

**The Management of Operational Risk
in
South African Banks**

by

Ja'nel Esterhuysen B.Comm (Hons)

Dissertation submitted for the partial fulfilment of the requirements for the degree

Master of Commerce

in the

School of Economics, Money and Banking and International Trade

& Centre for Business Mathematics & Informatics

at the

Potchefstroom University for Christian Higher Education

Supervisor: Prof Paul Styger

Potchefstroom

November, 2003



*To my parents,
Essie and Ria Esterhuysen*

*I firmly believe that any man's
finest hour is that moment when he
has worked his hart out in
good cause and lies on the battlefield exhausted,
but victorious.*

– Vince Lombardi

Abstract

One of the biggest problems South African banks are experiencing when managing operational risk is the lack of a single definition for operational risk. Operational risk can take many forms; for example computer system failure, the malfunction of an ATM or in some instances the long queues at a bank can be an operational risk. It is clear that banks lack sufficient information to distinguish between different operational risk events as well as other risk events like credit risk, market risk, etc. In other words, banks are experiencing great difficulties with the identification of operational risk in South Africa.

The study therefore aims to determine and construct a single definition of operational risk that will be sufficient for the assessment of operational risk management in South Africa. The study also aims to examine the existing as well as the possible methods to identify, quantify and measure operational risk. The main goal of this study is therefore to investigate the feasibility of capital provisions as a way of managing operational risk in South African banks, in other words the viability of the New Basel Capital Accord on South African banks. The methodology used includes a literature review, in-depth interviews and a case study on South African Retail Bank to determine and evaluate some of the most renowned indicators of operational risk in South Africa.

The first objective was to determine a single definition of operational risk in South Africa. As mentioned, South African banks are having great difficulties to find a single definition of operational risk and this is causing problems in identifying operational risks in South Africa. It is the view of this study that the Basel Committee's definition is not sufficient enough for operational risk management in South Africa; therefore there is a great need to find a single definition of operational risk in South African banks.

The second objective is to provide an overview of the Basel Committee and its Capital Accord, by focusing on one of the outstanding changes to the existing accord, which is the proposed explicit capital requirement for operational risk. It has been

established that the Basel Capital Accord is widely adopted around the world. Consequently, from the viewpoint of being competitive, it is to the advantage of a bank to adhere to the prescriptions of the Basel Capital Accord. However, to stay relevant, the Basel Capital Accord was due for a review. The Basel Committee released a proposal to replace the existing Basel Capital Accord with a more risk-sensitive framework. The new framework intends to improve safety and soundness in the financial system by placing more emphasis on banks' own internal control and management, the supervisory review process, and market discipline.

The third objective of this research was to present the theory of asset and liability management (ALM) within the unifying theme of operational risk management. It was indicated that capital is used to absorb an operational risk loss. The Asset and Liability Committee (ALCO) is responsible for the strategic management of a bank's balance sheet, therefore also ALM, and as capital forms part of the banks balance sheet, it is also the responsibility of the ALCO to manage the capital that is used as provision for an operational risk.

The fourth objective was to determine and evaluate the key risk indicators of operational risk in South Africa theoretically and then also by means of a case study on a South African Retail Bank and then to make some recommendations regarding the effective identification of the key indicators of operational risk in South Africa. It was indicated the challenge in identifying key operational risk indicators is to find indicators that is not only business-specific but are also firm wide indicators of operational risk. Recommendations on the effective identification of key operational risk indicators were made.

Key words: Operational Risk; Basel II; Operational Risk Indicators; South Africa

Acknowledgements

I wish to express my sincere thanks to everyone who contributed towards this dissertation. The following people/institutions deserve special mention:

My parents, my brother, and my sister, for their loving support and continued encouragement.

My supervisor, Prof Paul Styger, who always has great ideas and without whom this study would not be possible.

My friends at Patria Men's Residence, who always supported me through late nights, Saturdays, and difficult times especially those times when the thought of giving up seriously crossed my mind.

The School of Economics, Risk Management and International Trade, at the Potchefstroom University for presenting me with the opportunity to further my studies, especially Dr. Andrea Saayman, who always provided me with great ideas.

All the interviewees who took time to meet with me and who generously supplied the information that I required.

The Research Unit: Business Mathematics and Informatics at the Potchefstroom University for the financial support I received from them.

Ms Sorrina de Villiers who performed the proof-reading.

To the Lord, who gave me the ability and endurance to complete this dissertation.

The Author

Potchefstroom, 2003

Uittreksel

Een van die grootste probleme wat Suid-Afrikaanse banke ondervind met die bestuur van operasionele risiko is die afwesigheid van 'n enkelvoudige definisie van operasionele risiko. Operasionele risiko kan verskeie vorms aanneem. Voorbeelde kan die volgende wees: 'n onderbreking in rekenaarsistels, die foutwerking van 'n OTM, of in sekere gevalle kan 'n lang ry by 'n bank 'n operasionele risiko wees. Dit is duidelik dat banke nie altyd oor genoeg inligting beskik om duidelike onderskeid te tref tussen die verskillende operasionele risiko gebeure, sowel as ander risiko gebeure byvoorbeeld krediet- en mark risiko gebeure nie. Met ander woorde, banke ervaar probleme met die identifisering van operasionele risiko in Suid-Afrika.

Hierdie studie strewende daarna om 'n enkelvoudige definisie van operasionele risiko te bepaal sodat dit beter in 'n Suid-Afrikaanse konteks verstaan kan word. Hierdie studie strewende ook daarna om die bestaande sowel as die moontlike metodes vir die identifisering, kwantifisering en meting van operasionele risiko in Suid-Afrika te evalueer. Die primêre doelwit van hierdie studie is dan om die moontlikheid van kapitaalvoorsienings as 'n manier om operasionele risiko in Suid-Afrikaanse banke te bestuur, te ondersoek. Met ander woorde, die lewensvatbaarheid van die Basel II kapitaal akkoord in Suid-Afrikaanse banke word ondersoek. Die metodologie wat gebruik word sluit onder andere in 'n literatuur studie, diepgaande onderhoude sowel as 'n gevallestudie op 'n Suid-Afrikaanse kleinhandel bank.

Hierdie studie se eerste mikpunt was om 'n enkelvoudige definisie van operasionele risiko in Suid-Afrika te bepaal. Dit veroorsaak verdere probleme met die identifisering van operasionele risiko in Suid-Afrika. Hierdie studie sal aantoon dat die Basel kommittee se definisie nie voldoende is vir die bestuur van operasionele risiko in Suid-Afrika nie. Gevolglik bestaan die behoefte om 'n enkelvoudig definisie van operasionele risiko in Suid-Afrikaanse banke te bepaal.

Die tweede mikpunt was om 'n oorsig oor die Basel kommittee en sy kapitaal akkoord te gee deur te fokus op een van die uitstaande veranderings aan die bestaande raamwerk, naamlik 'n duidelike kapitaalvereiste vir operasionele risiko. Die Basel II

kapitaal akkoord is wêreldwyd aanvaarbaar. Gevolglik, met die doel om mededingend te bly, is dit tot 'n bank se voordeel om getrou te bly aan die vereistes van die Basel II kapitaal akkoord. Nietemin is dit moontlik om te sê dat dit nodig was om die bestaande Basel kapitaal akkoord te hersien. Die Basel kommittee het voorstelle uitgereik om die bestaande kapitaal akkoord met 'n meer risiko sensitiewe raamwerk te vervang.

Die derde mikpunt van hierdie studie was om die teorie van bate en laste bestuur (ALM) in die omvattende tema van operasionele risiko bestuur weer te gee. Daar is aanduiding gegee dat kapitaal gebruik word om verliese as gevolg van operasionele risiko te absorbeer. Die bate en laste kommittee (ALCO) is verantwoordelik vir die strategiese bestuur van 'n bank se balanstaat, met ander woorde verantwoordelik vir strategiese ALM. Kapitaal vorm deel van 'n bank se balanstaat, daarom is dit die verantwoordelikheid van die ALCO om die kapitaal te bestuur wat gebruik word om operasionele risiko verliese te absorbeer.

Die vierde mikpunt was om die sleutel risiko indikatore van operasionele risiko in Suid-Afrika teoreties te bepaal en dan te evalueer deur middel van 'n gevallestudie en dan verder sekere aanbevelings te maak aangaande die effektiewe identifisering van hierdie sleutel operasionele risiko indikatore. Die uitdaging met die identifisering van sleutel operasionele risiko indikatore is om risiko indikatore te identifiseer wat sowel as besigheids-wye en spesifieke besigheidslyn georiënteerde indikatore gebruik kan word. Aanbevelings is dan gemaak rakende die effektiewe identifisering van operasionele risiko indikatore in Suid-Afrika

Sleutel woorde: Operasionele risiko; Basel II, Operasionele Risiko Indikatore,
Suid-Afrika.

INDEX

Chapter 1

Introduction and Problem Statement

| | |
|---------------------------|---|
| 1.1 Background | 1 |
| 1.2 Problem Statement | 4 |
| 1.3 Aim of the Study | 5 |
| 1.4 Methodology | 6 |
| 1.4.1 Literature Review | 6 |
| 1.4.2 In-depth Interviews | 6 |
| 1.4.3 Questionnaires | 6 |
| 1.5 Scope of the Study | 7 |
| 1.6 Outline of the Study | 7 |

Chapter 2

Defining Operational Risk and the Basel Approach to Operational Risk management

| | |
|--|----|
| 2.1 Introduction | 9 |
| 2.2 Defining Operational Risk | 10 |
| 2.2.1 Formulating a single definition for Operational Risk | 10 |
| 2.2.1.1 People risk | 13 |
| 2.2.1.2 Process risk | 14 |
| 2.2.1.3 Technical risk | 14 |
| 2.2.1.4 Technological risk | 15 |
| 2.2.1.5 Physical risk | 15 |
| 2.2.2 Distinction between internal and external events | 16 |
| 2.2.2.1 Operational failure risk (Internal operational risk) | 16 |
| 2.2.2.2 Operational strategic risk (External operational risk) | 17 |
| 2.3 The Basel Committee | 18 |

| | |
|---|----|
| 2.3.1 Background to the Basel Committee | 19 |
| 2.3.2 Publications of the Basel Committee | 20 |
| 2.4 The New Basel Capital Accord | 21 |
| 2.4.1 Objectives of the New Basel Capital Accord | 23 |
| 2.4.2 Overall Capital | 25 |
| 2.4.3 The three pillars of the New Basel Capital Accord | 26 |
| 2.4.3.1 Pillar 1: Minimum capital requirements | 28 |
| 2.4.3.2 Pillar 2: Supervisory Review | 29 |
| 2.4.3.3 Pillar 3: Market discipline | 31 |
| 2.4.4 Approaches | 33 |
| 2.4.4.1 The Basic Indicator Approach | 34 |
| 2.4.4.2 The Standardized Approach | 35 |
| 2.4.4.3 The Internal Measurement Approach | 37 |
| 2.4.4.4 The Advanced Measurement Approach | 39 |
| 2.4.4.4.1 General Criteria | 40 |
| 2.4.4.4.2 Qualitative Standards | 41 |
| 2.4.4.4.3 Quantitative Standards | 41 |
| 2.4.5 Calibration of Capital Standards | 42 |
| 2.5 Proposed Practices Regarding Operational Risk Management | 44 |
| 2.5.1 The four key elements of operational risk management | 45 |
| 2.5.1.1 Development of an appropriate risk management environment | 45 |
| 2.5.1.2 Risk identification, Monitoring, Control and Measuring | 47 |
| 2.5.1.2.1 Risk Assessments | 48 |
| 2.5.1.2.2 Risk Mapping | 48 |
| 2.5.1.2.3 Key Risk Indicators | 49 |
| 2.5.1.2.4 Thresholds/limits | 49 |
| 2.5.1.2.5 Scorecards | 49 |
| 2.5.1.2.6 Control Activities | 49 |
| 2.5.1.3 Role of Supervisors | 50 |
| 2.5.1.4 Role of Disclosure | 51 |
| 2.5.1.5 Conclusion | 52 |

| | |
|--|----|
| 2.5.2 Management Structure and Responsibilities | 52 |
| 2.5.2.1 Background: Operational Risk Management Structures | 52 |
| 2.5.2.2 Basel's Guidance for management structure and responsibilities | 53 |
| 2.5.2.3 Conclusion | 54 |
| 2.6 Conclusion | 55 |

Chapter 3

Asset and Liability Management (ALM) for the Management of Operational Risk

| | |
|--|----|
| 3.1 Introduction | 57 |
| 3.2 Background | 58 |
| 3.3 Objectives of ALM | 62 |
| 3.3.1 Preservation and Enhancement of Net Worth | 63 |
| 3.3.2 Quantification of Risk in the Balance Sheet | 64 |
| 3.3.3 Management of Regulatory Capital | 66 |
| 3.3.4 Liquidity Management | 67 |
| 3.3.5 Actively Leveraging the Balance Sheet | 68 |
| 3.3.6 Managerial objectives in Financial Institutions | 69 |
| 3.3.6.1 Customer Needs Objectives | 70 |
| 3.3.6.2 Ownership Structure Objectives | 70 |
| 3.3.6.3 Evidence from research | 71 |
| 3.4 ALM Structures and Responsibilities | 72 |
| 3.4.1 Theories on the setting of Managerial Objectives | 72 |
| 3.4.1.1 The Classical Theory | 73 |
| 3.4.1.2 Agency Theory | 73 |
| 3.4.2 Forming an Asset and Liability Committee | 76 |
| 3.4.2.1 The ALCO in general | 76 |
| 3.4.2.2 ALCO in Strategic Management | 79 |
| 3.4.2.2.1 Strategic Management | 80 |
| 3.4.2.2.2 The ALM process | 81 |

| | |
|---|----|
| 3.4.2.3 The Strategic Planning Process | 85 |
| 3.5 Selection and Implementation of an Asset and Liability Simulation Model | 88 |
| 3.5.1 Develop a checklist of criteria and prioritise each item | 88 |
| 3.5.2 Planning the Implementation | 89 |
| 3.5.3 Vendor's support for the asset and liability simulation model | 90 |
| 3.5.4 Document preparation and the input process | 90 |
| 3.5.5 Assumptions | 90 |
| 3.5.6 Operating the Asset/Liability Model | 91 |
| 3.5.7 Standards and Internal Documentation | 92 |
| 3.5.7.1 Risk identification | 94 |
| 3.5.7.2 Risk evaluation | 95 |
| 3.5.7.3 Risk Control | 95 |
| 3.5.7.4 Risk Finance | 95 |
| 3.6 Conclusion | 96 |

Chapter 4

Key Risk Indicators: Cornerstones for Managing Operational Risk

| | |
|--|-----|
| 4.1 Introduction | 97 |
| 4.2 Key Risk Indicators (KRIs) vs. Key Performance Indicators (KPIs) | 98 |
| 4.2.1 Key Performance Indicators (KPIs) | 98 |
| 4.2.2 Key Performance Indicators (KPIs): Defined in a Risk-Return Framework. | 99 |
| 4.2.2.1 Return on Equity (ROE) | 101 |
| 4.2.2.1.1 Return on Assets (ROA) | 102 |
| 4.2.2.1.2 Equity Multiplier (EM) | 102 |
| 4.2.2.1.3 Stage two: Profit Margin and Asset Utilisation | 103 |
| 4.2.2.2 Conclusion | 105 |
| 4.2.3 Key Risk Indicators (KRIs) Defined | 105 |
| 4.2.3.1 The Basic of Key Risk Indicators (KRIs) | 107 |
| 4.2.3.1.1 Risk Indicators by Type | 107 |

| | |
|---|-----|
| 4.2.3.1.2 Risk Indicator by Risk Class | 108 |
| 4.2.3.1.2 Business-Specific vs. Firm wide KRIs | 108 |
| 4.3 Key Risk Indicators (KRIs) by type | 109 |
| 4.3.1 Inherent or Exposure Indicators | 109 |
| 4.3.2 Individual Management Control Indicators | 110 |
| 4.3.3 Composite Risk Indicators | 112 |
| 4.3.4 Operational Risk Model Factors | 115 |
| 4.3.5 Institutional Considerations | 115 |
| 4.3.6 Practical Considerations Regarding Definition, Data Collection, Standards, and Emphasis of KRIs. | 117 |
| 4.4 Scorecards System: The Nexus of Risk Assessments and Risk Indicators | 118 |
| 4.4.1 Creating KRI Scores from Qualitative Reviews at Dresdner Bank | 119 |
| 4.4.2 Converting Risk Scores to Heat Maps at Deutsche Bank | 121 |
| 4.4.3 Back-Testing Operational Risk Indicators and Scores: Some Case Examples | 123 |
| 4.4.4 Implementing a System of Operational Risk Indicators | 126 |
| 4.4.4.1 Identify and Define | 126 |
| 4.4.4.2 Data Collection, Tracking and Analysis | 126 |
| 4.4.4.3 Validation of Operational Risk Indicators | 126 |
| 4.4.5 Conclusion | 127 |
| 4.5 Identifying Key Risk Indicators KRIs | 128 |
| 4.5.1 Key Risk Indicators (KRIs): Basic Facts in Identifying KRIs | 128 |
| 4.5.2 Identifying KRIs in a Retail Bank | 131 |
| 4.5.2.1 Different Divisions of a Bank | 131 |
| 4.5.2.2 Elements in a Retail Division of a Bank | 134 |
| 4.5.2.3 KRIs of a Retail Division | 135 |
| 4.5.2.3.1 Key Risk Indicators (KRIs): Home Loans | 137 |
| 4.5.2.3.2 Key Risk Indicators (KRIs): Card Services | 138 |
| 4.5.2.3.3 Key Risk Indicators (KRIs); Direct Banking | 139 |
| 4.5.2.3.4 Key Risk Indicators (KRIs): Branch Network | 141 |

| | |
|---|-----|
| 4.5.2.3.5 Key Risk Indicators (KRIs): Bank Products (Savings & Current Account) | 142 |
| 4.5.2.3.6 Key Risk Indicators (KRIs): Marketing | 143 |
| 4.5.2.3.7 Key Risk Indicators (KRIs): Branch Insurance | 144 |
| 4.5.2.3.8 Key Risk Indicators (KRIs): Vehicle Finance | 144 |
| 4.6 Conclusion | 146 |

Chapter 5

Key Indicators of Operational Risk in a Retail Bank of South Africa: A Case Study

| | |
|---|-----|
| 5.1 Introduction | 148 |
| 5.2 Key operational risk indicators in a Retail Bank | 149 |
| 5.2.1 Employee indicators | 152 |
| 5.2.1.1 Employee turnover | 152 |
| 5.2.1.2 Overtime worked by employees | 153 |
| 5.2.1.3 Vacation and absenteeism rate | 153 |
| 5.2.1.4 Number of approved positions vs. actual compliment | 153 |
| 5.2.1.5 Number of temporary personnel vs. The total number of personnel | 153 |
| 5.2.1.6 Junior and senior staff tenure individual indicator | 153 |
| 5.2.1.7 Number of transactions per staff member | 154 |
| 5.2.1.8 Total for specific delivery failures | 154 |
| 5.2.1.9 Technology management control risk indicator | 154 |
| 5.2.2 Customer Indicators | 154 |
| 5.2.2.1 Customer complaints | 154 |
| 5.2.2.2 Repeat business vs. New business | 155 |
| 5.2.2.3 Application turnover time (customer satisfaction) | 155 |
| 5.2.2.4 Customer satisfaction survey | 155 |
| 5.2.2.5 Operating turnover | 155 |
| 5.2.2.6 Aged confirmations | 156 |
| 5.2.2.7 The number of cross selling | 156 |
| 5.2.2.8 Increase/decrease in the number of customers | 156 |

| | |
|---|-----|
| 5.2.3 Product indicators | 156 |
| 5.2.3.1 Product complexity | 156 |
| 5.2.3.2 Range of products | 157 |
| 5.2.3.3 Number of settlement fails | 157 |
| 5.2.3.4 Non-performance with compliance with policy | 157 |
| 5.2.3.5 The number of new accounts opened | 157 |
| 5.2.3.6 The number of accounts closed | 158 |
| 5.2.3.7 Increase in the number of lost and stolen ATM (credit cards) cards | 158 |
| 5.2.3.8 The total number of active credit card accounts | 158 |
| 5.2.3.9 Total applications received vs. Total applications approved | 158 |
| 5.2.3.10 Total applications denied | 158 |
| 5.2.3.11 Increase in the number of transactions | 159 |
| 5.2.4 System indicators | 159 |
| 5.2.4.1 IT-system downtime | 159 |
| 5.2.4.2 Number of hacking attempts detected | 159 |
| 5.2.4.3 Number of points of entry into the system | 159 |
| 5.2.4.4 Number of system problems detected | 160 |
| 5.2.4.5 Intranet between branches | 160 |
| 5.2.4.6 Number and value of Internet transactions | 160 |
| 5.2.5 Other indicators | 160 |
| 5.2.5.1 Number of critical/unacceptable ratings/findings received from completed audits | 161 |
| 5.2.5.2 Concentration of activities (transactions) | 161 |
| 5.2.5.3 Movement in market share | 161 |
| 5.2.5.4 Percentage movement in the total book value | 161 |
| 5.2.5.5 Number and value of physical losses | 162 |
| 5.3 Practical guidelines on designing a questionnaire | 162 |
| 5.3.1 Background on designing a questionnaire | 164 |
| 5.3.1.1 The purpose of a questionnaire | 164 |
| 5.3.1.2 The environment of the respondent | 164 |
| 5.3.1.3 Data gathering | 165 |

| | |
|---|-----|
| 5.3.2 The typology of a questionnaire | 165 |
| 5.3.2.1 Description of the occurrences | 165 |
| 5.3.2.2 Elucidation of occurrence | 166 |
| 5.3.2.3 Planning/determining of the policy | 167 |
| 5.3.2.4 Predicting of behaviour | 167 |
| 5.3.3 Question content and phrasing | 167 |
| 5.3.4 Question sequence of the questionnaire | 168 |
| 5.3.5 The question format of a questionnaire | 170 |
| 5.3.5.1 Dichotomous questions | 170 |
| 5.3.5.2 Multiple-choice questions with single answers | 171 |
| 5.3.5.3 Multiple-choice questions with multiple answers | 171 |
| 5.3.5.4 Checklists | 172 |
| 5.3.5.5 Rankings | 172 |
| 5.3.5.6 Grids | 172 |
| 5.3.5.7 Scaled questions | 173 |
| 5.3.6 Pre-testing | 174 |
| 5.3.7 Conclusion | 175 |
| 5.4 Results of questionnaires on KRIs in a Retail Bank | 175 |
| 5.4.1 Employee indicators | 176 |
| 5.4.2 Customer indicators | 178 |
| 5.4.3 Product indicators | 181 |
| 5.4.4 System indicators | 183 |
| 5.4.5 Other indicators of operational risk | 185 |
| 5.4.6 Overall results | 187 |
| 5.5 Conclusion | 189 |

| | | |
|----------------------|-------------------|-----|
| | Chapter 6 | |
| | Conclusion | |
| 6.1 Introduction | | 190 |
| 6.2 Conclusions | | 191 |
| 6.3 Further Research | | 194 |
| | | |
| Appendix 1 | | 196 |
| Appendix 2 | | 197 |
| Appendix 3 | | 207 |
| | | |
| References | | 209 |

