,000		
2	Boundary Event Type			80,000
3	Operational Event Type	80,000		
4	Operational Event Type	80,000		
5	Operational Event Type	80,000		
6	Boundary Event Type		80,000	80,000
7	Boundary Event Type		Not sure	80,000
8	Operational Event Type	80,000		
9	Boundary Event Type			80,000
10	Operational Event Type	80,000		
11	Operational Event Type	80,000		
12	Operational Event Type	80,000		
13	Operational Event Type	80,000		
14	Boundary Event Type			80,000
15	Boundary Event Type	-	-	80,000
16	Operational Event Type	80,000	-	-
17	Boundary Event Type			80,000
18	Boundary Event Type			80,000
19	Operational Event Type	80,000		

Responses to scenario 14

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Credit Event Type	20,000.00		
2	Credit Event Type	20,000.00		
3	Credit Event Type	20,000.00		
4	Credit Event Type	20,000.00		
5	Credit Event Type	20,000.00		
6	Credit Event Type	20,000.00		
7	Credit Event Type	20,000.00		
8	Credit Event Type	20,000.00		
9	Credit Event Type	20,000.00		
10	Credit Event Type	20,000.00		
11	Credit Event Type	20,000.00		
12	Credit Event Type	20,000.00		
13	Credit Event Type	20,000.00		
14	Credit Event Type	20,000.00		

15	Credit Event Type	20,000.00		
16	Credit Event Type	20,000.00		
17	Credit Event Type	20,000.00		
18	Credit Event Type	20,000.00		
19	Credit Event Type	20,000.00		

Responses to scenario 15

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	13,000		
2	Operational Event Type	13,000		
3	Operational Event Type	13,000		
4	Operational Event Type	13,000		
5	Operational Event Type	13,000		
6	Operational Event Type	13,000		
7	Operational Event Type	13,000		
8	Operational Event Type	13,000		
9	Operational Event Type	13,000		
10	Operational Event Type	13,000		
11	Operational Event Type	13,000		
12	Operational Event Type	13,000		
13	Operational Event Type	13,000		
14	Boundary Event Type			13,000
15	Operational Event Type	13,000		
16	Operational Event Type	13,000		
17	Operational Event Type	13,000		
18	Operational Event Type	13,000		
19	Operational Event Type	13,000		

Responses to scenario 16

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
1	Operational Event Type	400,000		
2	Operational Event Type	400,000		
3	Operational Event Type	400,000		
4	Operational Event Type	400,000		
5	Credit Event Type		700,000	
6	Credit Event Type		400,000	
7	Operational Event Type	400,000		
8	Operational Event Type	400,000		
9	Operational Event Type	400,000		
10	Boundary Event Type			400,000
11	Operational Event Type	400,000		
12	Credit Event Type		400,000	
13	Credit Event Type		700,000	
14	Operational Event Type	400,000		
15	Operational Event Type	400,000		

Respondents	Event Type	Operational Portion	Credit Portion	Boundary Portion
16	Operational Event Type	400,000		
17	Boundary Event Type			400,000
18	Boundary Event Type			400,000
19	Operational Event Type	400,000		

Appendix 5

The BA410

OPERATIONAL RISK

(Confidential and not available for inspection by the public)

Name of bank.....

Financial year ended.....(yyyy-mm-dd)

BA410

Annually

(All amounts to be rounded off to the nearest R'000)

Advanced measurement approach Selected information relating to loss events	Line no.	Event type							Total (of col. 1 to 7)	Loss event as % of gross income	Memorandum: threshold applied i.r.o data collection ¹	
		Internal fraud	External fraud	Employment practices and workplace safety	Client, products and business practices	Damage to physical assets	Business disruption and system failures	Execution, delivery and process management			Lowest	Highest
		1	2	3	4	5	6	7	8	9	10	11
Corporate finance												
Number of events ²	1											
Gross loss amount ³	2											
Total recoveries ⁴	3											
Current financial year	4											
Prior financial years	5											
Net loss amount ⁵	6											
Maximum single loss ⁶	7											
Trading and sales												
Number of events ²	8											
Gross loss amount ³	9											
Total recoveries ⁴	10											
Current financial year	11											
Prior financial years	12											
Net loss amount ⁵	13											
Maximum single loss ⁶	14											
Retail brokerage												
Number of events ²	15											
Gross loss amount ³	16											
Total recoveries ⁴	17											
Current financial year	18											
Prior financial years	19											
Net loss amount ⁵	20											
Maximum single loss ⁶	21											
Commercial banking												
Number of events ²	22											
Gross loss amount ³	23											
Total recoveries ⁴	24											
Current financial year	25											
Prior financial years	26											
Net loss amount ⁵	27											
Maximum single loss ⁶	28											

(All amounts to be rounded off to the nearest R'000)

Advanced measurement approach Selected information relating to loss events	Line no.	Event type						Total (of col. 1 to 7)	Loss event as % of gross income	Memorandum: threshold applied i.r.o data collection ¹	
		Internal fraud	External fraud	Employment practices and workplace safety	Client, products and business practices	Damage to physical assets	Business disruption and system failures			Lowest	Highest
		1	2	3	4	5	6			10	11
Retail banking											
Number of events ²	29										
Gross loss amount ³	30										
Total recoveries ⁴	31										
Current financial year	32										
Prior financial years	33										
Net loss amount ⁵	34										
Maximum single loss ⁶	35										
Payment and settlement											
Number of events ²	36										
Gross loss amount ³	37										
Total recoveries ⁴	38										
Current financial year	39										
Prior financial years	40										
Net loss amount ⁵	41										
Maximum single loss ⁶	42										
Agency services											
Number of events ²	43										
Gross loss amount ³	44										
Total recoveries ⁴	45										
Current financial year	46										
Prior financial years	47										
Net loss amount ⁵	48										
Maximum single loss ⁶	49										
Asset management											
Number of events ²	50										
Gross loss amount ³	51										
Total recoveries ⁴	52										
Current financial year	53										
Prior financial years	54										
Net loss amount ⁵	55										
Maximum single loss ⁶	56										
Total i.r.o event types											
Number of events ²	57										
Gross loss amount ³	58										
Total recoveries ⁴	59										
Current financial year	60										
Prior financial years	61										
Net loss amount ⁵	62										
Maximum single loss ⁶	63										

1. Means the relevant gross loss threshold amount specified by the bank for data collection.
2. Means the total number of occurrences of the particular event during the relevant financial year.
3. Means the total loss amount before any recoveries are taken into consideration.
4. Include an amount recovered in terms of insurance.
5. Means gross loss amount less total recoveries in the current financial year.
6. Means the largest individual gross loss amount incurred during the relevant financial year.