List of Figures

Chapter 2

Defining Operational Risk and the Basel Approach to Operational Risk Management

| | |
|---|----|
| Figure 2.1 Two Broad Categories of Operational Risk | 17 |
| Figure 2.2 The Three Pillars of the New Basel Capital Accord | 32 |
| Figure 2.3 The Four Elements of Operational Risk Management | 45 |

Chapter 3

Asset and Liability Management for the Management of Operational Risk

| | |
|---|----|
| Figure 3.1 The Balance Sheet | 61 |
| Figure 3.2 The Fundamental Objectives of ALM | 62 |
| Figure 3.3 The Major Components of Risk in the Balance Sheet | 65 |
| Figure 3.4 Asset and Liability Management Structure | 77 |
| Figure 3.5 The ALM Process | 83 |
| Figure 3.6 The Strategic Planning Process | 86 |
| Figure 3.7 Overview of the ALM Simulation Model | 93 |

Chapter 4

Key Risk Indicators: Cornerstones for Managing Operational Risk

| | |
|---|-----|
| Figure 4.1 A Risk-Return view of the overall bank performance | 100 |
| Figure 4.2 Key Risk Indicators: A Firm wide vs. Business-Specific | 108 |
| Figure 4.3 Risk Indicators: User Number Require Training | 111 |
| Figure 4.4 Business-Specific Indicators: Overtime Worked | 112 |
| Figure 4.5 Composite Risk Indicators: Training Dollars vs. Employee Error Rates Vs. Customer Complaints | 113 |
| Figure 4.6 Composite Risk Indicators: Number of Skilled Technology Users vs. Industry Benchmarks | 114 |

| | |
|---|-----|
| Figure 4.7 Converting Risk Scores to Heat Maps Deutsche Bank | 122 |
| Figure 4.8 Elements of a Retail Bank | 134 |
| Figure 4.9 Employee Indicators | 135 |

Chapter 5

Key Indicators of Operational Risk in a Retail Bank of South Africa: A Case Study

| | |
|--|-----|
| Figure 5.1 Typical operational risk indicators: Retail Bank | 149 |
| Figure 5.2 The integrated management of operational risk | 150 |
| Figure 5.3 Indicators of operational risk: Retail Bank | 151 |
| Figure 5.4 Questionnaire on operational risk indicators | 163 |
| Figure 5.5 The typology of a questionnaire | 166 |
| Figure 5.6 Multiple-choice questions with single answers | 171 |
| Figure 5.7 Multiple-choice questions with multiple answers | 171 |
| Figure 5.8 Grids | 173 |
| Figure 5.9 Ratings: Employee indicators | 177 |
| Figure 5.10 Percentage rating: Employee indicators | 178 |
| Figure 5.11 Ratings: Customer indicators | 180 |
| Figure 5.12 Percentage rating: Customer indicators | 180 |
| Figure 5.13 Ratings: Product indicators | 182 |
| Figure 5.14 Percentage rating: Product indicators | 183 |
| Figure 5.15 Ratings: System indicators | 184 |
| Figure 5.16 Percentage rating: System indicators | 185 |
| Figure 5.17 Ratings: Other indicators of operational risk | 186 |
| Figure 5.18 Percentage rating: Other indicators of operational risk | 187 |
| Figure 5.19 Overall ratings | 188 |
| Figure 5.20 Overall percentage rating | 189 |

List Of Tables

Chapter 2

Defining Operational Risk and the Basel Approach to Operational Risk Management

| | |
|--|----|
| Table 2.1 Rationale for a new accord: the need for more flexibility and sensitivity | 27 |
| Table 2.2 Beta factors for Business lines | 37 |

Chapter 3

Asset and Liability Management for the Management of Operational Risk

| | |
|---|----|
| Table 3.1 Example of a Growth Assumption | 91 |
|---|----|

Chapter 4

Key Risk Indicators: Cornerstones for Managing Operational Risk

| | |
|---|-----|
| Table 4.1 Return on Equity (ROE) Model | 104 |
| Table 4.2 Risk Subcategory – Human Capital | 120 |
| Table 4.3 Risk Subcategory – Unauthorized Activities | 120 |
| Table 4.4 Business Lines of a Bank and Risk Indicators | 132 |
| Table 4.5 Relative Weightings of the Business Lines | 133 |

Chapter 5

Key Indicators of Operational Risk in a Retail Bank of South Africa: A Case Study

| | |
|--|-----|
| Table 5.1 Ratings of employee indicators | 176 |
| Table 5.2 Ratings of customer indicators | 179 |
| Table 5.3 Ratings of product indicators | 181 |
| Table 5.4 Ratings of system indicators | 183 |
| Table 5.5 Ratings of other indicators of operational risk | 186 |
| Table 5.6 Overall ratings | 188 |

Chapter 1

Introduction and Problem Statement

*“Risk Management can help you seize opportunity,
not just avoid danger,” (Olsson, 2002: xiii).*

1.1 Background

Operational risk has been a challenge for financial service institutions for years, but according to Hoffman (2002: 1), it has not been recognized for its full potential until recently because of the high infrequency of losses. Large loss events have occurred before. For example in 1995 the actions of a single trader at Barings Bank, who was able to take extremely risky positions in the market without authority or detection, led to \$1.5 billion in losses that brought about the liquidation of Barings Bank (Crouhy *et al.*, 1998: 476). Another example is the Allied Irish Bank’s loss of \$750 million due to rogue trading (Olsson, 2002: 225). One-off events have caused both mass embarrassment and/or collapse, but they were widely considered to be extremely remote and perhaps even aberrations. For example the terrorist attacks on the World Trade Centre in 2001, where over 6000 lives were lost and an estimated loss of \$20 billion to business (Hoffman, 2002: xxvii). Thus, operational risk did not attract such significant attention until the 1990’s, when a series of life threatening or fatal operational loss events at a number of different financial institutions caused reorganization, a management shake-up or a refocus on control environments, and thus a new focus on operational risk.

At one time operational risk could be defined as an area characterized by frequent, small and predictable events such as processing errors, reconciliation breaks, or system glitches, accompanied by the one-in-five-year large system failure and loss, defalcation,

or customer dispute (Hoffman, 2002: 1). More recently however, these large loss events have become far too commonplace and visible in the industry news for management's comfort. Couple the above-mentioned with the advent of increased management and directorship accountability forced by legal actions against officers and directors and a chain reaction has been set in motion.

According to Hoffman (2002: 2) recent trends in the business complexity, highly visible operational losses, and the need to manage risk associated with them, have given rise to a new field called operational risk management (ORM). Many of its underlying component parts, like the existence of various control functions, have been in place for years. There is a new recognition however, of the importance identifying, understanding, and measuring operational risks more intelligently, as well as weaving an effective web of approaches to managing operational risks given their complexity and potentially devastating impact on institutions today.

As Marshall (2001: 35) puts it, much of the impetus for operational risk management has come from regulators and industry wide groups. In 1993, one of the most important industry groups – the Group of Thirty (G-30), an elite group of global investment banks – issued a highly influential report outlining twenty recommendations for good practice for derivative dealers and end users (Medova & Kyriacou, 2002: 249). Although its focus was derivatives, its conclusions have set the tone for securities dealing and processing as a whole. In particular, it makes a strong case for precisely defined risk management policies covering the scope and authorization of trading, acceptable control, product valuation and risk management approaches, and the critical importance of adequate disclosure and active senior management involvement.

As a result of the increasing awareness of the importance of operations and the risk to business, the Basel Committee on Banking Supervision¹ decided to include an explicit capital requirement for operational risk when undertaking a revision of the Basel Capital Accord¹. The revision started in 1998, and the first consultative document was published

in June 1999 (Cruz, 2002: 271). The introduction of this capital requirement took by surprise a good part of the financial services industry that did not believe that this would happen (Olsson, 2002: 225). Under the current accord it was assumed that the credit risk charge implicitly covers other risks including operational risk (Cruz, 2002: 271).

In addition to the above-mentioned, the focused discussion on current practices in operational risk management in the consultative document² of 1998, resulted from a working group of the Basel Committee. Thirty major banks were interviewed to discover their approaches to operational risk management. Although many of the correspondent banks were quickly moving in the direction of more formal approaches, few had formal, integrated systems for measuring operational risk. The report also suggested that most operational losses were due to breakdowns of internal controls and corporate governance. As Marshall (2001: 36) puts it, the challenge noted in the report was the integration of these disparate factors into a coherent picture of the operational risk of the business.

Along with the established capital charges for market and credit risks, the Basel Committee is also proposing an explicit capital charge to guard the banks against operational risk. The response from the banks has been an increased number of operational risk management initiatives with corresponding efforts to formulate a framework for capital allocation for operational risk (Medova & Kyriacou, 2002: 247). The above-mentioned proposing by the Basel Committee also contains a model for calculating the economic capital against extreme risks, which is the contribution to the quantification of operational risk. As Matten (2000: 81) puts it, although the mechanisms for measuring risk may differ between an individual institution's view and the regulatory approach, the philosophy is the same: Capital must be held in a sufficient amount to absorb large unexpected losses, to protect the depositors, and ensure the ongoing viability of the financial system.

¹ The Basel Committee on Banking Supervision as well as the Basel Capital Accord will be examined in chapter 2.

² The Basel Committee is issuing a proposal for a new capital adequacy standard framework to replace the existing 1988 Accord, which requires banks to hold capital equal to 8% of weighted assets against credit risk. The new framework is intended to cover capital adequacy standards for credit, market and operational risks.

Managing operational risk can only be done on a firm wide basis. This is because, as Hussain (2000: 5-6) points out, it includes the entire processes of policies, culture, procedures, expertise and systems that an institution needs in order to manage all the risks resulting from its financial transactions. In fact, in order to effectively manage market and credit risks, it is necessary to have the relevant skills and expertise in staff, technical and organizational infrastructure as well as monitoring and control systems. As all of these are components of operational risk, it becomes apparent that an integrated risk management approach needs to focus on operational risk.

1.2 Problem statement

One of the biggest problems managers are experiencing when managing operational risk in South African banks is the lack of a single definition for operational risk. Operational risk can take many forms; for example a computer system failure, the malfunction of an ATM or in some instances the long queues at a bank can be an operational risk. It is clear that banks lack sufficient information to distinguish between different operational risk events as well as other risk events like credit risk, market risk, etc. In other words, banks are experiencing difficulties with the identification of an operational risk event.

Another key problem is the quantification of operational risk. As mentioned, operational risk can take many forms; for example a computer breakdown for which it is difficult to quantify the expected loss (EL). EL is the product of the probability of the event occurring, which will be referred to as the “likelihood”, and the cost of the event, if it does occur, will be referred to as the “severity”. Both these numbers are difficult to calculate for an event like a computer breakdown, which occurs infrequently and in the form of a discrete event.

In addition to the above-mentioned, the attention given to the operational risk by the proposed New Capital Accord of the Basel Committee, initiated the idea to research operational risk as a separate risk category and to discover what the implications of capital requirement for operational risk will be. To be able to determine how much

capital must be allocated specifically for operational risk, it must be possible to measure operational risk. Therefore the available methods for the identification, quantification as well as the measurement of operational risk in South African banks have to be identified and evaluated.

1.3 Aim of the study

In the problem statement, it was indicated that there is a lack of a single definition of operational risk in the South African banking industry. The study therefore aims to determine and construct a single definition of operational risk that will be sufficient for the assessment of operational risk management in South African banks. The study also aims to identify and examine some of the key indicators of operational risk and to determine their importance in identifying operational risks in South African banks. The study further aims to evaluate the viability of capital provisions as a way of managing operational risk in South African banks, in other words the feasibility of the New Basel Capital Accord³ on South African banks.

In order to determine whether the above-mentioned is viable, this study set the following objectives:

- The first objective is to determine a single definition of operational risk in South Africa in order to better understand the management of operational risk in South African banks.
- The second objective is to provide an overview of the Basel Committee and its Capital Accord, by focusing on one of the outstanding changes to the existing accord, which is the proposed explicit capital requirement for operational risk.
- The third objective is to investigate the role that a bank's Asset and Liability Management (ALM) plays in operational risk management in South African

³ The New Basel Capital Accord is providing a capital adequacy standard for the management of operational risk. The New Basel Capital Accord will also be examined in chapter 2.

banks and to determine the importance of the Asset and Liability Committee (ALCO) in operational risk management.

- The fourth objective is to identify and evaluate some of the key indicators of operational risk in South African banks and then also to determine their viability by means of a case study on a South African Retail Bank.

1.4 Methodology

In order to reach the goal and objectives, the methodology implemented in the study includes a literature review, in depth interviews with current experts and relevant parties in the South African banking sector, as well as a case study to determine and evaluate some of the key risk indicators of operational risk in South African banks.

1.4.1 Literature review

The literature review focuses on the concepts of operational risk, operational risk management, Asset and Liability Management (ALM) and capital allocation. Sources include books, published articles, media reports, company reports, relevant acts and accounting standards as well as the Internet.

The literature review investigates operational risk in the banking system in terms of the measurement, the need for, the sources and management of operational risk as well as the Basel Committee's recommendations for the management of operational risk in terms of the New Basel Capital Accord.

1.4.2 In-depth interviews

Due to a lack of sufficient literature on the operational risk management in South African banks, in-depth interviews were held with relevant market players. The goal of the interviews was to identify some of the most renowned key indicators of operational risk in South African banks and to determine their viability.

1.4.3 Questionnaires

Questionnaires were handed out to key players in operational risk management in a South African Retail Bank to determine the viability of some of the most renowned indicators of operational risk. These questionnaires are based on a seven point Likert scale and the development of these questionnaires will be thoroughly discussed in chapter 5.

1.5 Scope of the study

The study focuses on the situation of the “big 4” banks in South Africa, which include ABSA, Standard Bank (Case Study), Nedcor and FirstRand (Reuters, 2002a: 3). The study does not focus on the situation of the small banks in South Africa, which is defined as a bank with total assets of between R1 billion and R7 billion (Reuters, 2002a: 3).

The study only focuses on the problems the “big 4” banks face with regard to operational risk and the investigation regarding the other risks (credit risk, market risk, interest rate risk, etc.) and the magnitude of these risks do not fall within the scope of this study. The study will therefore only make recommendations regarding the management of operational risk in the “big 4” banks in South Africa.

1.6 Outline of the study

Chapter 2 provides a single definition of operational risk, which is based on eight other published definitions of operational risk. Chapter 2 also then provides an overview of the Basel Committee and its Capital Accord as the authority in banking regulation for internationally active banks. It focuses on one of the outstanding changes to the existing accord, which is the proposed explicit capital requirement for operational risk. The chapter outlines the three pillars on which the revised accord will be based and explain the concept of eligible capital. Finally, chapter 2 also examines the Basel Committee’s principles for the management of operational risk.

Chapter 3 investigates the role that the bank's Asset and Liability Management (ALM) play in risk management; especially in operational risk management. In chapter 3, the meaning, definition and the scope of ALM is examined and the Asset and Liability Committee (ALCO) is identified as the personnel who are responsible for ALM in banks. The role that the ALCO plays in operational risk management in South African banks is also examined in chapter 3.

Chapter 4 evaluates the difference between key risk indicators (KRIs) and key performance indicators (KPIs). Chapter 4 then theoretically evaluates the KRIs of operational risk and provides an in-depth look at the different categories of KRIs. Chapter 4 also identifies some of the most renowned KRIs of operational risk in South African banks

Chapter 5 is done on a practical basis. It will determine and evaluate the most important key indicators of operational risk in a South African Retail Bank by means of a questionnaire, and will also make recommendations regarding these risk indicators.

Chapter 6 concludes the study and also makes recommendations regarding the management of operational risk in South African banks.

Chapter 2

Defining Operational Risk and The Basel Approach to Operational Risk Management

“Looking ahead, the risks that we face are increasing in scale and complexity. Unfortunately our ability to respond has not kept pace” (Olsson, 2002: 259).

2.1 Introduction

During the past few decades, risk management and risk control have emerged as a critical important management concern. The Basel Committee has made a substantial contribution to the risk management and mitigation process in banking. Before the formal guidance of the Basel Committee, regulatory requirements were basic and there was little focus on capital adequacy.

An important new development in the Basel Committee’s approach to risk management is to extend the focus of risk management to operational risk (BIS, 2001: 3). It has been noted that operational risk management is the ‘last piece in the puzzle’ for banks wishing to both protect themselves and to optimise their risk taking behaviour. However, although the importance of managing operational risk is realized, many practical problems exist.

The industry comments (BIS, 2001: 3) on the proposed treatment of operational risk in the New Basel Capital Accord give an indication of the challenges that are faced when managing operational risk and when determining adequate capital to cover operational

risk. Before this study can proceed to evaluate the Basel Committee and its proposals for operational risk, it is important that operational risk is first clearly defined. As mentioned in the problem statement, the identification of an operational risk event is one of the major concerns regarding operational risk, probably because of the lack of a single definition of operational risk. The following section of chapter 2 therefore aims to determine a single definition of operational risk, in order to better understand what events can be regarded as operational risk events.

2.2 Defining Operational Risk

The Basel Committee has adopted a standard industry definition of operational risk namely, *“the risk a of direct or indirect loss resulting from adequate or failed internal processes, people and systems or from external events”* (BIS, 2001b: 2). This definition includes legal risk, but for the purposes of minimum regulatory operational risk capital charge, strategic and reputation risk it is not included (BIS, 2001b: 2). The above-mentioned definition is one of the most frequent used definitions of operational risk, but it is the view of this study that it is not adequate to evaluate operational risk by using only this definition. The following section of this chapter will examine operational risk by providing eight examples of definitions and will then aim to formulate a single definition of operational risk based on these eight stated definitions. The following sections will also make a distinction between the internal and external operational risks.

2.2.1 Formulating a single definition of operational risk

The aim of this section of chapter 2 is to formulate a single definition of operational risk, but for a better understanding of the definition of operational risk, it is important to first have a clear view on what events can be regarded as possible operational risk events. The BIS (1998: 12) affirmed the following possible causes/events of operational risks:

- If it is not well controlled, the use of more highly automated technology has the potential to transform risk from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems.
- Growth of e-commerce brings with it potential risks (e.g., external fraud and other system securities issues) that are not yet fully understood.
- Large-scale mergers and consolidations test the viability of new or integrated systems and have resulted in some noteworthy problems.
- The emergence of banks acting as very large-volume services providers creates the need for continual maintenance of high grade internal controls and back-up systems.
- Banks might engage in risk mitigation techniques (e.g., collateral, credit derivatives, and asset securitisation) to optimise the exposure to market risk and credit risk, but which in turn may produce other forms of risk.
- The growing use of outsourcing arrangements and the participation in third party clearing systems can mitigate some risk but can also present significant other risks to banks.

With the above-mentioned in mind this section can proceed to provide eight examples of definitions of operational risk and then construct a single definition based on these definitions:

- *“In the concept of a Trading or Financial institution, it refers to a range of possible failures in the operations of the institution that are not related directly to market or credit risk. These failures include computer breakdown, a bug in the key piece of a computer system, etc.”* (Crouhy et al, 1998: 475).
- *“Operational risk is defined as the measure of the link between a firm’s business activities and the variation of the business results.”* (King, 2000: 7).

- *“Operational risks are those risks of our interconnected world becoming disrupted in a large scale, or locally in our workplaces and our neighbourhoods through acts of man or by nature,” (Hoffman, 2002: xxvi).*
- *“Operational risk is defined as a consequence of critical contingencies, most of which are quantitative in nature,” (Medova & Kyriacou, 2002: 247).*
- *“Operational risk is trigger points in manufacturing plants and can usually be measured as can several of staff matters – for example overtime levels, number of vacancies, etc.,” (Olsson, 2002: 127).*
- *“Operational risks are those risks of malfunctions of the information systems, reporting systems, internal risk-monitoring rules and internal procedures to take timely corrective actions, or compliance with internal risk policy rules,” (Bessis, 2001: 20).*
- *Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events,” (BIS, 2001a: 2).*
- *Operational risk refers to the possibility that operating expenses might vary significantly from what is expected, producing a decline in net income and firm value,” (Koch, 1997: 108).*

From the above, operational risk can then be defined as the risk of a external or internal loss resulting from a range of possible events, which include a human or employee error, a disruption in the work environment, a breakdown of processes, a malfunction in the information system and or a computer system failure due to ineffective technology.

Bessis (2001: 21) stated four levels at which an operational risk can appear and include the following:

- People.
- Processes.
- Technical.
- Technological.

The following sections therefore want to evaluate the above-given definition of operational risk in terms of these four levels, but also want to include an additional level to the above-mentioned, which is the physical level of operational risk.

2.2.1.1 People risk

People risk is the risk due to a human (employee) error, a lack of expertise and fraud, including a lack of compliance with existing procedures and policies (Bessis, 2001: 21). In other words it is the risk associated with the employment of people (e.g., that an employee intentionally or unintentionally causes loss to a firm; losses involving employment liabilities) and is regarded as the first level of operational risk (Crouhy *et al*, 1998: 41). In the formulated definition of operational risk the term “human and employee error” are mentioned and it is important that these two terms must be understood in terms of the different appearances that it can have, which include the following (Crouhy *et al*, 1998: 41):

- Employee errors, which cause a disruption in the business processes due to an employee’s mistakes (for example, documentation and keying-in errors).
- Employee misdeeds, which cause a disruption in the business processes resulting from an employee’s dishonest, fraudulent or malicious activities against a firm.
- Employee unavailability, which results in a disruption in the business processes due to personnel not being available at vital times, or the risk of key people leaving the institution.

- Employment practices which cause losses to a firm due to discrimination within the institution, harassment of employees or other civil rights abuses, wrongful termination of employees, and employee health and safety issues.

2.2.1.2 Process risk

Process risk is as a result of a malfunction in the information system and can be external or internal (King, 2000: 24). The scope of process risk includes (Bessis, 2001: 21):

- Inadequate procedures and controls for reporting, monitoring and decision-making.
- Inadequate procedures on processing information, such as errors in booking transactions and failure to scrutinize legal documentation.
- Organizational deficiencies.
- Errors in the recording process of transactions.
- The technical deficiencies of the information system or the risk measures.
- Risk surveillance and excess limits: management deficiencies in risk monitoring, such as not providing the right insensitive to report risks, or not abiding by the procedures and policies in force.

2.2.1.3 Technical risk

Technical risk is the third level of operational risk and relates to model errors, implementation and the absence of adequate tools for measuring risks (Bessis, 2001: 21). A technical risk can also be the risk of a loss of electricity at a crucial time or the incorrect instalment of certain software, or an outdated computer (King, 2000: 34).

2.2.1.4 Technology risks

Technology risk relates to deficiencies of the information system and system failure (Bessis, 2001: 21). This risk level is almost the same as technical risk but is regarded as

more advanced and also more complex. Some examples of specific loss scenarios of technology risks include external disruption and system maintenance. External disruption is a disruption in the business processes due to system failures outside the firm, for example (Crouhy et al, 1998: 44):

- Failures of exchanges (equities, commodities, etc.).
- Third-party system failure.

System maintenance is a disruption in the business processes due to the institution's technological (hardware and software) failures, for example (Crouhy et al, 1998: 44):

- Software problems.
- System outdated and unable to handle the institution's needs.
- System integration risks.
- System developments being delayed and over budget.

2.2.1.5 Physical risk

The physical risk level or category is the fifth risk category of operational risk but is not included in the four risk levels stated by Bessis (2000: 21) (see section 2.2.1), but it is the believe that it also plays an integral part in operational risk. This risk level is the risk to an institution's business processes and key facilities due to unavailable or improper maintenance of physical assets (Crouhy et al, 1998: 46). Some examples of specific loss scenarios are crime, disasters and product/facility damage, and can cause a temporal or permanent disruption in the work environment (Crouhy et al, 1998: 46):

- Disasters include natural disasters like earthquakes, tornados, and hurricanes and unnatural disasters like bombs, fires and explosions (King, 2000: 36).
- Product/facility damage is damage to physical plant, facility, or product leading to losses, for example, contamination (i.e., air water, raw materials) and product recalls (Crouhy et al, 1998: 46).

The above-mentioned are regarded as the different levels or categories of operational risk and it is important for managers to distinguish between these categories in order to effectively identify an operational risk event. To further the evaluation of the definition of operational risk it is important to distinguish between the terms operational failure risk (internal) and operational strategic risk (external). The following section will make that distinction.

2.2.2 Distinction between external and internal operational risk

In addition to section 2.2.1, this section wants to clarify what events can be regarded as internal or external operational risks event. Operational risk covers such a wide area that it is important to subdivide operational risk into two components, operational strategic risk and operational failure risk, in other words, internal operational risks and external operational risks.

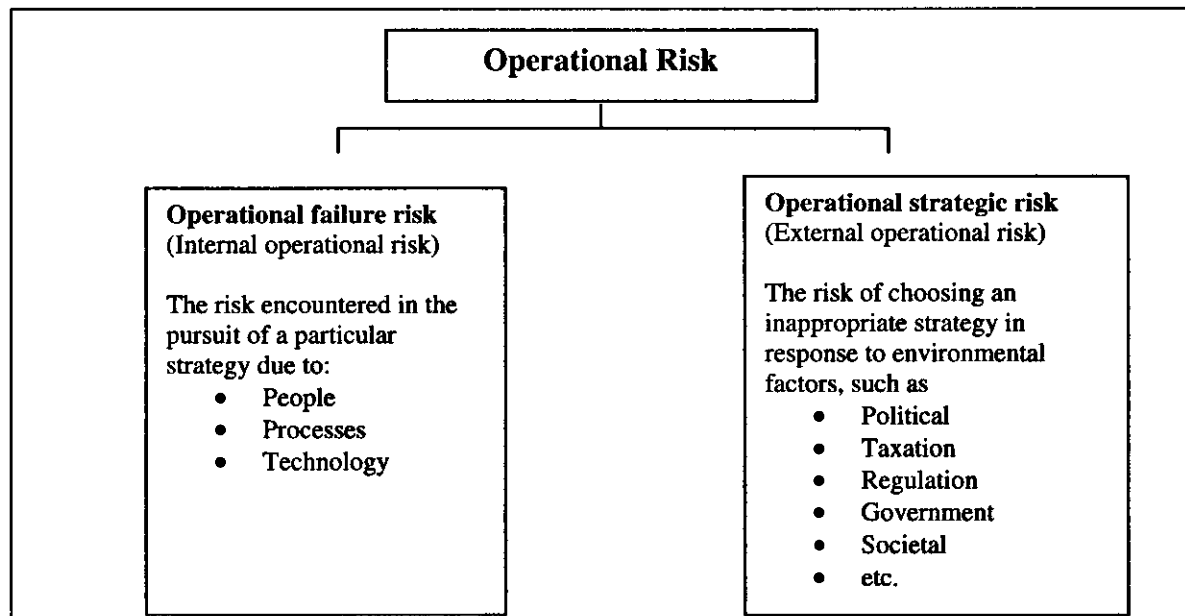
2.2.2.1 Operational failure risk (Internal operational risk)

Operational failure risks arise from the potential for failure in the courses of operating the business. Crouhy *et al* (1998: 479) clarifies that an institution uses people, processes, and technology to achieve business plans, and any one of these factors may experience a failure of some kind. Accordingly, operational failure risk can be defined as the risk that there will be a failure of people, processes or technology within the business unit, in other words, an internal operational risk (Crouhy *et al*, 1998: 479). A proportion of the failures may be anticipated, and these risks should be built into the business plan (Olsson, 2002: 275). But if it is unanticipated, it is therefore uncertain failures that give rise to operational risks. These failures can be expected to occur periodically, although both their impact and their frequency may be uncertain (Olsson, 2002: 276).

2.2.2.2 Operational strategic risk (External operational risk)

Operational strategic risk arises from environmental factors, such as a new competitor that changes the business paradigm, a major political and regulatory regime change, or earthquakes and other such factors that are outside the control of the institution (Crouhy *et al*, 1998: 479). It also arises from major new strategic initiatives, such as developing a new line of business or re-engineering an existing business (King, 2000: 35). Crouhy *et al* (1998: 480) also declared that all businesses rely on people, processes, and technology outside their business unit, and the potential for failure exists there too, therefore this type of risk can also be referred to as an external dependency risk. Figure 2.1 summarizes the relationship between operational failure risk and operational strategic risk. As mentioned, these two principal categories of risk are also sometimes defined (slightly differently) as internal and external operational risk (Crouhy *et al*, 1998: 479).

Figure 2.1 Two broad categories of operational risk



Source: (Crouhy *et al*, 1998: 480)

This study does not just focus on external or internal operational risk alone, but focus on both internal and external operational risks. It is important to see that a failure to address

an operational strategic risk (external) issue can easily translate into an operational failure (internal) risk (Olsson, 2002: 35). For example, a change in the tax laws is an operational strategic risk and the failure to comply with the tax laws is an operational failure risk (Olsson, 2002: 36). Furthermore, Olsson (2002: 36) stated that from a business unit perspective it might be argued that the external dependencies include support groups within the bank, such as information technology. In other words, the two types of risks are interrelated and tend to overlap.

The formulated definition of operational risk that is then going to be used in this study is the one that was already mentioned in section 2.2.1. Operational risk can be defined as: *“the risk of an external or internal loss resulting from a range of possible events, which include a human or employee error, a disruption in the work environment, a breakdown of processes, a malfunction in the information system and or a computer system failure due to ineffective technology”*.

The above concluded the defining of operational risk and now that operational risk is defined for a financial institution and the different levels and categories are also examined, the study can proceed to evaluate the Basel Committee and its proposals for operational risk and operational risk management.

2.3 The Basel Committee

Over the past three decades the Basel Committee has formulated and promoted sound supervisory standards for active internationally banks worldwide. The Basel Committee's history started in 1974 with its most influential document, The Basel Capital Accord published in 1988 (BIS, 2001g: 1). The Basel Committee does not possess any formal supranational supervisory authority, and its conclusions were never intended to have legal force. It formulates broad supervisory standards and guidelines in the expectation that individual authorities will implement them through detailed arrangements best suited to their own national systems (BIS, 2001g: 2).

2.3.1 Background to the Basel Committee

The Basel Committee was formed in 1974 by the governors of central banks of the Group of Ten (G-10) countries. Instability, for example the fall of the Bretton Woods System, characterized world markets in the 1970's. The insolvency of one of the most well known banks of Germany, Bankhaus Herstatt compelled the Group of Ten Countries to take action (Styger, 1998a).

Today the Basel Committee consists of supervisory representatives from Belgium, Canada, France, Germany, Italy, Japan, Luxemburg, the Netherlands, Spain, Switzerland, United Kingdom and the United States (BIS, 2001g: 1). Countries are represented by their central bank and also the authority with formal responsibilities for the prudential supervision of banking businesses where this is not the central bank (BIS, 2001g: 2). The Basel Committee usually meets at the Bank for International Settlements (BIS) in Basel, where its permanent Secretariat is located. It has about thirty technical working groups and tasks forces that also meet regularly. The present chairman of the Basel Committee is Mr. William J. McDonough, President and CEO of the Federal Reserve Bank of New York (Raghavan, 2001: 2).

The Basel Committee has several goals with banking supervision, which include the following (Styger 1998a):

- Improving the safety of the international banking industry through capital adequacy requirements.
- Levelling the international playing fields between banks.
- Narrowing the gap in international banking supervision.

Since its foundation, the Basel Committee has been the main driving force behind bank regulations. The three principle proposals/objectives of the Basel Committee mentioned above are intended to make banks safer from the perspective of the client and of the investor. The Basel Committee therefore focuses mainly on capital adequacy for banks

(Styger, 1998a). Although the Basel Accord framework is intended to apply to internationally active banks supervised by the Group of Ten Countries (G-10), other countries have adopted it as compliance, giving banks a 'seal of approval' in terms of capital adequacy, which makes it easier for them to compete. It has been applied, not only to internationally active banks, but also to eliminate inequalities between internationally active banks and their competitors in domestic markets (Matten, 2000: 97).

2.3.2 Publications of the Basel Committee

The Basel Committee has published several documents on banking supervision and the following section will highlight some of the key documents. The first was published in 1975 and after several revisions it was republished in 1983 as "*Principles for the Supervision of Banks' Foreign Establishments*" (Styger, 1998a). This was one of the three documents that especially changed the banking environment forever (Styger, 1998a). The second influential document – "*Capital Accord – Internationally Convergence of capital measurement and capital standards*" – was the prescription for minimum capital requirements published in July 1988, with the aim of being converted into national regulations "as soon as possible" (Styger, 1998a). In 1995 the Basel Committee started to address market risk and in January 1996 the third influential document was published, via "*Amendments to the capital accord to incorporate market risk*" (Styger, 1998a).

The Capital Accord of 1988, mentioned above, was aimed to ensure an adequate level of capital in the international banking system and to create a "more level playing field" in competitive terms between banks internationally (see 2.3.1). The Capital Accord requires banks to hold capital to at least eight percent of a basket of assets weighted according to their risks (BIS, 2001a: 9). Assets were classified into four buckets (0 per cent, 20 per cent, 50 per cent and 100 per cent) according to the perceived risk of the debtor category (BIS, 2001a: 10). Off-balance sheet items are converted into a credit-equivalent amount

through a scale of conversion factors, and are then weighted according to the counterpart's risk weighting (Barbour et al, 1991: 291).

The 1988 Capital Accord also did not recognize credit risk mitigation techniques and the simple bucket system has given banks the incentive to move high quality assets off their balance sheets, thereby reducing the average quality of the banks' asset portfolio (Saayman, 2002: 126). Because of this, the Basel Committee decided to propose a more risk sensitive framework for capital adequacy measurement (BIS, 2001a: 11-12). The new proposal (as documented in the Consultative Document of the Basel Committee in January 2001) with regard to risk management (see BIS, 2001c) and the concerns about the implications of the proposal are subsequently discussed.

2.4 The New Basel Capital Accord

In addition to the 1988 Capital Accord, the Basel Committee has issued a paper on the regulatory capital requirements for credit and operational risks in banks, which is called the New Basel Capital Accord (Saayman, 2002: 127). The Basel Committee has also released a second consultative package on the New Basel Capital Accord – the Revised Accord¹, which will be implemented in 2006 (BIS, 2001a: 12). It is notable that the New Basel Capital Accord is more extensive and complex than the 1998 Capital Accord and is intended to develop a risk-sensitive framework that contains a wider range of new options of measuring both credit and operational risk.

Also in addition to the 1988 Capital Accord, the proposals of the New Basel Capital Accord contained three fundamental innovations, each designed to introduce greater risk sensitivity into the New Basel Capital Accord. One was to introduce a three-pillar approach, with a risk-sensitive framework being reinforced by supervisory review and enhanced disclosure (Barcklays, 2001: 2).

¹ The Revised Accord will be evaluated in detail in a latter section of this chapter.

The second and third innovations both aim at making capital charges more correlated with banks' risk profiles (Barcklays, 2001: 2-3). Banks with advanced risk management capabilities would be permitted to use their own internal systems for evaluating credit risk, known as "internal ratings²", instead of standardized risk-weights for each class of asset. The third principle innovation was to allow banks to use the risk grades provided by approved external credit assessments institutions to classify their exposures into risk buckets (Barcklays, 2001: 2-3).

Another improvement to the 1988 Capital Accord is that the New Basel Capital Accord recognizes that the best way to measure, manage and mitigate risk differs from bank to bank, whereas the 1988 Capital Accord provided essentially only one option for measuring capital adequacy (BIS, 2001a: 3). Consequently, the New Basel Capital Accord provides for a spectrum of approaches for the measurement of credit risk in determining capital levels and the flexible structure allows banks to adopt approaches, which best fit, their levels of sophistication and their risk profiles, subject to supervisory approval.

As mentioned, one of the proposals of the New Basel Capital Accord is to implement a three-pillar framework, which include the following (Bessis, 2001: 40-41):

- Pillar 1: Minimum capital requirements, which seek to refine the standardized rules, set forth in 1988.
- Pillar 2: Supervisory review of an institutions' internal assessment process and capital adequacy.
- Pillar 3: An effective use of disclosure to strengthen market discipline as a compliment to supervisory efforts.

Bessis (2001: 42) also highlighted the fact that the New Basel Capital Accord cannot be considered fully implemented if all three above-mentioned pillars are not in place.

² Internal ratings are assessments of relative credit risks of borrowers and/or facilities, assigned by banks (Bessis, 2001: 42).

Minimum implementation of one or two of the pillars will not deliver an adequate level of soundness. The Basel Committee recognizes that in certain jurisdictions it is not at present possible to implement all three pillars fully. In such a case, the Basel Committee recommends that supervisors consider more intensive use of the other implemented pillars (BIS, 2001a: 3). For example, supervisors could use the supervisory review process to encourage improvement in transparency, disclosure and consequently market discipline. The Basel Committee considers the implementation of Pillar 1 as a minimum requirement for the implementation of the New Basel Capital Accord (BIS, 2001a: 3).

2.4.1 Objectives of the New Basel Capital Accord

With the implementation of the New Basel Capital Accord, the Basel Committee is aiming to achieve the following objectives (BIS, 2001a: 6):

- The Accord should continue to promote safety and soundness in the financial system and, as such, the new framework should at least maintain the current overall level of capital in the system.
- The Accord should continue to enhance competitive quality.
- The Accord should constitute a more comprehensive approach to addressing risks.
- The Accord should contain approaches to capital adequacy that is appropriately sensitive to the degree of risks involved in a bank's positions and activities.
- The Accord should focus on internationally active banks, although its underlining principles should be a suitable application for banks of varying levels of complexity and sophistication.

The main innovations of the New Basel Capital Accord compared with the 1988 Capital Accord are as follows. Firstly, it aims to bring the methodology of calculating capital requirements more closely into line with the advances in risk management technology that have occurred since 1988 (De Beer, 2002: 217). The new capital framework aims to go further than simply bringing a number of innovative financial instruments within the scope of the New Basel Capital Accord (BIS, 2001a: 6). De Beer (2002: 217) also stated

that the new capital framework also aims to be forward looking by making capital standards less distortionary *ex ante*. The overall objective is to limit the incentives that capital standards create for banks to arbitrage its requirements by more closely aligning regulatory capital charges with the concept of loss risks (Karacadag & Taylor, 2000: 13-14).

Secondly, the new framework aims to move capital regulation in a more process-orientated direction (De Beer, 2002: 217). Whereas the 1998 Capital Accord laid down a series of simple rules in order to develop a common metric for setting capital requirements, the new capital framework envisages an approach in which supervisors will become less involved in determining the precise rules of calculating capital adequacy (BIS, 2001a: 6). Instead, supervisors will concentrate on ensuring that a bank's internal risk management procedures are adequate. This can be seen as a relative shift away from the mechanistic, prescribed approach to setting bank capital (rules-driven) towards a more process-orientated form of regulation.

The change from a rules-driven to process-orientated is a matter of degree, not of kind: it is not all-or-nothing. Thus, as De Beer (2002: 217) stated, the new capital framework retains elements of regulatory and rules-based capital regulation, just as the new capital framework incorporated elements of economic and process-orientated approaches. This shift in emphasis from a rules- to process-orientated involves foregoing the verifiability and comparability of capital ratios across banks and banking systems to the extent that it involves greater reliance on internal risk measurement and control systems. As Saayman (2002: 176) mentioned, this will have an important consequence. Capital ratios will become more difficult to interpret in isolation and the terms "under-capitalized" and "well-capitalized" will be difficult to designate without an in-depth analysis, taking into account whether or not the level of capital adequately reflects the risk embedded in the asset portfolio.

The need for a more in-depth analysis of banks under the new capital framework raises two additional issues, especially with respect to the third pillar (see section 2.4). Firstly,

internal processes of capital allocation are inherently less transparent than current capital ratios. Unless essential elements of internal risk management and capital allocation mechanisms are disclosed, market participants may not have the information required to evaluate capital adequacy (though supervisors presumably would have greater access) (De Beer, 2002: 219). This would undermine the market's ability to exert discipline, and along with it, the effectiveness of the third pillar (also see section 2.4). Secondly, even if sufficient information was available, market participants would have to devote much more resources to analyse banks, which they may not elect to undertake given the "free-rider" problem in the market for risk analysis (Saayman, 2002: 167).

The above then concluded the evaluation of the objectives of the New Basel Capital Accord and it is important to have an understanding of the objectives of the new framework to be able to understand what the Basel Committee is trying to achieve with the new framework. The following section of chapter 2 will now discuss the overall level of capital of the New Basel Capital Accord, which is one of the most debated aspects of the New Basel Capital Accord.

2.4.2 Overall capital

Regarding the overall level of regulatory capital resulting from its proposals, the Basel Committee believes that it is important to be as clear as possible about its ultimate intentions with the New Basel Capital Accord (Bessis, 2001: 40). The new framework intends to maintain the overall level of regulatory capital in the banking system while providing approaches, which are more sensitive to risk than the approaches of the 1988 Capital Accord. Consistent with the objectives of the New Basel Capital Accord, the Basel Committee envisages the following (UBS, 2001: 1):

- Under the standardized approach (see section 2.4.4.2), the Basel Committee maintains the 8% minimum capital requirement and states that they "desire neither to produce a net increase or a net decrease on average in minimum regulatory capital".

- With respect to the Internal Ratings-Based Approach (IRB), the Basel Committee's ultimate goals are to ensure that the overall level of regulatory capital generated is sufficient to address the underlying credit risk and is such that it provides capital incentives relative to the standardized approach.
- Consequently, for foundation IRB institutions, the Basel Committee is aiming for a small (2-3%) average decline in minimum capital requirements compared to current capital requirements and the proposed standardized approach.
- For institutions on the advanced IRB approach a further fall of similar average magnitude is being targeted.

The Basel Committee recognizes the difficulty in assessing the average impact of its above-mentioned proposals across a diverse range of internationally active banks (BIS, 2001a: 16). In addition to the 1988 Capital Accord, the new Basel Capital Accord consists out of three pillars, which include minimum regulatory capital, supervisors review and thirdly, market discipline. The following section will then continue the evaluation of the New Basel Capital Accord, in terms of the three pillars of the new framework.

2.4.3 The three pillars of the New Basel Capital Accord

As mentioned the New Basel Capital Accord is a set of consultative documents that describes recommended rules for enhancing credit risk measures, extending the scope of capital requirements to operational risk, providing various enhancements to the 1988 Capital Accord and detailing the 'supervision' and 'market discipline' pillars (Bessis, 2001: 41). The New Basel Capital Accord is very extensive, which provides a menu of options, extended coverage and more elaborate measures, in addition to descriptions of work in progress, with yet unsettled issues to be streamlined in the final package.

The New Basel Capital Accord comprises three pillars, which were already mentioned in the earlier sections of this chapter and include the following:

- Pillar 1: Minimum capital requirements.
- Pillar 2: Supervisory review process.
- Pillar 3: Market discipline.

Table 2.1 describes the rationale for the New Basel Capital Accord.

Table 2.1 Rationale for a new accord: the need for more flexibility and risk sensitivity.

| Existing Accord | Proposed New Accord |
|---|--|
| <p>Focusing on a single risk measure</p> <p>One size fits all: only one option proposed to banks.</p> <p>Broad brush structure (forfeits)</p> | <p>More emphasis on banks' own internal methodologies, supervisory review and market discipline.</p> <p>Flexibility, menu of approaches, incentives: banks have several options.</p> <p>More credit risk sensitivity for better risk management.</p> |

Source: (Bessis, 2001: 41)

The Basel Committee emphasizes the mutually reinforcing role of the three pillars, and avowed that taken together, the three pillars contribute to a higher level of safety and soundness in the financial system (Bessis, 2001: 41). Previous implementations of the regulations for credit and market risk, confirmed by value at risk (VaR)³ models for both risks, revealed that the banking book generates more risks than the trading book and necessitates a more in-deep look at the above-mentioned pillars (BIS, 2003: 128). The following section of this chapter therefore aims to evaluate the above-mentioned pillars as part of the evaluation of the New Basel Capital Accord.

2.4.3.1 Pillar 1: Minimum capital requirement

The Basel Committee's proposals for minimum capital requirements are based on fundamental elements of the 1988 Capital Accord: a common definition of regulatory capital that remains unchanged and minimum ratios of capital to risk-weighted assets (BIS, 2000d: 2). It is the measurement of risk embodied in the risk-weighted assets that the New Basel Capital Accord addresses. Under the New Basel Capital Accord, the denominator of the minimum total capital ratio will consist of the following three parts (Bessis, 2001: 42):

- The sum of risk-weighted assets for credit risk.
- Plus 12.5 times the capital charge for market risk.
- Plus 12.5 times the capital charge for operational risk.

The following example will explain the above-mentioned. Assuming that a bank has \$875 of risk-weighted assets, market risk capital charge of \$10 plus an operational risk charge of \$20, the denominator of the total capital ratio would equal $875 + [(10 + 20) \times 12.5]$ or \$1,259. When multiplying by 12.5, the bank creates a numerical link between the calculation of the capital requirement for credit risk, where the capital charge is based on risk-weighted assets, and the capital requirements for operational and market risk (Koch & McDonald, 2000: 376).

Pillar 1 covers regulatory capital requirements for both credit and operational risk. To improve risk-sensitivity, the Basel Committee is proposing a range of options for addressing both credit and operational risks. The primary changes to the minimum capital requirements set out in the 1988 Capital Accord are firstly the approaches to credit risk and secondly the inclusion of explicit capital requirements for operational risk (Bessis, 2001: 42), and thirdly the decision of the Basel Committee to treat interest rate risk under pillar 2 (Banking Council, 2001: 14).

³ VaR is the focus on valuing a risk as a capital charge (Bessis, 2001: 12).

With regard to other risks, the Basel Committee has decided to narrow its focus on pillar 1 to the treatment of operational risk. In line with its approach to credit and market risk, the Basel Committee (BIS, 2003a: 126) offer several approaches to the minimum capital requirements for operational risks that will be discussed in section 2.4.3.

2.4.3.2 Pillar 2: Supervisory review

The Basel Committee view supervisory review as a critical component to the minimum capital requirements (pillar 1) and market discipline (pillar 3). The second pillar of the New Basel Capital Accord is intended to ensure that each bank has sound internal processes in place, to assess the adequacy of its capital based on a thorough evaluation of its risks (Barckleys, 2001: 4-5). Supervisors will be responsible for evaluating on how well banks are addressing their capital adequacy needs relative to their risks. In doing so, supervisors will draw on, among other considerations, their knowledge of best practices across institutions (Barckleys, 2001: 5).

The Basel Committee sees four areas where supervisory review is a necessarily complement to pillar 1 minimum capital requirements and the disclosure requirement of pillar 3 (Karacadag & Taylor, 2000: 27):

- Dealing with risk only partially addressed in pillar 1, where the review of individual institutions reveals issues that are not adequately covered by the general requirement.
- Capturing risks that have been left out of pillar 1 (e.g. interest rate risk in the banking book and strategic and reputational risks facing the institution).
- Assessing factors external to the institution (e.g. effects of the business cycle).
- Ensuring compliance with the various operational and disclosure standards associated with the use of advanced approaches for credit and operational risk or the use of particular credit risk mitigation techniques.

In addition to the above-mentioned, supervisors will have already reviewed and evaluated the bank's capital adequacy through on-site examinations, off-site surveillance, and reviewed the work of external and internal auditors (Karacadag & Taylor, 2000: 28). Under the new approach, supervisors will also review the internal capital adequacy assessments of a bank and discuss the internal capital targets set by each bank (Hoffman, 2002: 4). The goal of supervisors reviewing the bank's capital position is to ensure that the position is consistent with its overall risk profile and strategy (Hoffman, 2002: 4). Furthermore, supervisory review is assigned the task of ensuring that banks are operating above the minimum regulatory capital ratios and to enable early supervisory intervention if the capital does not provide a sufficient buffer against risk (Karacadag & Taylor, 2000: 28).

This proposal by the Basel Committee is not a way intended to replace the judgment and expertise of a bank's management, or to shift the responsibility of maintaining capital adequacy to supervisors (Karacadag & Taylor, 2000: 30). On the contrary, it is well understood that managers have the complete understanding of the risk their institutions face and it is they who have the ultimate responsibility of managing those risks. Furthermore, capital should not be regarded as a substitute for addressing fundamentally inadequate control or risk management processes (Bessis, 2001: 48). The Basel Committee also formulated four basic principles that should inspire supervisor's policies (Bessis, 2001: 49):

- Principle 1: Banks should have a process for assessing their overall capital in relation to their risk profile and strategy for maintaining their capital levels.
- Principle 2: Supervisors should review and evaluate banks' internal capital adequacy and assessment strategies, as well as their ability to monitor and ensure their compliance with regulatory capital ratios. Supervisors should take appropriate supervisory action if they are not satisfied with the results of the process.

- Principle 3: Supervisors should expect banks to operate above the minimum regulatory capital ratios and should have the ability to require banks to hold capital in excess of the minimum.
- Principle 4: Supervisors should seek to intervene at an early stage to prevent capital from falling below the minimum required to support the risk characteristics of a particular bank and should require rapid remedial actions if capital is not maintained or restored.

The implementation process can reveal some concerns regarding pillar 2. The detailed requirements of pillar 2 can be perceived as an indication that the supervisory review will be intrusive (Hoffman, 2002: 13). Furthermore, Principle 3 suggests that regulators will, as a matter course, require banks to hold capital above the regulatory minimum even where there is no well-defined weakness or lack of management and control.

In addition to the above-mentioned, the UBS (2001: 26) questioned that in the light of the considerable capital safety margin incorporated in pillar 1, the suggestion that banks with sound internal risk management and control practices and standards should be required to hold more than the regulatory minimum capital calculated under pillar 1. It is the believe of the Basel Committee that the above-mentioned will be fully addressed, with the implementation of the new framework in 2006.

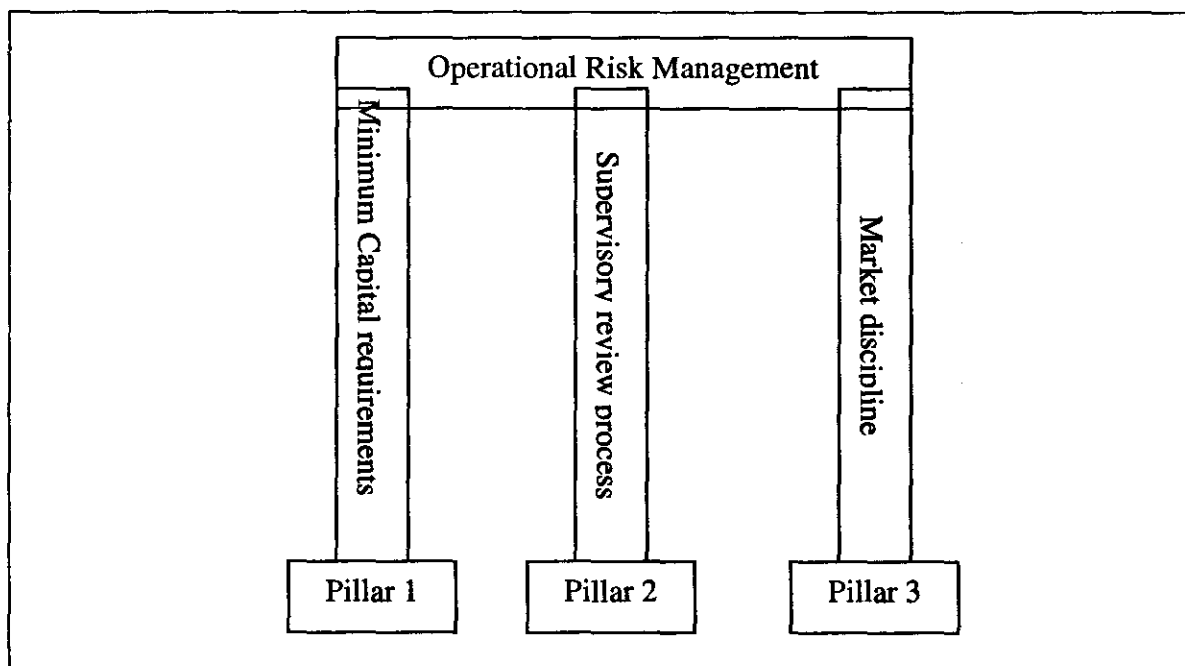
2.4.3.3 Pillar 3: Market discipline

The third major element of the Basel Committee's approach to capital adequacy is market discipline. Market discipline can play an equally important role in capital standards by serving the purpose of reviewing the reviewers. Supervisors not only face a technically more challenging task, but in the exercise of discretion and judgment over subjective and qualitative matters, they are likely to come under political pressure from banks and other interested parties (Hoffman, 2002: 13). Market discipline could act to counter such forces and provide supervisors with incentives to conduct their responsibilities rigorously and even-handedly (BIS, 2001a: 40).

Empirical studies indicate that neither the market nor supervisors possess clearly superior quality assessments. This is recognized by the Basel proposals, with market discipline and supervisory review as part of an integrated three-pillar approach. The supervisor's, advantage over outside investors is that they can require access to all data, including confidential information that the bank would prefer not to make public. At the same time, supervisors are more constraint by law, regulation, and data availability to keep their formal analytical methods constraint for relatively long periods of time (Bliss & Flannery, 2001: 8).

Figure 2.2 is an illustration of the three pillars of the New Basel Capital Accord:

Figure 2.2 The three pillars of the New Basel Capital Accord



Source: (Compiled by the author)

The strength of market quality assessments is that investors can investigate any information that seems relevant, and they can freely change their analytical methods when circumstances seem to warrant it (Bliss & Flannery, 2001: 8). In addition to the above-mentioned, the Basel Committee expects supervisors to take a supervisory

response aimed at remedying a situation where a bank does not comply with the disclosure recommendations under pillar 3 (BIS, 2001c: 2). The strength of this response should depend on the nature, implications and duration of non-compliance (BIS, 2001c: 2).

As already mentioned, the success of the New Basel Capital Accord depends on the implementation of all three pillars, as well as the coordination between them. As also mentioned in previous sections of this chapter, the New Basel Capital Accord cannot be considered fully implemented if all three pillars are not fully implemented. The following sections will provide the different methods/approaches available to banks for the assessment of their overall operational risk capital charge under the new framework.

2.4.4 Approaches

The proposed risk capital framework under the New Basel Capital Accord provides certain methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity. The methods include the following (BIS, 2003a: 121):

- The Basic Indicator Approach.
- The Standardized Approach.
- Internal Measurement Approach (IMA).
- Advanced Measurement Approach (AMA).

The Basic Indicator Approach is the less complex of the four where AMA is the most complex. A bank will not be allowed to choose to revert to a simpler approach once it has been approved for a more advanced approach without supervisory approval (BIS, 2003a: 120). In addition, if a supervisor determines that a bank using a more advanced approach no longer meets the qualifying criteria for the specific approach, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by the supervisor for returning to a more advanced approach (BIS,

2003a: 120). The following sections will evaluate the above-mentioned approaches in more detail.

2.4.4.1 The Basic Indicator Approach

This is the most basic approach as it links the capital charge to a single indicator, for example gross income. This indicator will serve as a proxy for overall operational risk exposure. Each bank will hold capital for operational risk equal to a fixed percentage (α) of the indicator (BIS, 2001b: 6).

The capital charge for the Basic Indicator Approach may then be expressed as follows (BIS, 2003a: 121):

$$K_{BIA} = GI \times \alpha$$

Where: K_{BIA} = the capital charge against the Basic Indicator Approach

GI = average annual gross income over the previous three years

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

There are no specific criteria for the use of the Basic Indicator Approach, which is set in the New Basel Capital Accord, but banks that are using this approach are encouraged to comply with the Basel Committee's guidance for the management of operational risk.

2.4.4.2 The Standardized Approach

Bank activities are divided into standardized industry business lines, each with its own indicator of operational risk and own fixed percentage (β) (BIS, 2003a: 121). The business lines can include the following (BIS, 2003a: 122):

- Corporate finance.
- Trading & sales.
- Retail banking.
- Commercial Banking.
- Payment and Settlement.
- Asset Management.

The capital charge for each business line is calculated by multiplying gross income by the factor β , which is assigned to each business line. Beta (β) serves as proxy for industry wide relationships between the operational risk loss experience for a given business line and the aggregate level of gross income for that business line (BIS, 2003a: 122). However, the determination of the beta factor for each of the business line is problematic. It should be calculated according to loss experience and the calculation should be done by using a clear and objective methodology (BIS, 2001b: 7). In practice, this is not yet achievable in South Africa.

The current available databases of operational losses tend to be biased to, for example, larger losses and to data that is publicly available. Internal loss data collection is also still in the developing phase for most banks. This necessitates subjective analysis of the risk and the possible losses (BIS, 2003: 123).

The Basel Committee has estimated preliminary beta factors based on data from a sample of internationally active banks (BIS, 2001b: 6). The levels of these factors vary widely, reflecting the different weightings of the business lines, the choice of different indicators and the size of the sample (BIS, 2001a: 6). Mathematically the beta factor of each business line is the product of 20% of current minimum capital requirement (MRC) from the bank sample and the business line weighting, divided by the summation of the financial indicators for the business line (BIS, 2001b: 21):

$$\beta = \frac{[20\% \text{ current total MRC } (\$)] \times [\text{business line weighting } (\%)]}{\sum \text{ Financial indicators for the business line from bank sample } (\$)}$$

The capital charge for the standardized Approach may then be expressed as follows (BIS, 2003a: 122):

$$K_{TSA} = \sum (GI_{1-8} \times \beta_{1-8})$$

Where:

K_{TSA} = the capital charge under the standardized approach

GI_{1-8} = the average level of gross income over the past three years for each business line.

β_{1-8} = a fixed percentage set by the Basel Committee.

The results of the Basel Committee's initial assessment also suggest that there will be a very wide dispersion of operational capital charges for individual banks above and below the assumed industry average of 20% of current minimum regulatory capital (BIS, 2003a: 124). The preliminary findings indicated that some banks would be required to hold more than twice the assumed industry average, while other banks face a charge well below the average.

For international active banks to use the Standardized Approach they must meet the following criteria (BIS, 2003a: 124):

- The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function.
- The bank must track relevant operational risk data including material losses by business lines as part of its internal operational risk assessment system.
- Operational risk exposures, including material operational losses, must be reported regular to the board of directors and senior management.
- The bank's operational risk management system must be well documented.
- The bank's operational risk management processes and assessment system must be subjected to validation and regular independent review.

Table 2.2 is an illustration of some examples of the above-mentioned beta factors that are used for the standardized approach in different business lines.

Table 2.2 Beta factors for business lines

| Business lines | Beta factors |
|--------------------------------------|---------------------|
| Corporate Finance (β_1) | 18% |
| Trading and Sales (β_2) | 18% |
| Retail Banking (β_3) | 12% |
| Commercial Banking (β_4) | 15% |
| Payment and settlement (β_5) | 18% |
| Agency services (β_6) | 15% |
| Asset management (β_7) | 12% |
| Retail Brokerage (β_8) | 12% |

Source: (BIS, 2003a: 123)

2.4.4.3 The Internal Measurement Approach (IMA)

Banks meeting certain strict supervisory standards will be allowed to use internal loss data to calculate the required capital. Currently there is not sufficient data available at the industry level or in a sufficient range of individual institutions to calibrate the capital charge under this approach (De Beer, 2002: 236). Banks would have to collect the necessary data over the years to come to be able to implement this approach before a satisfactory database has been established by the industry and by the individual banks.

Under this approach a capital charge for operational risk of a bank would be determined according to the following steps (BIS, 2001b: 8-9):

- As with the standardized approach, the banks' activities will be divided into business lines. For each business line possible operational loss types will be identified.
- For each business line/loss type combination, the supervisor will specify an exposure indicator (EI), which is a proxy for the amount of risk of each business line's operational risk exposure.
- Next, a parameter representing the probability of the loss event (PE), as well as a parameter representing the loss given for that event (LGE), must be determined. The product of EI, PE and LGE equals the expected loss (EL) for each business line/loss type combination.
- The supervisor supplies a fixed percentage (the gamma factor) for each business line/loss type combination, which translates the expected loss (EL) into a capital charge. The overall capital charge for the bank is the sum of all the resulting products.
- To facilitate the process of supervisory validation; banks will have to supply their supervisors with the individual components of the expected loss calculation and not just the product EL.

There is also a gamma factor (γ), which represents a constant that is used to transform expected loss (EL) into a risk or a capital charge (BIS, 2001b: 9). This is defined as the maximum amount of loss per holding period within a certain confidence interval (BIS, 2001b: 9). The scale of gamma will be determined and fixed by supervisors for each business line/loss type and its determination will further be based on an industry wide loss distribution (BIS, 2001b: 10). However, the risk profile of each bank is not necessarily equivalent to the industry wide loss distribution. The Basel Committee is investigating the use of a Risk Profile Index as a possible way to address this problem.

The Internal Measurement Approach (IMA) will require banks to have a sound internal loss reporting practice, as well as an operational loss data base, extending back for a number of years for significant business lines (De Beer, 2002: 237). The internal loss data will have to be supplemented by relevant external loss data. Sources of external data

will have to be reviewed regularly to ensure the accuracy and the applicability thereof. Knowledgeable staff, a sound measurement methodology and an appropriate systems infrastructure will be indispensable to meet these, and all other requirements (De Beer, 2002: 237-238).

The accuracy of loss data will also have to be established through “use tests” (BIS, 2001b: 10). This means that the bank must use the collected data and the resulting risk analysis, risk reporting, and so on. Banks that do not fully integrate an internal measurement methodology into daily activities and business decisions should not qualify for this approach (De Beer, 2002: 237). De Beer (2002: 238) also affirmed that banks would have to validate whether the operational environment is accurately reflected in the collected data and estimations and should incorporate experience and judgment into analysis.

The conditions, under which judgments or ‘over-rides’ may be used, will have to be specified, clearly documented and be subject to independent review. Supervisors will also examine the data collection, measurement, and validation process and assess the appropriateness of the operational risk control environment of the bank.

2.4.4.4 Advanced Measurement Approach (AMA)

The Advanced Measurement Approach is the fourth and most complex of the four approaches and is regarded as more advanced than the Internal Measurement Approach. The regulatory capital under this approach will equal the measure generated by the bank’s internal operational risk measure system using the quantitative as well as the qualitative criteria for AMA (see sections 2.4.4.2 & 2.4.4.3). Banks, which adopted the AMA, will be required to calculate their capital requirement using this approach as well as the existing Basel Capital Accord for a year prior to implementation of the New Basel Capital Accord at the end of 2006 (BIS, 2003a: 124).

There are also different qualifying criteria for banks to meet in order for them to be able to use the AMA and these criteria includes the following:

2.4.4.4.1 General criteria

In order for banks to use the AMA they must satisfy the supervisor on at least two of the following (BIS, 2003a: 124):

- The board of directors and the management of the bank must be actively involved in the oversight of the operational risk management framework.
- The bank must have a risk management system that is conceptually sound and is implemented with integrity.
- The bank must have sufficient resources in the main business lines as well as in the control and audit areas.

Before the AMA can be used for regulatory purposes, supervisors must monitor it, which will allow them to determine if the approach is credible and appropriate. It is also important that a bank's measurement system must be capable of supporting an allocation of economic capital for operational risk across the business lines in a manner that creates incentives to improve business line operational risk management (BIS, 2003a: 125). As mentioned earlier, for the use of the AMA banks are also subjected to some qualitative and quantitative standards, and both of these will be discussed in the following sections.

2.4.4.4.2 Qualitative standards

A bank must meet the following qualitative standards before it is permitted to use the AMA (BIS, 2003a: 125):

- There must be an independent operational risk management function within the bank that is responsible for the design and implementation of the bank's operational risk management framework.

- The bank's internal operational risk management system must be closely integrated into the day-to-day risk management processes of the bank.
- Operational risk exposure as well as loss experience must be reported to senior management and the board of directors.
- The bank's risk management system must be well documented.
- Regular review must be done by internal or external auditors.

2.4.4.4.3 Qualitative standards

The BIS (2003a: 126) stated the following qualitative standards for the use of the AMA:

- **The AMA soundness standard:** It is important that a bank must be able to demonstrate that its approach captures potentially severe "tail loss" events⁵. Whatever approach is used, a bank must demonstrate that its operational risk measurement meets a soundness standard comparable to that of the Internal Ratings Based Approach for credit risk (i.e. comparable to one-year holding period and 99.9% confidence interval).
- **Detailed criteria:** Supervisors will require the bank to calculate its regulatory capital requirements as the sum of the expected loss (EL) (see 1.2) and unexpected loss (UL), unless the bank can demonstrate that it adequately captures EL in its internal business practices. A bank's risk management system must be granular to capture the major drivers of operational risk affecting the tail of the loss estimates.
- **Internal data:** The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk measurement system. Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience.

- **External data:** A bank's operational risk measurement system must use relevant external data, especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe losses.
- **Scenario analysis:** A bank must use a scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high severity events.

The intention of the above continuum of approaches is that improvements in operational risk management would eventually reflect in a lower capital charge. The Basel Committee also believes that with the introduction of the AMA bank will find it easier to calculate their capital charge for operational risk, but are still developing ways to lower the capital charge for operational risk. The following section, therefore wants to discuss the calibration of capital charges for operational risk.

2.4.5 Calibration of capital charges

The industry consistently criticized the setting of the operational risk component at approximately 15% of the total minimum regulatory capital charge (Hoffman, 2002: 9). The Austrian banking industry even goes as far as to accuse the Basel Committee of first setting the desired level of capital charges and then calibrating measurements to suit that figure (Hoffman, 2002: 10). It is understood by the commentators that this 15% figure is based on a survey undertaken by a limited number of banks on how much economic capital was internally allocated to "other risk". It is the belief of banks that the results were heavily influenced by the respondent banks' interpretation of what other risks include (BIS, 2001a: 34). Evidence from Australian banks seems to suggest that the definition of operational risk now being employed by the Basel Committee (see section 2.2) produces a capital requirement of less than 15%. However, if other risks such as reputational risk and strategic risk are included, the benchmark could be as high as 40% to 50% (De Beer, 2002: 239).

⁵ Chapter 4 will explain a tail loss event.

According to the British Banking Association (Hoffman 2002: 13), the 15% figure also appears to have been based on the assumptions that banks are average sized, and that banks are averagely distributed across the seven business lines relative to the calibration pool. Hoffman (2002; 13) also stated that for some specialist institutions an appropriate charge will be very different from that suggested – the further the bank is from the mean, the more unrealistic the calibration is likely to be.

The Swiss Bankers Association (Hoffman, 2002: 15) strongly doubts whether this calibration represents the importance of operational risk relatively to credit risk in a realistic way. Their point is that, if the Basel Committee's perspective is that the 15% calibration choice comes from modifications of capital requirements for credit risk, the calibration is very arbitrary. Though the industry supports the Basel Committee's stated intention not to increase the overall capital requirements, they are of opinion that calibration should result from concrete risk considerations, instead of reasoning with respect to the maintenance of the overall capital level. As the Credit Suisse Group mentioned that there is no empirical basis for assuming that operational risk accounts for 15% of the current minimum regulatory capital requirement (King, 2000: 110).

The above-mentioned then conclude the first part of chapter 2, which was a short summary of the Basel Committee's New Basel Capital Accord and especially the proposals for operational risk. The second part of chapter 2 will continue the evaluation of the New Basel Capital Accord but the evaluation will be done in terms of the Basel Committee's proposals/principles for the **management of operational risk**, and will also focus more on operational risk as a "subset" of other risks.

2.5 Proposed practices regarding operational risk management

The Basel Committee recognizes that operational risk is a substantial element of other risks, and is an area to which banks themselves are devoting considerable attention and resources. Operational risk lends itself more easily to quantification, and hence effective management, than the elements of other risks. Nevertheless, banks should seek to

manage all significant risks, and supervisors will review them as part of the supervisory Review under pillar 2 (see section 2.4.3.2) of the New Basel Capital Accord.

On its work on operational risk, the Basel Committee has also aimed to develop a greater understanding of the current industry trends and practices for the management of operational risk. These efforts involve numerous meetings with banking organizations, surveys of industry practices and an analysis of results. Based upon these sources of information, the Basel Committee believes that it has a good understanding of both the banking industry's current range of practices as well as the industry's efforts to develop methods for managing operational risk.

This section of chapter 2 will aim to outline the set of principles proposed by the Basel Committee, which provides a framework for the effective management and supervision of operational risk and also for the use of internationally active banks and supervisory authorities when evaluating operational risk management policies, procedures and practices. The guidance mentioned in this part of chapter 2 is intended to apply to internationally active banks (e.g., on the basis of size complexity or systematic importance) or to the smaller or less complex banks.

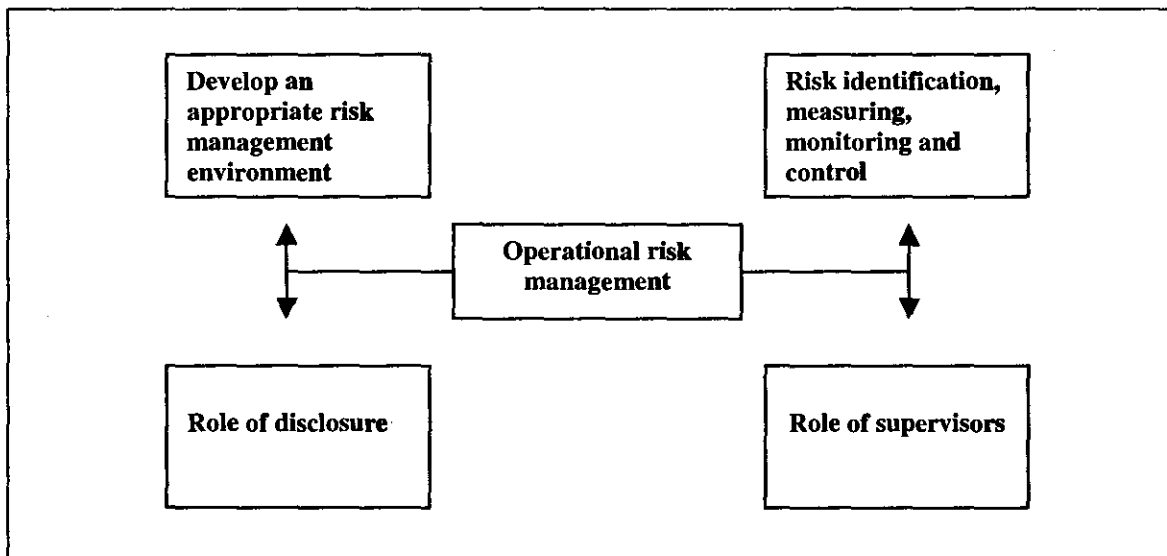
The evaluation of the Basel Committee, in terms of its proposals for operational risk management, will begin by a thorough evaluation of the four key elements of operational risk management followed by an evaluation of the Basel Committee's supervisory guidance in terms of management's structure and responsibilities.

2.5.1 The four key elements of operational risk management

The Basel Committee has identified four key elements in operational risk management, which includes the following (BIS, 2000g: 3):

- Development of an appropriate risk management environment.
- The identification, measuring, monitoring and controlling of the risk.
- The role of supervisors.
- The role of disclosure.

Figure 2.3 The four key elements of operational risk management



Source: (Compiled by the author)

2.5.1.1 Development of an appropriate risk management environment

The Basel Committee stated three basic principles that management must follow when developing an appropriate risk management environment, which include the following (BIS, 2000g: 4-6):

Principle 1: Senior management should be aware of the major aspects of the bank's operational risk as a distinct and controllable risk category and should approve and periodically review the bank's operational risk strategy. The strategy should reflect the bank's tolerance for the risk and its understanding of the specific characteristics of this risk category. Management should also be responsible for approving the basic structure

of the framework for managing operational risk and ensuring that the senior personnel are carrying out its risk management responsibilities.

Principle 2: Senior management should have the responsibility of implementing the operational risk strategy approved by the board of directors. The strategy should be implemented consistently throughout the whole banking organization, and all levels of personnel should understand their responsibilities with respect to operational risk management. Senior management should also have the responsibility for developing policies, processes and procedures for managing operational risk in all of the banks products, activities, processes and systems.

Principle 3: Information flows within the banking organization play a key role in establishing and maintaining an effective operational risk management framework. Communication flows within the bank should establish a consistent operational risk management culture across the bank. Reporting flows should enable senior management to monitor the effectiveness of the risk management system for operational risk, and also enable the board of directors to oversee senior management performance.

Cade (1997: 34) confirmed the above-mentioned by stating that the risk incurred by the bank should determine the formality and sophistication of the operational risk management environment. If a bank fails to address operational risk, which is virtually present in all bank activities, it may greatly increase the likelihood that some risk may go unrecognised and uncontrolled. Management must also translate the operational risk strategy established by the board of directors into policies, processes and procedures that can be implemented and verified (Cade, 1997: 35). While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management must clearly assign authority, responsibility and reporting relationships to encourage this responsibility. The above-mentioned responsibility includes ensuring that the necessary resources are available to manage operational risk (Cade, 1997: 35).

Moreover, senior management should assess the appropriateness of the management oversight in the light of risk inherent in a business line strategy and ensure that staff is apprised of their responsibilities. The key element in developing an appropriate risk management environment is to ensure that personnel exactly know what are required from them (King, 2000: 55). If an appropriate operational risk management environment is developed, it will improve the effectiveness of the identification, measuring, monitoring and control of operational risk, which is the Basel Committee's second key element of operational risk management.

2.5.1.2 Risk identification, measuring, monitoring and control

The second key element of operational risk management identified by the Basel Committee is the identification, measurement⁶, monitoring and control of operational risk. This key element exists out of four basic principles, which include the following (BIS, 2000g: 6):

Principle 1: Managers should identify the operational risk inherent in all types of products, activities, processes and systems. Managers should also ensure that before new products, activities, etc., are introduced or undertaken the operational risk inherent in them is subject to adequate assessment procedures.

Principle 2: Managers should establish the processes necessary for measuring operational risk (see chapter 4).

Principle 3: Managers should implement a system to monitor, on an on-going basis, operational risk exposure and loss events by major business lines.

Principle 4: Managers should have policies, procedures and processes to control or mitigate operational risk. Managers should assess the cost and the benefits of alternative

⁶ The measurement of operational risk will be discussed in chapter 4.

risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies.

In addition to the principle 1 mentioned above, this section just wants to highlight some of the processes commonly used by institutions to identify risks. The Basel Committee identified six processes that could assist managers in identifying risks, which include the following (Crouhy *et al.*, 1998: 90):

2.5.1.2.1 Risk assessments

A bank assesses its operations and activities against a menu of operational risk events. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment.

2.5.1.2.2 Risk mapping

In this process various business units, organizational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management actions.

2.5.1.2.3 Key risk indicators⁷

Risk indicators are statistics and/or metrics, often financial, which can provide insight into banks' risk position (Crouhy *et al.*, 1998: 92). These indicators should be reviewed in a periodical basis (often monthly or quarterly) to alert banks to changes that may be incentives of risk concerns. Such indicators may include for example the number of failed trades, staff turnover rates and the frequency and/or the severity of errors or omissions (BIS, 2000g: 7). (Other examples of risk indicators will be mentioned in chapter 4 and 5).

⁷ Chapter 4 and 5 will evaluate the key indicators of operational risk.

2.5.1.2.4 Thresholds/limits

Thresholds/limits are tied to the key risk indicators and alert management when there are changes in the key risk indicators and also highlight potential problem areas.

2.5.1.2.5 Scorecards

These provide a means of translating qualitative assessments into quantitative metrics that can be used to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

2.5.1.2.6 Control activities

Control activities are designed and implemented to address the risk that the bank has identified (BIS, 2000g: 15). For those risks that are controllable, the bank must decide the extent to which it wishes to use control procedures and other appropriate techniques or bear the risk. For those risks that cannot be controlled, the bank must decide whether to accept these risks or to withdraw from or reduce the level of business activity involved. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with documented set of internal policies concerning the risk management system. These control activities should also be an integral part of the regular activities of the bank for it to be effective, and should involve all levels of personnel both senior management and business unit personnel. There should also be an appropriate segregation of duties and it is important that personnel are not assigned responsibilities, which may create conflict of interest (Crouhy *et al*, 1998: 93).

2.5.1.3 The role of supervisors

The role of supervisors is the third key element in operational risk management identified by the Basel Committee (BIS, 2000g: 15). When describing the role of supervisors in

operational risk management it is important to take the two following principles in consideration (BIS, 2000g: 16):

Principle 1: Banking supervisors should require banks to have an effective system in place to identify, measure, monitor and control operational risk as part of the overall approach to operational risk management.

Principle 2: Supervisors should conduct, directly or indirectly, regular independent evaluation of bank strategies, policies, procedures and practices related to operational risk. Supervisors should ensure that there are effective reporting mechanisms in place, which allow them to remain apprised of developments of banks.

With the two above-mentioned principles in consideration, the Basel Committee has thought to establish better supervision and control over operational risk management by implementing pillar 2 (supervisory review) in the New Basel Capital Accord (see section 2.4.3.2). pillar 2 of the New Basel Capital Accord is an integral and critical component and is intended to ensure that banks have adequate capital to support the risks in their business, but also to encourage banks to develop and use better techniques in managing those risks. In cases where supervisors determine that a bank's operational risk management is either inadequate or ineffective for the bank's specific risk profile, supervisors should require improvements along with the possibility of interim additional capital buffer for operational risk, consistent with pillar 2 (Barckleys, 2001: 7).

Medova & Kyriacou (2002: 276) also stated that supervisors should seek to ensure that, where banks are part of a financial group, there are procedures in place to ensure that operational risk is managed in a consistent and propositioned way across the group. In forming this assessment, cooperation and exchange of information with other supervisors may be necessary and in some extreme cases the help of external auditors may be acquired.

2.5.1.4 The role of disclosure

The role of disclosure is the fourth key element in operational risk management identified by the Basel Committee and is based on a single principle (BIS, 2000g: 18):

Principle 1: Banks should make sufficient public disclosure to allow market participants to assess their operational risk exposure and quality of operational risk management.

Pillar 3 (see section 2.4.3.3) of the new Basel Capital Accord emphasis the importance of market discipline in supporting minimum capital requirements and the supervisory review process. The Basel Committee believes that the timely and frequent public disclosure of information by banks may lead to enhance market discipline. However, this area of operational risk disclosure is not yet well established, primarily because banks are still in the process of developing operational risk techniques (King, 2000: 167). It is the believe of the Basel Committee that where a bank has a sound operational risk management framework that identifies, control, measure and monitor operational risk in an effective manner, only then will such a disclosure framework be beneficial for assessing the markets and improve effective capital allocation and pricing (BIS, 2001a: 13).

2.5.1.5 Conclusion

The Basel Committee outlines the fact that these above-mentioned four key elements in operational risk management is not the solitary elements that bank must consider when managing operational risk, but regard it as the foundation for an effective operational risk management programme or strategy. The following section of chapter 2 will give a brief overview of the Basel Committee's supervisory guidance in terms of management structure and responsibilities.

2.5.2 Management structure and responsibilities

The Basel Committee recognizes the fact that processes for managing operational risk are evolving and want to encourage continued innovation. The Basel Committee also recognizes that few banks have in place all the elements of a sound operational risk management programme and that some banks are having difficulties with the implementation of their management structures regarding operational risk. This section therefore aims at clarifying the guidance that the Basel Committee is providing regarding the management structure and responsibility of operational risk management.

2.5.2.1 Background: Operational risk management structures

Discussions with many banks with diversified business activities indicated that operational risk is a very important component of their overall risk profiles. At a number of banks, operational risk is considered to rank second only to credit risk in terms of risk exposure and may be greater than market risk (for example, when measured in terms of economic capital allocations) (BIS, 2000g: 12). In some banks that focus on asset management or payments and processing activities, however, operational risk may present the largest potential loss exposure to a bank. The BIS (2000g: 12) stated that against this background, leading banks have, or are in the process of putting in place, clearly defined organizational structures for market and credit risk and which, in principle, reflect a decision making process that set policy on a centralized basis (generally working closely with affected business lines) and executes it on a decentralized basis.

Banks' management structures and responsibilities for operational risk vary, but a number of themes are emerging at leading banks. Many banks have established an independent operational risk management function at the corporate level that has a direct reporting line to senior management (e.g., the Chief Risk Officer) (King, 2000: 37). An emerging practice at leading banks is to rationalize the potentially overlapping responsibilities of various operational risk management committees and activities by

forming a bank-wide operational risk committee or unit with a designated head of operational risk. The head of the operational risk may, in turn, participate in a bank-wide risk committee that includes credit and market risk and can provide an effective forum to coordinate risk management activities and address potential gaps or overlaps (BIS, 2000g: 14).

2.5.2.2 The Basel Committee guidance for management structures and responsibilities

The Basel Committee has listed a number of management responsibilities for the management of operational risk, which include the following (King, 2000; 40):

- Establishing consistent definitions for operational risk across the bank's business units.
- Developing bank-level policies, procedures and practices to ensure that operational risk is appropriately identified, measured, monitored and controlled (see section 2.5.1.2).
- Producing bank-level operational risk exposure reports and forward looking key risk and performance indicators or scorecards (see section 2.5.1.2.3 & 2.5.1.2.5) for senior management.
- Overseeing and ensuring the integrity of the operational risk assessment process within the business lines.
- Implementing and maintaining the bank's economic capital assessment and allocation methodologies for operational risk.
- Developing strategies for mitigating operational risk, possibly in conjunction with risk-mitigation products such as operational risk insurance, outsourcing, operational risk derivatives and pooling arrangements.

The Basel Committee outlines the fact that the above-mentioned as well as the establishment of a bank-wide perspective on operational risk and an effective operational risk management structure is grounded in the insights and expertise of the business line

managers (BIS, 2000g: 19). The operational risk management functions typically work closely with business lines to implement bank-level policies. In many cases, the operational risk management function has independent operational risk managers within each of the major business lines whose responsibility is to assess risks at the ground level and ensure that corporate risk management policies are put in practice.

As the case for market and credit risk, management in each of the business lines will have much more detailed understanding of business processes and the primary points of vulnerability that may result in significant operational risk exposures (BIS, 2000g: 19). In many banks, business line managers are responsible for developing tracking measures for the major sources of operational risk, reporting issues for finding the independent operational risk management functions and putting in place appropriate controls.

2.5.2.3 Conclusion

The Basel Committee highlighted that guidance on management's responsibilities and structures are still in the development phase and are still not adequate for effective operational risk management. The Basel Committee also emphasizes that major discussions with banks are underway to obtain information regarding the shortcomings of management in terms of their responsibilities and structures for the effective management of operational risk. This section can then also be regarded as an introduction to chapter 3, which will examine management's conscientiousness in operational risk management in terms of asset and liability management (ALM).

2.6 Conclusion

The aim of chapter 2 was to provide an evaluation of the definition of operational risk in banks, as well as to provide an overview on the Basel Committee and its proposal for operational risk management. Regarding the definition of operational risk, the finding was that it is almost impossible to provide a single definition, because of the fact that operational risk can take so many forms. The definition provided by this chapter is also

not intended to be the decisive definition of operational risk, but it is merely intended to guide the reader of this study to a better understanding of the nature of operational risk.

Concerning the Basel Committee, it has done some fundamental work on risk management in the past few years, and the most outstanding was the issuing of a Capital Accord, which guide banks to make capital provisions for risks. It has been established that the Basel Capital Accord is widely adopted around the world. Consequently, from the viewpoint of being competitive, it is to the advantage of a bank to adhere to the prescriptions of the Basel Capital Accord. However, to stay relevant, the Basel Capital Accord was due for a review. The Basel Committee released a proposal to replace the existing Basel Capital Accord with a more risk-sensitive framework. The new framework intends to improve safety and soundness in the financial system by placing more emphasis on bank's own internal control and management, the supervisory review process, and market discipline.

The new framework also proposes for the first time a measure for operational risk. The work on operational risk is in the development stage, but three different approaches of sophistication (Basic Indicator Approach, Standardized Approach, and Advanced Measurement Approach) have been put forward. The Basel Committee expects operational risk on average to constitute approximately 15% of the overall capital charge under the new framework. The Basel Committee has stated that its goal is not to raise the aggregate regulatory capital inclusive of operational risk. Whether this is a realistic goal, is one of the issues debated by the interested parties through their comments on the proposed new Basel Capital Accord. Even the choice of definition will greatly affect the resulting capital charge. A big concern is that even the Advanced Measurement Approach will lead to excessive regulatory capital. In addition, there are concerns about the cost of compliance.

What is clear though, is that an explicit capital requirement for operational risk will have a definite impact on capital adequacy. The magnitude of this impact will be largely determined by the approach applied to calculate the operational risk capital requirement.

Which approach a bank will be allowed to use, will in turn largely depend on the quality of operational risk management and measurement.

The next chapter will evaluate the role that a bank's asset and liability management (ALM) can play in operational risk management.

Chapter 3

Asset and Liability Management for the Management of Operational Risk

“To view risk management only as the process of reducing risk is to miss potentially significant efficiency enhancement and new business and product development opportunities” (Olsson, 2002: 99).

3.1 Introduction

Concerned primarily with the strategic positioning of the balance sheet, Asset and Liability Management (ALM) is a critical function in a bank. Not only does effective ALM contribute significantly to the profitable growth of the bank, but it can be the vehicle for the bank's very survival (Fabozzi & Konishi, 1996: 1-2). The objective of this chapter is to present the theory of ALM in banks within the unifying theme of risk management and capital allocation for the management of operational risk. It is important to note that the above-mentioned will be discussed as part of the strategic management within a bank. From the outset, it should be noted that this theory is the one that provides the framework within which a bank's Asset and Liability Committee (ALCO) executes the responsibility of the overall financial planning and management of profitability and risk profile in practice.

The important part played by ALM in the overall success of the bank is being increasingly recognized across the financial sector. This, together with the realization that the ALM process involves all the activities of the bank, is transforming ALM from its traditional focus on interest rate risk management to the management of other banking risks like credit, market and operational risk, and to assist in the management and allocation of capital.

A conflict generally exists between the lenders and borrowers within a financial system. As Koch & McDonald (2000: vii) put it, borrowers are normally prepared to lend their surplus funds on a short-term basis, while lenders would acquire funds on a much longer term to finance some form of capital expansion. For a bank, which acts as financial intermediary, this results in a balance sheet with a long-term asset profile and a short-term liability profile. A bank therefore faces certain risks within the ALM structure, which must be managed by the Asset and Liability Committee (ALCO).

This chapter discusses the methods available to manage credit, market and operational risk with specific focus on risk versus return¹. As Platt (2000: 261) stated, the use of a good asset and liability model will result in better profits within a financial institution. As one of the objectives of operational risk management is to find the optimum amount of capital to absorb an operational risk loss event, an increase in profits will provide more capital and thus more capital to absorb operational risk losses. But, before this chapter starts to evaluate the importance of ALM in operational risk management, some background on ALM will be provided.

3.2 Background on ALM

To begin with an evaluation of ALM, it is important to first provide the definition of ALM in financial institutions. Thornhill (1993: 10) defines Asset and Liability Management (ALM) as the strategic planning, implementation and control processes that affect the volume, mix maturity, rate sensitivity, quality and liquidity of the banks assets and liabilities. As can be seen in the above-mentioned definition, ALM is more than just effective control of individual assets and liability categories. Bessis (2001: 21) and Gardner *et al* (2001: 30) have stated that ALM is also the attempt to stabilize net interest margin with no expected variation – that is, together with the attempt to minimize risk. It is an integrated approach to financial management, requiring simultaneous decisions about the types and amounts of financial assets and liabilities the institution holds

¹ Risk versus return focus on finding the optimal between risks that the bank takes and the profit it makes. The bank will try to maximize profit while maintaining an acceptable level of risks.

(Gardner *et al.*, 2001: 31). In addition to the above-mentioned, ALM also requires an understanding of a broad range of financial markets in which institutions operate. Among the most significant financial market issues to consider, is how interest rates are determined, and why they change over time and what is the impact of the changes in the interest rate on the net interest margin (NIM). ALM entails understanding of the non-interest revenue and expense implications of an institution asset and liabilities, as well as the efforts to limit the volatility of the earnings. Ong (1998: 23) stated that an ALM always starts with an analysis of the balance sheet – an analysis of what items are regarded as on-balance sheet items and what items are regarded as off-balance² sheet items. In addition to the above-mentioned, the balance sheet can be defined as a statement of financial institution's financial position of business enterprise which report major categories and amounts of assets, liabilities and stockholders equity and the interrelationship in a specific point in time (Ong, 1998: 24). In its Statement of Financial Accounting Concepts (SFAC), the Financial Accounting Standards Board (FASB) define the above-mentioned three elements of the balance sheet as (Dempsey & Pieters, 1996: 2-5):

- **Assets:** Assets are the probable future benefits obtained or controlled by a particular entry as a result of past transactions or events.
- **Liabilities:** Liabilities are probable future sacrifices of economic benefits arising from present obligations of a particular entity to transfer assets or to provide services to other entities in the future as a result of past transactions or events.
- **Equity:** Equity is the residual interest in the net assets of an entity that remains after deducting liabilities, which include stockholders equity.

The major categories of assets, liabilities and equities are classified according to liquidity – that is their expected use in operations or conversions in cash in the case of assets, and

² Items not included in the balance sheet are called off-balance sheet items, and both on-and-off-balance sheet items are then carefully accounted for.

time to maturity for liabilities (Botha, 1999: 154). Dempsey and Pieters (1996: 1) classify assets in two classifications:

- **Current assets:** Current assets are assets which are expected to be converted to cash or used within one year or operating cycle. Current assets include cash and cash equivalents, marketable equity securities, receivables, inventories and prepaid expenses.
- **Long-term assets:** Long-term assets are assets which are expected to provide benefits and services over periods longer than a year. Long-term assets include property equipment, investments in affiliated companies and intangibles such as brand names, patents, copyrights, and goodwill.

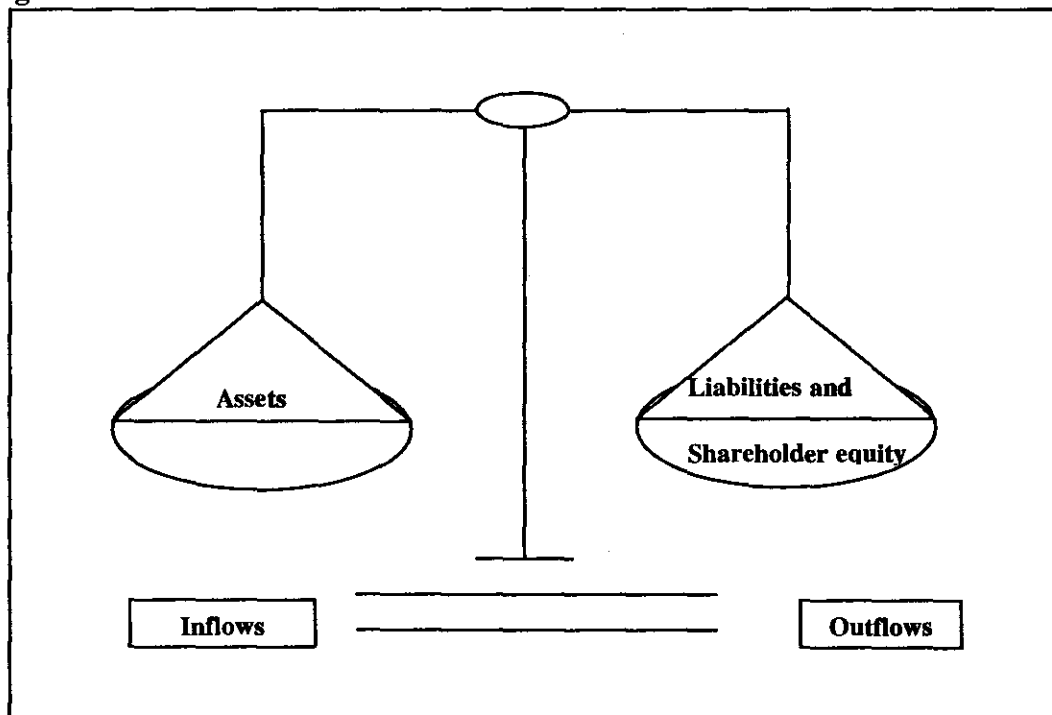
A similar classification hold for liabilities (Dempsey & Pieters, 1996: 2):

- **Current liabilities:** Current liabilities are obligations the institution is expected to settle within one year or operating cycle.
- **Long-term liabilities:** Long-term liabilities are obligations the institution has to repay more than one year later. These include bank debt, obligations, pensions, and other liabilities such as defined income taxes and minority interest in net assets of conciliated affiliates.

When ALM is understood, it can become a process universally known as a system of timely matching of cash in- and outflows that is liquidity management (Bastany, 1994: 43). These cash in- and outflows are illustrated in figure 3.1 as part of an illustration of a balance sheet of a financial institution. With a balance sheet, all the assets are on the one side with all the liabilities on the other side, and it is important that these assets and liabilities balance each other out in order for the balance sheet to be an effective reflection of the institution's financial wellbeing. The above-mentioned will be better understood when viewing it in terms of cash in- and outflows. In the balance sheet the

inflows must equal the outflows in order for it to balance. In other words, for each outflow of funds there must be an inflow of funds. If the in- and outflows balance there will be no liquidity gap³ and there will be an inflow of funds when there is an outflow of funds. In other words, there will be funds available when needed; for instance, funds to buffer an operational risk loss event.

Fig. 3.1 The balance sheet



Source: (Ong, 1998: 201)

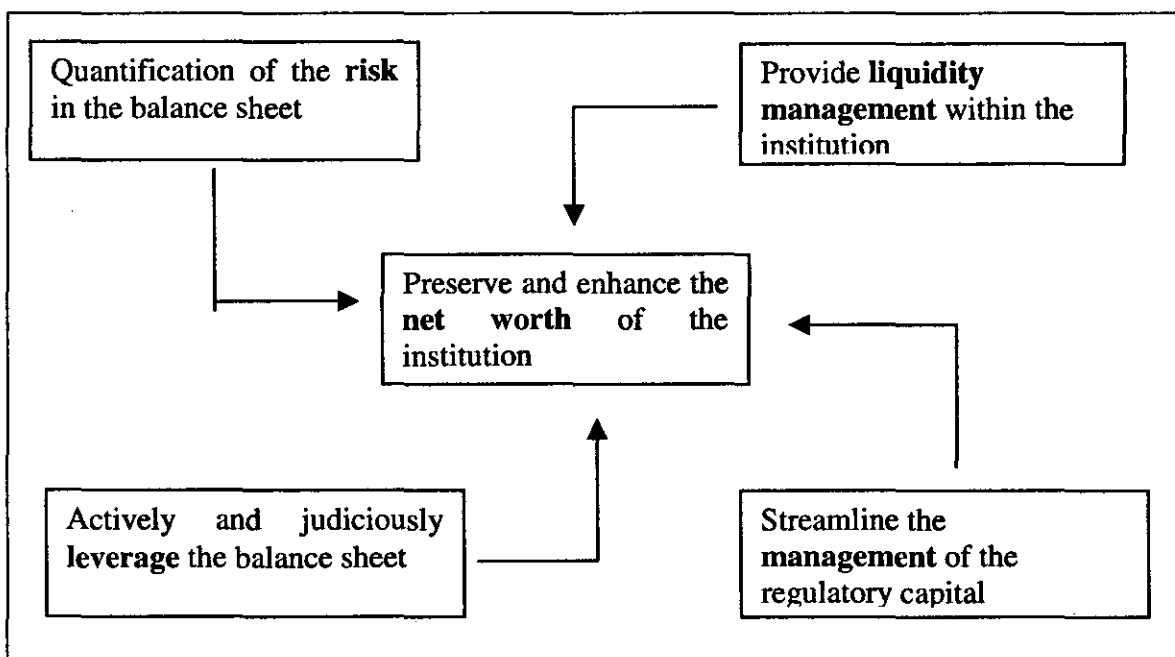
The above-mentioned then concludes the discussions on the background of ALM. The following sections of chapter 3 will now discuss the objectives of ALM followed by a discussion of the ALM structure and responsibilities.

³ A liquidity gap is differences between outstanding balances of assets and liabilities, or between their

3.3 Objectives of ALM

It is important to evaluate the objectives of ALM in order to get a clear view on what a bank is trying to achieve with ALM. Some may ask the question, why mention the objectives of ALM when evaluating operational risk management? The answer is simple. ALM is in charge of managing the inflow and outflow of asset/liability related funds. In other words managing the bank's balance sheet. Capital is also part of the bank's balance sheet, and as mentioned in chapter 2, capital is also used to absorb risk-related losses. Therefore in terms of risk management, ALM plays a fundamental part in risk management by ensuring that the right amount of capital will be available at the right time. It is important to keep the above-mentioned in mind, to be able to understand the following sections in terms of operational risk management.

Fig. 3.2 Fundamental objectives of ALM



Source: (Grosse & Hempel, 1999: 27)

changes over time (Bessis, 2001: 137).

The following points will then name the fundamental objectives of ALM stated by Sargent (1995: 103) and are also illustrated in figure 3.2.

- The ALM process must preserve and enhance the net worth of the institution.
- ALM is the quantification of various risks in the balance sheet.
- ALM must streamline the management of regulatory capital.
- ALM should provide liquidity management within the institution.
- ALM should actively and judiciously leverage the balance sheet.

These objectives, although stated broadly – tacitly assume a financial accounting framework, but they do not highlight accounting as the ultimate goal. Proactively tacking a stance to quantify risk, ALM is streamlining management processes with the ultimate goal of preserving and enhancing the institution’s net worth through whatever means.

The following sections of chapter 3 will then describe the above-mentioned fundamental objectives of ALM in more detail.

3.3.1 Preservation and enhancement of net worth

As mentioned in previous sections, the most important function of ALM is to preserve and enhance the net worth of the institution through whatever means available to it (Ong, 1998: 3). The objectives mentioned above do not limit the scope of ALM functionally to mere risk assessment, but expand the process to the taking on of risks that might conceivably result in an increase in economic value of the balance sheet. As Sargent (1995: 103) puts it, ALM should focus on managing the net worth of the institution under uncertainty while satisfying certain constraints. The uncertainty may take the form of interest rate movements, volatility in portfolio earnings and/or general economic conditions; while the constraints can be driven primarily by regulatory requirements, corporate appetite for risk, and expected levels of performance and returns (Ong, 1998: 4).

The ability to balance the uncertainty with the constraints while maintaining (or even increasing) the net economic value of the institution, is the major concern for ALM. In fact, after all is said and done, the ALM function indeed serves as the single most important risk management function of the institution, encompassing both reactive and proactive stances against market movements and projected market conditions – and this is what makes ALM strategic.

3.3.2 Quantification of risk in the balance sheet

As mentioned in the problem statement in chapter 1, the effective quantification of a risk is one of the biggest concerns for risk managers. The second objective of ALM is then to quantify risk in the balance sheet and is another important reason why ALM is important for operational risk management. The delicate act required in the preservation and enhancement of its net worth presupposes an institution's ability to measure thoroughly all the various manifestations of risk on and off the balance sheet. There are five basic risks that need to be measured and managed in the balance sheet and include credit, market, operational, interest and liquidity risk. These risks also exist of different components as is illustrated in figure 3.3 on page 65.

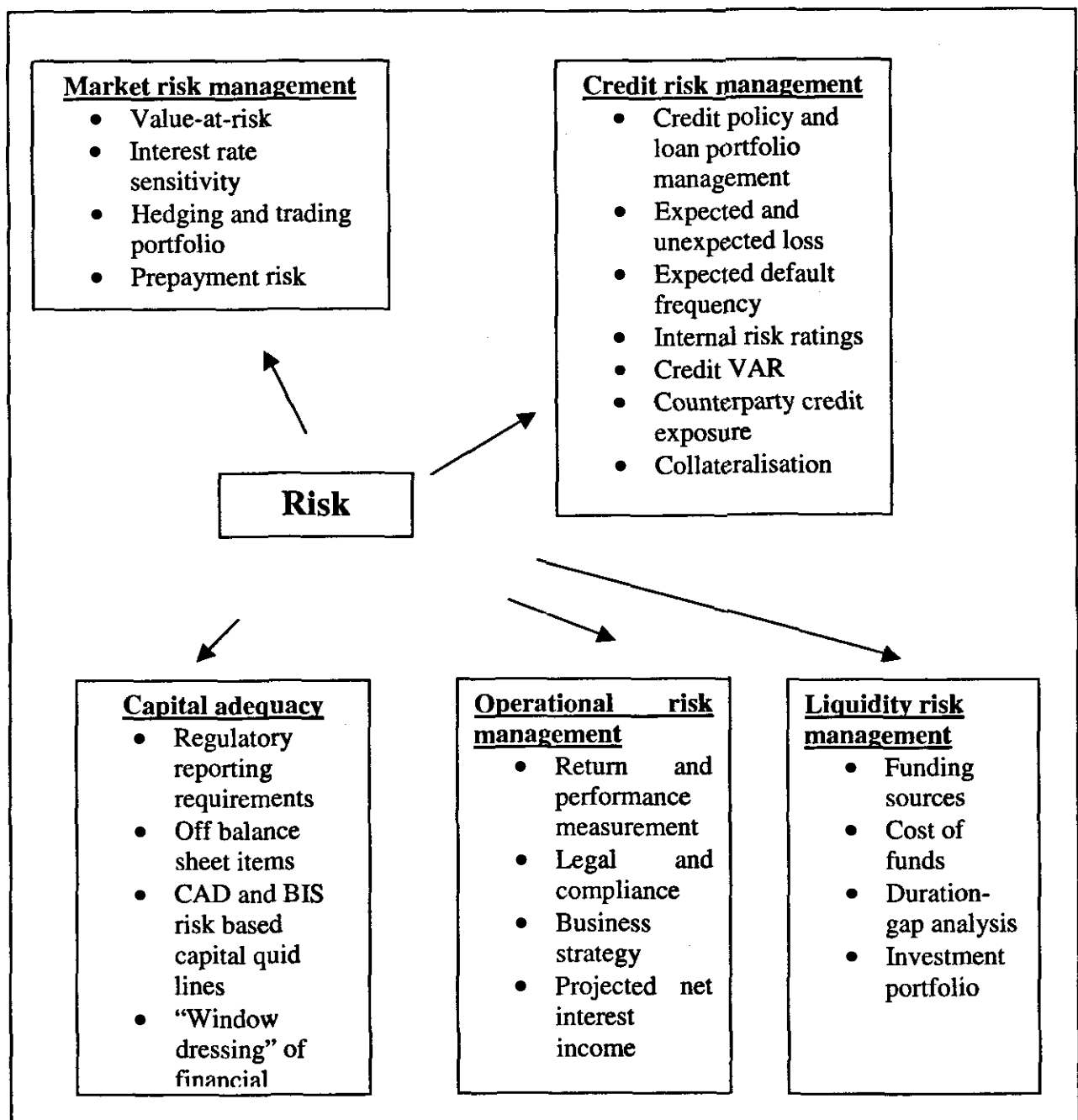
In addition to the above-mentioned, Jarrow and Van Deventer (1999: 132) declared that as financial markets continue to become more transparent, two important phenomena regarding the quantification of risk begin to emerge:

- Objective statistical measures of risk are rapidly supplanting traditional assets and liability measures.
- Market-to-market valuation of assets and liabilities becomes more readily available as markets become more liquid and better established.

These two above-mentioned developments allow a significant portion of the embedded risk in a financial institution's balance sheet to be adequately quantified, and they

therefore facilitate prudent risk management. Consequently, institutions that primarily serve as financial

Fig 3.3 Major components of risk in the Balance Sheet



Source: (Jarrow & Van Deventer, 1999: 4)

intermediaries can take on larger amounts of risky assets and yet be able to transform them into relatively safer ones by means of diversification and specific expertise in market and credit risk management (Jarrow & Van Deventer, 1999: 17). Furthermore, these two developments in the market did not arrive unnoticed within regulatory circles. As a consequence of the increasing ability to use market-to-market valuations and statistical quantification of risks, new regulatory rules were enacted (Jarrow & Van Deventer, 1999: 17). These actions also partly stem from the uniform authority of financial institution's asking for the mandate to begin using their own internal models for risk measurement and capital attribution (Jarrow & Van Deventer, 1999: 17).

3.3.3 Management of regulatory capital

The management of regulatory capital is the third objective of ALM. More recently, risk-based adequacy requirements have been extended to include the market risk activities undertaken by an institution (see chapter 2). The wisdom is that, other things being equal, institutions holding a riskier portfolio must have higher capital reserves levied against them (Jarrow & Van Deventer, 1999: 19). In other word the higher the potential risk the bank face, the higher amount of capital must be held.

Depending on how financial institutions leverage their balance sheets and how they circumvent the interpretation of these capital adequacy guidelines, the capital requirements across similar types of institutions can vary widely. On its introduction on May 1993, the Financial Accounting Standards Board (FASB) statement no. 115 (Bitner & Goddard, 1995: 110), forced many financial institutions to rethink how their portfolios are managed for income, liquidity and control of operational and interest rate risk (Bitner & Goddard, 1995: 111). How did this happen? The answer is simple. Prior to FASB 115, accounting restrictions governing the scale of investments allowed many financial institutions to follow a buy-and-hold investment strategy, whereby securities are held to maturity except for certain permissible sale and transfer in the events of deterioration in a users credit quality.

Under the FASB 115, securities in the portfolios are then classified as one of the following (Bitner & Goddard, 1995: 111):

- **Hold to maturity (HTM):** Debt securities that is intended to be held to maturity and whose valuations are reported at amortized cost.
- **Trading securities:** Debt and equity securities purchased for short-term gains and for which assets are required to be market-to-market for reporting purposes.
- **Available for sale (AFS):** Debt and equity securities which are neither intended for, nor held to maturity, and whose valuations are reported at fair market values.

Placing an asset in the appropriate category has significant ramifications as far as an institutions ability to manage interest rate and liquidity risk and its flexibility in leverage the balance sheet (see section 3.3.5) are concerned, but when a financial institution has its assets in an appropriate category the risk that a booking error can be made is also minimized because of better control over the balance sheet. Therefore, the risk of human errors is also minimized and thus operational risk as well. This objective of ALM is probably the most applicable to operational risk management in the sense that if it is effectively achieved, there will be sufficient capital to absorb an operational risk loss event. The management of regulatory capital is essential for operational risk management, but cannot be achieved without the following objective, which is liquidity management.

3.3.4 Liquidity management

Every financial institution requires a certain amount of liquidity to meet its short-term liabilities. Although in principle this implies either the need for access to quick short-term and low cost funding, in the event of an unexpected operational risk loss event, or to have assets with significant short-term cash flows, in the event of an expected operational risk loss event (Maitz & Smith, 2001: 12). As Bitner & Goddard (1995: 112) stated, a

combination of both is ideal since low cost funding might not be available all the time. The role of the ALM process is to ensure that the short-term in-and outflow processes in the balance are carefully balanced to prevent a funding crises (Maitz & Smith, 2001: 12). Classifying too many assets as available for sale, results in too many assets being regarded as capital adequacy risk items (Cade, 1997: 469). Classifying too few as capital adequacy risk items may result in a decrease in the investment portfolio (Cade, 1997: 469). In many ways therefore, financial institutions are faced with a double-edged sword in providing liquidity, and yet, being able to protect their capital. Liquidity management and the streamlining of regulatory capital in the ALM process is therefore one and the same issue and are, therefore both important to the management of operational risk (Cade, 1997: 470).

Liquidity management is one of the main objectives of a bank or financial institution, because if there are not enough internal funds available, a bank must raise funds externally, which is nine times out of ten more expensive. Liquidity risk might become a major risk for the banking portfolio, but does not fall within the scope of this study.

3.3.5 Actively leveraging the balance sheet

Why take risk if there is no reward? Why balance the balance sheet if the ultimate purpose is simply the mere act of balancing inflows with outflows. There has to be a profitable side to risk management, and this is where the fifth objective of ALM comes in. ALM is an insurance policy that allows financial institutions to assume intermediation risk (Jarrow & Van Deventer, 1999: 137). In their intermediary and fiduciary roles, institutions assume primarily two kinds of risks – interest rate and credit risk – amongst others, but there is one risk that is having an increased effect on financial institutions – operational risk.

Relative to its competitors, an institution actively and judiciously shifts positions (either through trading activities or by asset classification) within the balance sheet and off balance sheet, capitalizing on its (Jarrow & Van Deventer, 1999: 141):

- Superior internal expertise in market and credit risk analysis and risk management systems for measuring and control.
- Superb delivering system and low cost funding access.
- Excellent management of regulatory and economic capital.
- Proper use of risk-adjusted return methodology.
- Cutting edge quantification of the embedded optionality in the balance sheet to hedge against prepayment risk.
- Prudent use of derivatives to hedge against portfolio risks.

An institution does this with the aim of deriving a significant advantage, Vis-à-vis its competitors, in leveraging its own balance sheet, thereby enhancing its value and at the same time assuming only a reasonable level of risk. The above-mentioned then concludes the discussion on the fundamental objectives of ALM and the following sections will then discuss the managerial objectives of ALM, which will also play a part in operational risk management.

3.3.6 Managerial objectives in financial institutions

It is the view of this study that these managerial objectives of ALM will also improve operational risk management, and will therefore be discussed in the following section. Fabozzi and Konishi (1996: 173) classified two types of managerial objectives in financial institutions:

- Customer needs objectives.
- Ownership needs objectives.

These two above-mentioned objectives are crucial for the effective control over ALM, and for reducing the cost associated with the management of a financial institution (Cebnoyan *et al*, 1993: 153). As mentioned, these objectives will provide better control over ALM and this control will ensure that fewer operational risks will occur in ALM itself. The following sections will then discuss these above-mentioned objectives. It is

important to remember that these managerial objectives are not necessarily the managerial objectives of operational risk management, but are mere intended to give some background on ALM.

3.3.6.1 Customer needs objectives

Because financial institutions provide liquidity to customers when using secondary security such as demand deposits, the problem of identifying customer needs in financial institutions differs from those in non-financial institutions, which face no need to honour financial liabilities on demand (Gardner et al, 2001: 174). Therefore, the need to provide customers with the benefits of intermediation must be considered in establishing managerial objectives for financial institutions. In addition, asset and liability decisions must be made simultaneously in financial institutions, but the classical theory of non-financial institutions does not consume joint considerations of investment and financial decisions (Gardner et al, 2001: 174).

It is important then from the above-mentioned, that financial institutions must have personnel responsible for identifying customer needs in order for management to set objectives to serve these needs in such a way that customers will be satisfied with the service they had received, and that the financial institution benefit from these services.

3.3.6.2 Ownership structure objectives

The ownership structure of many financial institutions also differs from those of non-financial institutions. Instead of being owned by stockholders⁴, many financial institutions are mutually owned, except for South African institutions and firms (Saayman, 2002: 121). The mutual form of organization is particularly prevalent among insurance companies and savings banks (Maitz & Smith, 2001: 19), although many have converted in recent years to stockholder-owned institutions. It is enough to recognize

⁴ Stockholders are people who have risk funds to start a business and who are entitled to residual profits that the institutions generates.

that the so-called owners of mutual owned institutions are owners in the classical sense, because they are not entitled to personal claims on residual profits. Therefore, the classical theory based on the idea that those whose risk funds are entitled to establish the objectives of the enterprise and may not be directly relevant to market organizations. In addition to the above-mentioned, the following section will provide some practical evidence from research.

3.3.6.2.1 Evidence from research

Empirical evidence of stockholder owned institutions suggests that unmonitored managers do act to maximize their own rather than the owner's welfare, whether or not they should do so (Allen & Cebenoyan, 1991: 425-428) – thus agency costs arise. This can then also be a potential operational risk that can be included in the list of potential operational risk events mentioned in chapter 2. This evidence also noted that built-in “brakes” in manager behaviour in stockholder-owned institutions may help to reduce these cost. These limitations arise both from potential monitoring actions by current stockholders themselves, and from the discipline imposed on managers by external financial market participants. For example, contracts may specify that managers will be compensated in part through stock options, thus ensuring at least partial compatibility between their interest and those of current owners (Gardner *et al.*, 2001: 27).

Secondly, stockholder exercise voting control has been implemented in such a way that stockholders can radiate managers for overly self-interest decisions made by them. Finally, stockholder-owned institutions operate within a market for corporate control; outsiders who believe that an institution is not well served by current management, may bid for the institution's stock and hire new managers to control the assets (Cole & Eisenbeis, 1996: 27). Empirical research on large banks and thrifts suggests that rising management compensation corresponds to increase institution performance, and that managers risk taking behaviour is related to the value of their holdings of the institution's stock, subjected to the regulatory environment (Cole & Eisenbeis, 1996: 28).

As mentioned earlier in this section, these managerial objectives do not necessarily form part of operational risk management but are merely intended for a better understanding of ALM in order to better understand the role that ALM plays in operational risk management. This section then also concluded the first part of chapter 3, which was intended to name and evaluate the objectives of ALM. The second part of chapter 3 will evaluate the management structure and responsibilities of ALM, in other words the people who are responsible for setting and implementing these above-mentioned objectives. The second part of chapter 3 will then go further and also give a thorough evaluation of the Asset and Liability Committee (ALCO) – the personnel who are responsible for the whole ALM process and then also to determine the role that they play in operational risk management.

3.4 ALM structure and responsibilities

Section 3.4 is intended to give an overview of the people who are responsible for setting the above-mentioned objectives and overseeing that they are achieved. As mentioned ALM involves managing the institutions net interest margin (NIM) in accordance with its objectives and, therefore managers are required to understand these objectives and also have the responsibility of setting them (Gardner et al, 2001: 34). The identification of objects is somewhat more complex for financial institutions than for other business. To understand this complexity, a brief outline of theories on the setting of managerial objectives, amongst other, must be considered. These theories have arisen from the study of financial management of non-financial institutions (Gardner et al, 1996: 34). These above-mentioned theories will now be discussed in the following sections.

3.4.1 Theories on the setting of managerial objectives

Observers often argue that owners should set objectives for financial institutions operating in competitive markets (Kupiec & Nickerson, 2001: 12 & 15). Owners, unlike directors, provide the initial funds to operate the business, so they are entitled to many benefits resulting from superior operations. There are two theories that must be

considered when setting objectives for ALM, and these include the following (Kupiec & Nickerson, 2001: 15):

- The classical theory.
- Agency theory.

3.4.1.1 The classical theory⁵

The classical theory of the institution focuses on how managers should act, and thus it is considered a normative theory (Gardner & Mills, 1997: 120). This approach states clear criteria for managerial decision-making. If a decision provides net benefits to owners, it should be made; otherwise, it should not. This classical theory leaves no doubt that the institution's owners (i.e., the board of directors) are the ones to set objectives for ALM (Gardner & Mills, 1997: 120).

This theory also directs managers to ignore their personal risk/return preferences in making the institution's decisions. Instead they should concentrate on maximising expected benefits to owners, consistent with the risk that owners are willing to bear. Managers that allow non-owner determined objectives to influence their decisions will presumably be removed by unhappy owners (Gardner *et al.*, 2001: 33).

3.4.1.2 Agency theory

Agency theory is a positive theory of managerial behaviour. Positive theories in managerial behaviour focus on explaining how decisions are made by business managers, rather than on prescribing how they should be made (Bastany, 1994: 331). When owners also manage their financial institutions, the way they should behave must then also be with respect to other financial institutions that are managed by non-owners and with respect to the way they manage their institutions. But if managers and owners are

⁵ This classical theory of managerial objectives is developed in Fisher, 1930. Extensions of Fisher's work are provided in Hirschlifer, 1958 and in Hirschlifer, 1965.

different people, managers' risk/return preferences may differ from those of owners. The question is what managers must do under these circumstances. Positive theories of management objectives attempt to explain the behaviour of managers arising from separation of ownership and control (Cruz, 2002: 12).

As mentioned above, a positive theory of managerial decision making suggests that managers are no different from other individuals: if left unmonitored, they will pursue their personal risk/return preferences (Gardner et al, 2001: 110). Thus, owners may incur costs in making sure that their preferences are recognized. Agency theory examines the relationship between non-owner managers (agents) and owners (principles) and the contract arising as a result. These agent/principle agreements are yet another form of financial contracting, leading to associated monitoring cost (Gardner et al, 2001: 12). At one extreme, an agent/principle contract could be structured in such a way that every action of the agent would be prescribed and closely monitored, leaving the manager no discretion (Jackson et al, 1997: 343). Such a contract would be very costly for the principle to enforce. At the other extreme, the owner could take a "hands-off" approach, leaving all matters to the manager's judgment. Although monitoring cost would be zero under such a contract, the potential losses to owners could be considerable if managers exclusively pursue their own interest. Normally, therefore, terms of agent/principle contracts fall between those extremes. Any reduction or benefit to owners stemming from contracts governing the separation of ownership and control are known as agency cost (Gardner et al, 2001: 13).

In practice, agency cost can take many different forms, such as legal expenses to draw up contracts that limit the manager's salaries and expense accounts and also the resources managers spend on annual reports convincing owners decisions considering their wishes (Jackson et al, 1997: 344). Agency cost arising from managers' unmonitored actions may be more difficult to measure. One example is the potential loss when managers are lending to a friend's business at a rate lower than justified by the risk of the loan.

An institution may incur a special type of agency cost when managers are not closely monitored; which can lead to so called managerial expenses preferences, which is the tendency for some managers to enhance the benefits they receive from their institutions by hiring larger staff than necessary or furnishing offices lavishly and/or enjoying high class travel arrangements⁶ (Jackson et al, 1997: 340). Financial institutions face even a greater chance of a potential abuse by managers and other employees in the form of fraud or embezzlements than non-financial institutions. All types of agency costs reduce the owner's welfare and would not be incurred if owners managed their companies.

Examples of the above-mentioned expenses preferences behaviour are widespread. In particular, managers of a number of savings and loans in the 1980's made purchases that approached looting their institutions (Jackson et al, 1997: 341). David Paul, the CEO of Centrust Savings in Miami, Florida, bought an expensive rare art worth \$29 million with bank funds, also spending \$17 million on a yacht and \$1.4 million for a corporate jet (Falkena et al, 1995: 197). Owners therefore, must structure contracts that align managers' rewards with their own, to keep their cost lower than the cost they would incur by letting managers operate unchecked (Falkena et al, 1995: 199). Agency cost theory therefore, implies that managers set ALM objectives and that owners protect their interest by setting appropriate constraints.

The above section then provides the answer to the question of who is responsible for setting ALM objectives, which is the responsibility of the Board of Directors, and also discussed the theories that will help them in achieving these objectives. The following section will then continue the evaluation of ALM and the role that it plays in operational risk management by evaluating the Asset and Liability Committee (ALCO) and the role they are playing in operational risk management. The section will begin by describing how an ALCO is formed, followed by a discussion of the ALM process, which is the responsibility of the ALCO.

⁶ The theory of managerial expenses preferences was developed by Williamson, 1963.

3.4.2 Forming an Asset and Liability Committee (ALCO)

The foundation of ALM is the Asset and Liability Committee (ALCO), which is responsible for the ALM process in banks (Marè, 1995: 3), and the forming of such a committee must be one of the first steps when developing an asset and liability strategy (Marè, 1995: 5). The following section will provide some general information regarding the ALCO and the people who are responsible for forming an ALCO.

3.4.2.1 The ALCO in general

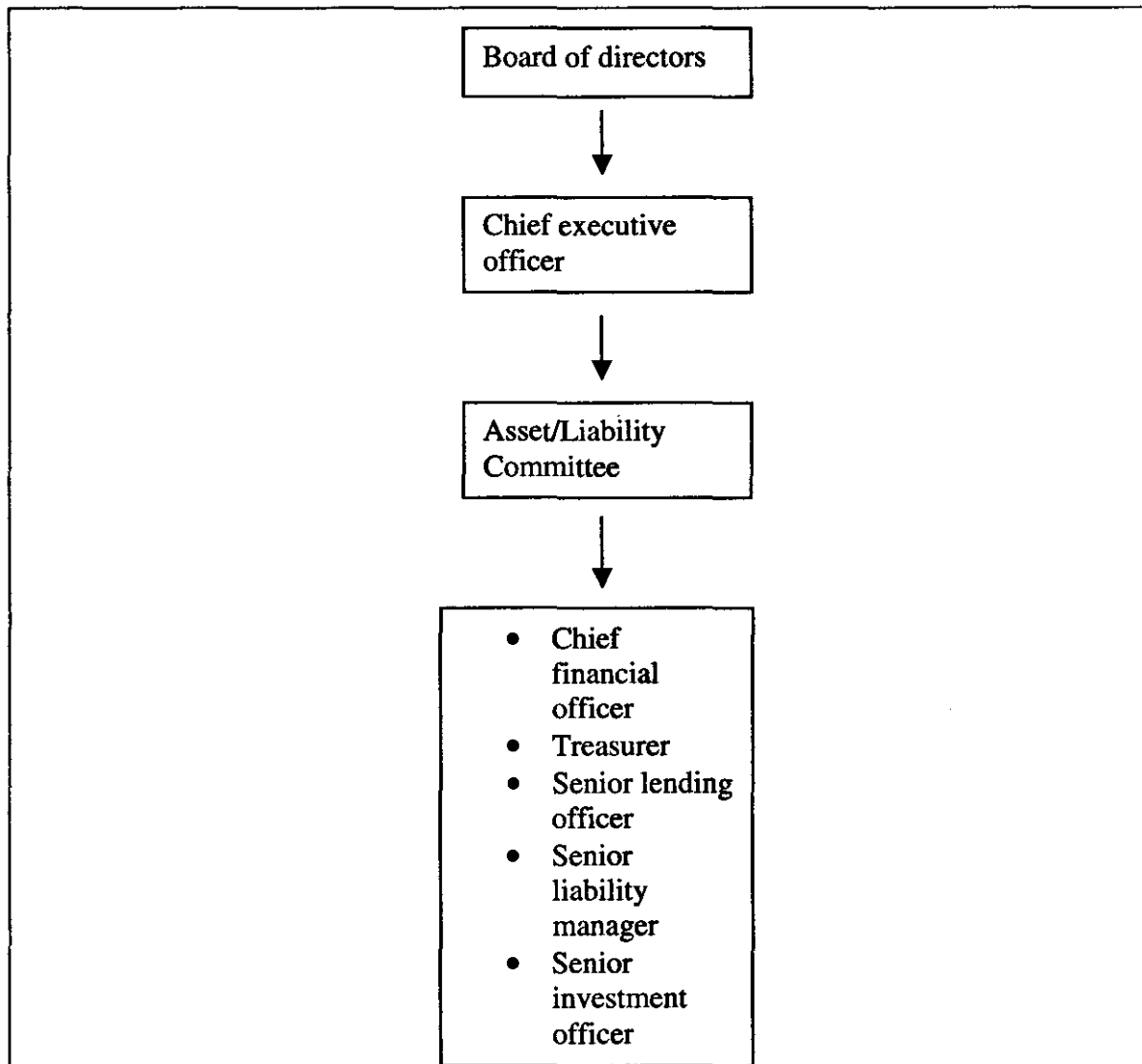
As mentioned above, the ALCO is in charge of the ALM process and one of the major reasons for the failing of ALM is that some managers do not give enough attention to this part of the ALM process, which may lead to an ineffective ALCO in banks (Styger, 1997: 2). The ineffective forming of an ALCO can then also be considered as an operational risk that the bank must cope with. The most important factor when forming an ALCO must be to have the support of the chief executive officer (CEO) (Styger, 1998: 12).

The CEO's support should be a clear indication to all the departments of the organization to cooperate with the asset/liability manager in establishing and maintaining the ALM process. It is necessary to have the cooperation of all the departments because every area of the organization will be involved in the process (Bitner & Goddard, 1995: 10). The accounting department must supply a constant supply of current and historical data to the asset/liability system. The marketing department is used to design new products and encourage customers to use certain existing products that are consistent with the ALCO' objectives. The investment department's actions as well as the pricing of loans and deposit products must be coordinated with the liquidity and interest rate risk objectives of the ALCO. Because ALM addresses the risk inherent in the balance sheet, every area of the institution is involved in the ALM process (Bitner & Goddard, 1995: 11).

The CEO's support must be more than tactical permission for the development of an ALM process. The CEO must designate ALM as a high priority objective of the

institution and clearly communicate that message to every level of management within the institution (Styger, 1997: 2). If the CEO is not going to assume responsibility for the ALM process, a senior manager must be designated as the asset/liability manager. A good candidate for the asset/liability manager would be a senior executive, thoroughly familiar with finance and, in particular interest rate theory (Bitner & Goddard, 1995: 13).

Fig. 3.4 Asset and liability management structure



Source: (Bitner & Goddard, 1995: 17)

Figure 3.4 is an illustration of an ALM structure and it is important to notice that it is the responsibility of the board of directors as well as the CEO to select an ALCO which is represented by senior staff, which include the chief financial officer, the treasurer, the senior lending officer, the senior liability officer and the senior investment officer (as seen in figure 3.4) (Bitner & Goddard, 1995: 12).

The first action of the asset/liability manager should be to appoint the members of the ALCO. The ALCO must be large enough to include the major areas of the institution that will be the most heavily involved in ALM, but not be so large that it becomes difficult to function effectively (Bitner & Goddard, 1995: 22). Ideally the ALCO should consist of at least four members, but not exceed eight members (Styger, 1997: 4). The ALCO will made major decisions based on the data entered into the simulation model⁷ and other reports supplied by the accounting department (Bitner & Goddard, 1995: 19).

There are several goals that the ALCO is trying to achieve, which include the following (Marè, 1995: 6):

- Keep the level of interest rate within stated goals.
- Enhance the institution's net income.
- Provide adequate liquidity to the institution.

Defining the role of the ALM function and stating the ALCO's above-mentioned general goals, not only prove a clearly stated base for the future ALM actions, but also form the beginning of the ALM policy. Marè (1995: 7), not only affirmed the main goals or objectives of the ALCO, but had also stated some of the reasons for the ALCO to fail. These reasons include the following:

- **Unclear purpose:** Not everyone in the ALCO knows what is required of him or her and what management want him or her to achieve in the ALCO.

⁷ The building of an ALM simulation model will be discussed in a later section of this chapter.

- **Wrong Tools:** Members of the ALCO are sometimes using the wrong tools for the job; for example, they are using a long-term analysis when a short-term analysis is required.
- **Staffing of the ALCO:** The ALCO is sometimes wrongly staffed; for example, a driven bank is staffed with investment personnel and vice versa.

The above section was intended to provide an overview on the ALCO and its objectives. In this section, it has become clear that the ALM of a bank can only be effective if the ALCO is effective. It is thus important that the members of the ALCO are personnel with a thorough knowledge of the banking industry and in particular the ALM structure within a bank. As Marè (1995: 2) mentioned, ALM is strategic. In other words, ALM uses simulations to predict certain events (for example an increase in the interest rate) to make an informed decisions regarding, for example, the selling or buying of an asset or liability. As an operational risk event can occur at any time in the future, these ALM simulations may also assists mangers in identifying a potential operational risk event. This is where the ALCO comes in. As mentioned in the beginning of this section, the ALCO is in charge of the ALM structure and the ALM process and it is also the ALCO who uses these simulations to make their decisions, thus, by doing these simulations, the ALCO is in the position to identify a potential operational risk. The following section will now evaluate strategic management and then also determine the role that the ALCO is playing in strategic management as well as in operational risk management.

3.4.2.2 ALCO in strategic management

As acknowledged by Maitz & Smith (2001: 15), risk management is not about avoiding risk, but it is about managing the risk. These risks must be made visible, measured and managed, and the interrelation between these risks must be understood (Maitz& Smith, 2001: 15). In the past, the task of the strategic management of a bank's assets and liabilities have been delegated to the CEO of the bank. But now, the board of directors is required to be fully informed of the details of the bank's strategic management process of the assets and liabilities and its execution by the CEO (Styger, 1997: 2-3).

The ALM process (see section 3.4.2.2.2) is the bank's strategic decision-making process (Styger, 1997: 2) and it is required of the board of directors to have a good knowledge of this process. The board should also have a good working knowledge of the ALM strategic decision-making process and simulation software, its capabilities and its proper use. In the above-mentioned paragraphs, a lot has been said about strategic management. But, what is strategic management? The following section will provide the answer to this question and also provide a detailed evaluation of the strategic ALM process.

3.4.2.2.1 Strategic management

Strategic management is necessary to bridge the gap between the current state of the institution and the desirable future state (Kroon, 2000: 35). Formal strategic planning systems not only improves the performance of the institution but also forces management to consider and support strategic issues. Now what exactly is a strategy? A strategy is (Kroon, 2000: 35):

- Fundamental patterns of planned and present objectives.
- Resource deployments.
- Interaction of an institution with the market competitors and other environmental factors.

In addition to the objectives of ALM discussed in section 3.3, the following objectives can be included with strategic ALM:

- Reduce the variation in the interest margin.
- Increase price gains.
- Reduce price losses.

The ALM process is both static and dynamic. Static ALM involves the identification of existing risks and re-positioning assets or liabilities to reduce risks or to increase profits. Dynamic ALM involves identifying likely future vents and planning responses or strategies, which involves the institutions' mix of assets and liabilities (Scott, 1999: 215-216). There are seven known advantages of a strategic ALM-process (Styger, 1997):

- Better control of the net interest margin.
- Better cash flow/liquidity management.
- To be pro-active, rather than reactive.
- Better equipped for increased competition.
- Better equipped for more sophisticated markets.
- Can demonstrate that the treatment of public savings is done in a scientific basis in other words, pass the reasonable man test
- Improve the budgeting process.

The above-mentioned, are the advantages that a strategic ALM brings to a bank, but more important is that a strategic ALM improves operational risk management in the sense that potential operational risk events can be predicted to a certain degree of accuracy. If, for example an operational risk event can be predicted to a certain degree of accuracy, it would be easier to measure this event and it would be easier to provide sufficient capital to absorb this event, in other words to ensure against the risk. For the ALCO to be strategic and to assist the bank in risk management, it must follow a strategic process, which is called the ALM process (Marè, 1995: 5). The following section will provide an insight into this process.

3.4.2.2.2 The ALM process

ALCO is in charge of the strategic ALM of the bank and a ten-step process represents this strategy (Marè, 1995: 5). It is important to keep in mind that capital must be held to absorb an operational risk loss, and it is the intention of the bank to predict such an event to be sure that there is sufficient capital to absorb such a loss. The ALM process can

assist risk managers in predicting such an event, and this is one of the main reasons why ALCO is important in operational risk management. Marè (1995: 2-5) affirmed the following ten steps of the ALM process.

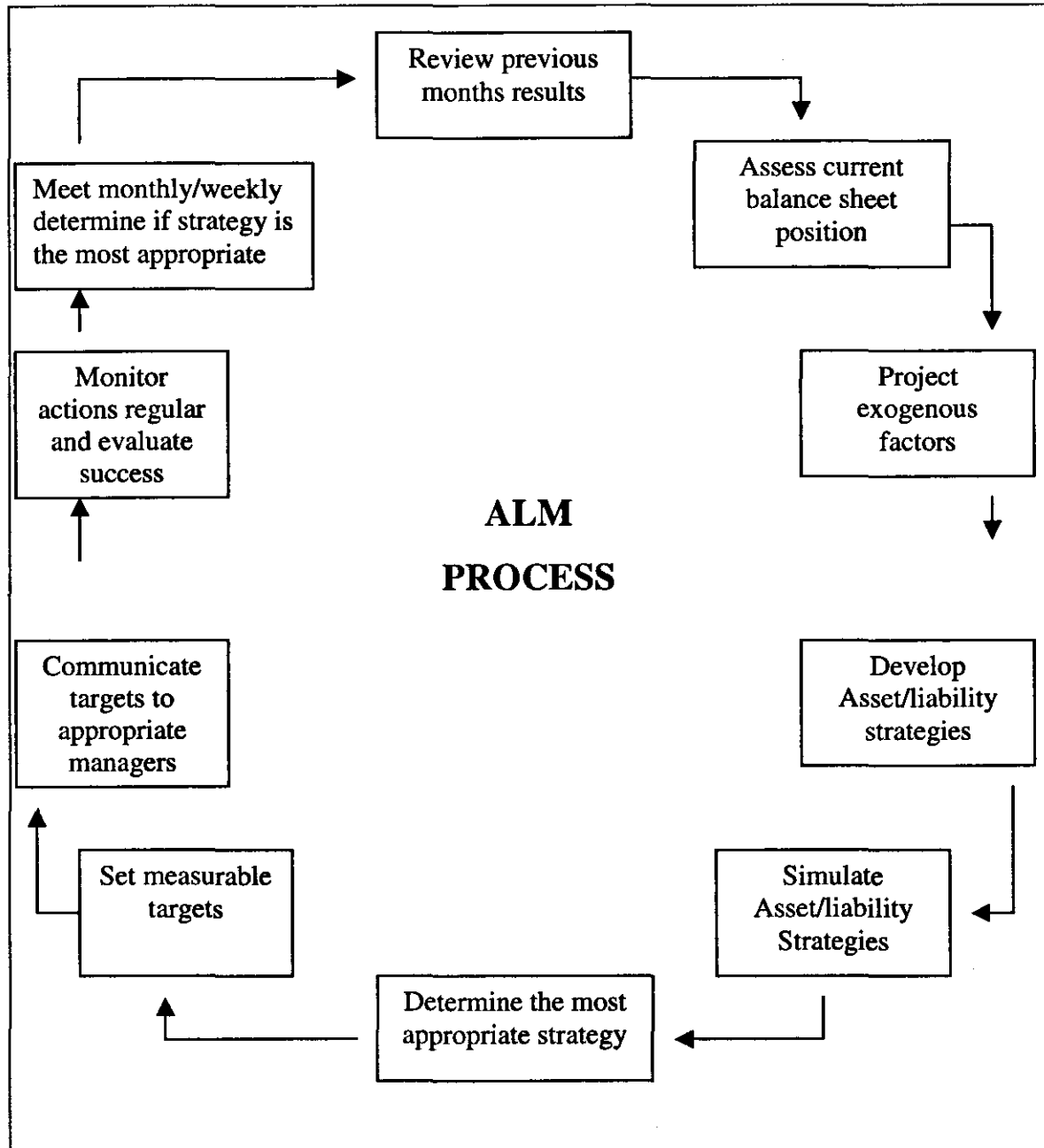
- **Step 1. Review the previous months results:** The variance report forms the basis of this evaluation. The policy document should specify the limits of variance that can be tolerated and procedures to identify the causes of unacceptable variance. It must also specify procedures to correct unacceptable deviations and steps to prevent future occurrences. This policy should be inline with the bank's personnel management policy and procedures regarding the steps to reward performance above the norms and taking steps against risk management.

- **Step 2. Access to current financial statements and risk reports:** The ALCO policy document should specify the different benchmarks that should be used to evaluate the present situation. These benchmarks include the following (Marè: 1995: 3):
 - ⇒ Financial management benchmarks such as ROE and ROA, cost/income ratio, or profit per person, etc.
 - ⇒ Strategic risk benchmarks such as GAP, liquidity, maturity, profit, and credit risk on an aggregate level.
 - ⇒ Tactical risk benchmarks such as value at risk (VaR) and the totals of different hedging portfolios.
 - ⇒ Performance measures such as RAROC and ROC.
 - ⇒ Regulatory requirements and in-bank benchmarks regarding amounts over and above prescribed requirements.

- **Step 3. Project exogenous factors:** This part of the ALM process is an important part of the pre-ALCO meeting functions. The main variables driving the simulation of the different strategies (interest rates and enhance rates) should be forecasted, and decisions about the upper and lower limits as well as the most

likely scenario for these variables should be decided upon before the ALCO meeting. Heated discussions about these inputs are another reason why the ALCO fails – it distracts the ALCO.

Fig. 3.5 The ALM Process



Source: (Marè, 1995: 3)

- **Step 4. Develop an asset and liability strategy:** Step four of the ALM process forms parts of the pre-ALCO meeting; broad strategies in reaction to the forecasts of the external factors should be formulated. The inputs from other departments in this process should be clearly defined. Specific personnel should dedicate their attention to this process and specific delivery dates should be stipulated. This step would include the so called “what if” scenarios.
- **Step 5. Simulating an asset and liability strategy:** The ALCO policy document should also provide guidelines regarding the time frames that should be used for different simulations. Guidelines regarding the different outcomes should also be supplied. A list stating the purpose of the different simulations should also be supplied to ensure that the ALCO meeting is supplied with the relevant information needed to formulate strategies.
- **Step 6. Determine the most appropriate strategy:** The ALCO policy document should specify the different management and risk reports that should be produced, as well as the times when to and to whom they should be made available. Thus, the ALCO members should have the necessary information prior to the ALCO meeting. The policy document should also specify a systematic approach to deal with the issues at hand – one or more problems and opportunities should not overshadow the rest.
- **Step 7. Setting measurable targets:** This step of the ALM process also deals with the accessing of financial statements and risk reports. The policy document should provide clear guidance for the translation of the ALCO decisions into quantifiable actions. The list should form the basis of the communications process and channels from the ALCO to the responsible persons.
- **Step 8. Communicate appropriate targets to managers:** This step forms part of the personnel policy. The ALCO policy document should include a detailed list

of the personnel responsible for the specific tasks. The list should form the basis of the communication process and channels from the ALCO to the responsible persons.

- **Step 9. Monitoring actions and evaluating success:** The terms of reference for the evaluation of personnel achievements as corrective or incentive actions should be clearly specified in the ALCO policy document and should be in accordance with the broad personnel policy. Guidelines on how the variance analysis should be specified as well as the benchmarks used to evaluate the success, the steps to determine the reasons for not achieving the targets and the process for corrective measures that should be taken.

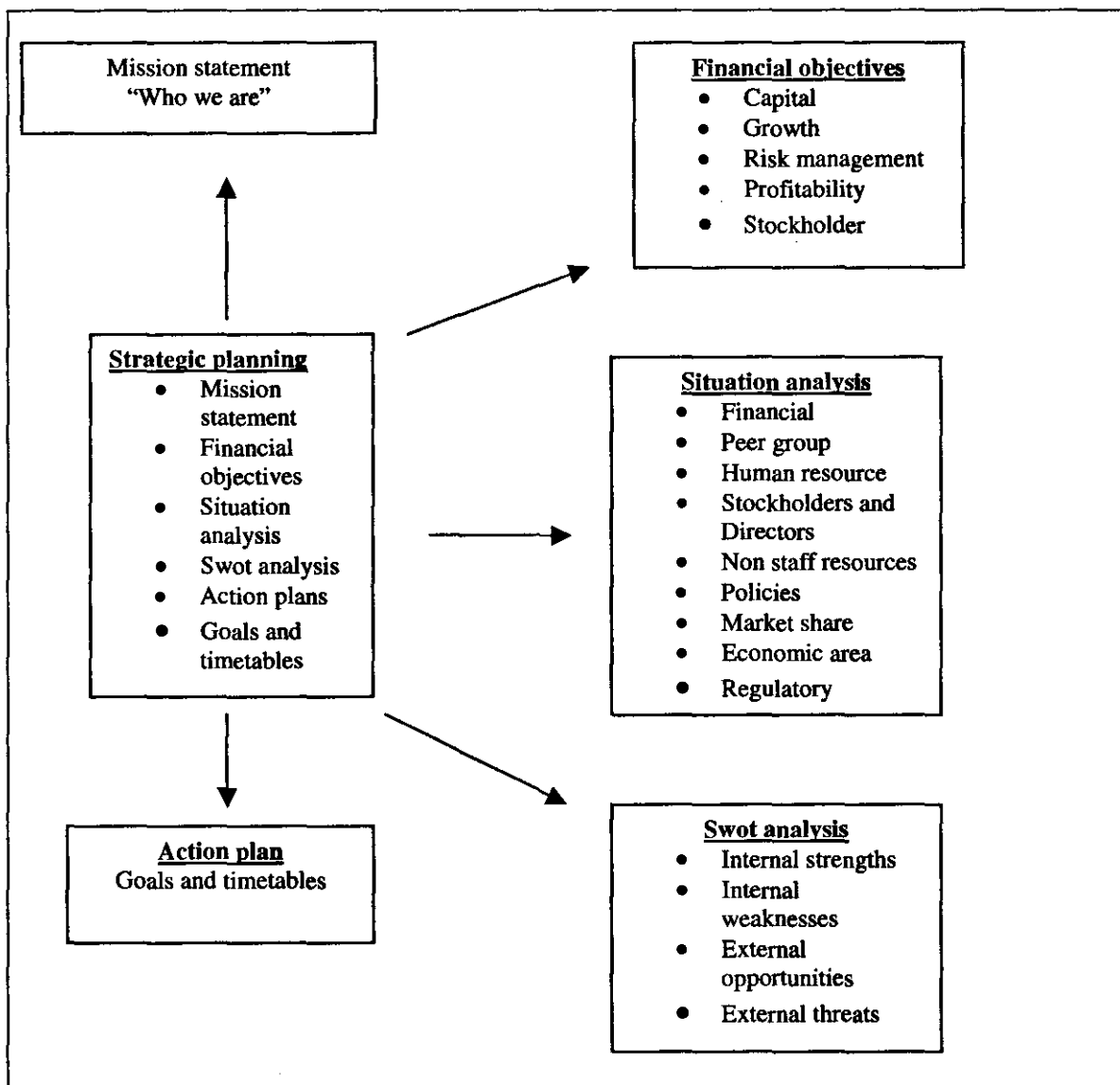
- **Step 10. Determine if the current strategy is appropriate:** The exogenous factors change constantly and the institution has to adjust to these changing environments. It is not only about damage control, but also to ensure that present strategies take the most advantage from opportunities. The policy documents should provide guidelines, procedures and responsible personnel to enable this process to be as effective as possible and to be a core element of strategic management.

As seen in the above sections, the ALM process is a strategic planning and execution process, which enables asset/liability managers to make informed decision regarding the bank's assets and liabilities. In addition to the above-mentioned, the ALCO process can then also be seen as a strategic risk management programme, which can assist risk managers in managing the bank's risks. The above sections have aimed to provide an overview on the ALCO and the ALCO process and what role it plays in ALM and in operational risk management. To better understand the above-mentioned, this study feels that it is necessary to provide an evaluation of a strategic planning process.

3.4.3.2 The strategic planning process

The strategic planning process is the process through which managers formulate the bank's mission, establish goals and objectives, assess strengths and weaknesses of the banks current operating and financial condition, identify opportunities and treats and to design strategies (Kroon, 2000: 38). Figure 3.6 is an illustration of strategic planning process.

Figure 3.6 The strategic planning process



Source: (Koch & McDonald, 2000: 178)

Koch & McDonald (2000: 179) also affirmed that the planning process used by each bank would differ in terms of each institution's structure and size. The basic format is outlined figure 3.6 and include the following (Kroon: 2000: 35):

- Mission statement.
- Financial objectives.
- Situation analysis.
- Analysis of strengths and weaknesses.
- Action plan.
- Goals and time tables.

The first three parts address the bank's current condition. The analysis of strengths and weaknesses, opportunities, and treats (the SWOT analysis) indicates what the bank could be in the future (Koch & McDonald, 2000: 181). It makes managers aware of both the problem areas as well as the strengths. The final two parts require that managers determine what the bank wants to be like in the future and specify how and when to accomplish it. Most strategic plans look forward at least five years, although this can vary. Once a plan is in place, managers can conduct regular audits to monitor performance and to modify the plan if needed, which typically forms part of step ten of the ALM process.

As seen in the above sections, the ALCO and the ALM process are fundamental in the ALM of banks, but also play a big part in operational risk management. The ALCO process is a strategic planning process, which assists managers in their management of assets and liabilities. If this planning process is done thoroughly, managers will also be able to identify potential operational risk events, in this case operational risk events. Not only can managers identify potential risk events by doing a strategic planning process, but it will also ensure that the bank will have a better liquidity position as well as sufficient capital in case of an operational risk loss, because by using simulations managers can predict when there will be an inflow or an outflow of funds. To conclude the discussion on the ALCO, it can be said that the ALCO, who are responsible for ALM

in banks, plays a double role in operational risk management. First, the ALCO can assist in identifying possible operational risks and secondly the ALCO will ensure that the bank has adequate capital.

In the above section, a lot has been mentioned about the simulations that the asset/liability managers use in their planning process. The following section will now provide a more in-depth look at these simulations and simulation models.

3.5 Selecting and implementation of an asset/liability model

Selecting an appropriate asset and liability model is an important part of the ALM process (Cole & Eisenbeis, 1996: 52). The selecting of an appropriate ALM model will not just ensure an effective ALM, but will also be sufficient in effectively identifying potential operational risk events. Since the late 1940's, when the commercial models were first offered, substantial improvements have occurred in the software and hardware products. This simulation process will provide the foundation for the preliminary comparisons of models and enable managers to make better decisions regarding risks. The following factors will provide an insight into the building of a simulation model and the installation of such a model.

3.5.1 Develop a checklist of criteria and prioritise each item

When developing an asset/liability simulation model, it is important to first consider the following criteria (Bitner & Goddard, 1995: 42):

- Information about the company.
- Model hardware requirements.
- Downloading capabilities.
- Input requirements.
- User manual and Help Screens.
- Index/driver rates.

- Ability to account for synthetic instruments (Futures, Swaps, etc.).
- Availability of historical data.
- Reporting and output capabilities.
- Model installation time.
- Vendor support.

The above-mentioned will assist a potential buyer on the decision regarding the buying of an appropriate ALM simulation model and will also provide sufficient information prior to the implementation of such a model. The above-mentioned aspects will also assist managers in the planning phase of the implementation, which will be discussed in the following section.

3.5.2 Planning the implementation

Once an appropriate simulation model is selected, the planning phase of the implementation begins. This phase is critical to the successful start and continuing of the ALM process. The process of installing and loading the data into the model will require ALM managers to spend a considerable amount of time with the vendor's installing personnel (Mihaltian, 1998: 137). The process begins by developing a timeline for each component of the plan and determining the resources required to successfully complete the instalment of the simulation model (Mihaltian, 1998: 138).

The implementation process may be done in six to nine months. In-house support staff will be needed to develop a data gathering procedure and to provide current data for the model. The number of support staff required depends on the size of the institution, the complexity of its general ledger and the flexibility of the loan and deposit reporting systems (Bitner & Goddard, 1995: 43). Also part of the installation process is to determine the vendor's support. The following section will therefore continue the evaluation of the implementation of an asset and liability simulation model by taking a brief look at the vendor's support for such a model, because without sufficient vendor support the institution will be exposed to a high operational risk.

3.5.3 Vendor's support for an asset and liability simulation model

The essence of most simulation models is a defined chart of accounts (Crosse & Hempel, 1999: 19). The initial chart may only remotely resemble the institutions actual chart of accounts, because the interest rate sensitivity of each asset and liability type requires that the variable and fixed components be identified and segregated. This is not an easy task, because the traditional trial balances for loans and deposits are rarely sorted by reprising characteristics (Crosse & Hempel, 1999: 20), and at the end of the implementation, the chart of account must clearly be a correct reflection of the institution's business. For many asset/liability managers maturity data will be the only detailed information that is readily available. It is difficult to identify reprising rates for loans because each loan is unique. Reprising rates use various rate indices, different margins, and multitude of interest rate reset dates. However, for each simulation mode to function properly, it is necessary to separate each loan category into its fixed and variable components (Crosse & Hempel, 1999: 21).

3.5.4 Document preparation and the input process

The development of input documents is the next phase of an ALM simulation model implementation process (Cade, 1997: 122). The structure of the documents provides a framework that will enable the institution to organize its complex data. The previously identified chart of accounts serve as a means by which the data may be input into the model via direct data entry (Cade, 1997: 122). The input documents provide the structure and discipline that assists the support staff in their data gathering, and the institution can provide its own forms; however, most vendors will provide the necessary documents.

3.5.5 Assumptions

Once the data is gathered and the necessary documentation is in place, a determination of growth assumptions for both assets and liabilities must be made (Cade, 1997: 130). Each category identified in the chart of accounts requires a factor of net growth (new business

in excess of principle payments) or net reduction (principle payments in excess of new business). Asset/liability managers must consult with division heads of various lines of business within the organization to obtain their best estimate for growth assumptions for assets and liabilities for which they are responsible (King, 2000: 77). Most growth assumptions will be for a twelve-month period, unless the organization is involved in longer term strategic planning and should also represent the institution's budget. The ALCO uses assumptions to build their simulations, for example, the ALCO assume that interest rates will increase and decide to cut their liabilities. An example of a growth assumption for a loan type is as follows:

Table 3.1 Example of a growth assumption

| | | | |
|-------------------|------------|------------|------------------|
| | | | Growth |
| | Month 1 | Month 12 | \$ % |
| Comm. Real estate | \$20 mill. | \$45 mill. | \$25 mill. X 12% |

Source: (Tlali, 2002: 57)

In this example, month 1 is the current input data, where month 12 is the resultant balance after the growth assumption were added and the principle payment subtracted.

3.5.6 Operating the asset/liability simulation model

To be able to operate an asset/liability simulation model must probably be the most important function of ALM. Each of the members of the ALCO is supposed to have a good understanding on how an asset/liability model work and its components. The processing or operating time is dependant on the complexity of the model, the size of the chart of accounts, the number of the data input entries and the available memory and configuration of the computer (Styger & Bothma, 1998: 13). It is not common to run the model frequently during the first few weeks and months of new installation.

Repeated operation of the model is required to adjust output data delivered as part of the reporting process and to conduct trail runs as part of the initial debugging procedures (Bitner & Goddard, 1995: 50).

If the ALCO and the personnel of ALM do not know how to operate the asset/liability model, ALM will fail and it will be impossible for managers to identify potential operational risks. Much more can be said about the operating of an asset/liability model, but the above-mentioned will be sufficient for the discussion on ALM in operational risk management. The following section will provide an insight into the standards and internal documentation of an asset/liability simulation model and will also conclude the evaluation of an asset/liability simulation model by this study.

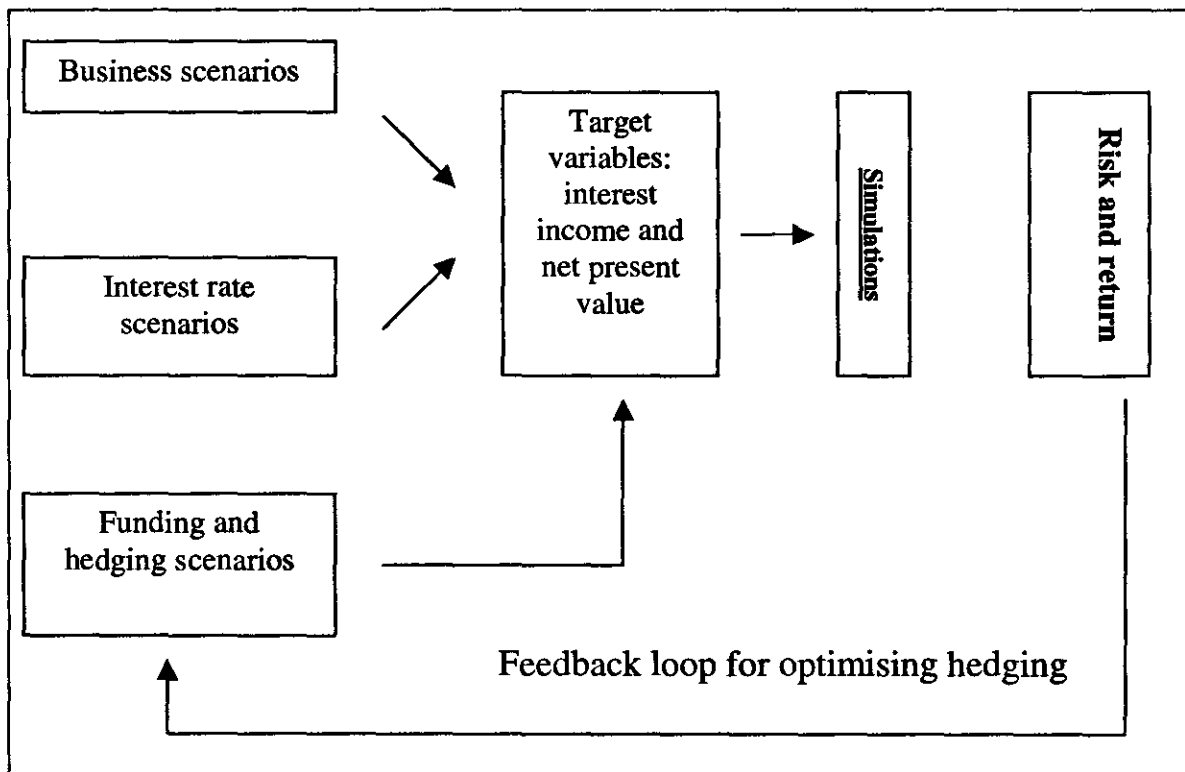
3.5.7 Standards and internal documentation

An important aspect of asset/liability model simulation is the development of internal standards and operating procedures (Tlali, 2002: 60). The need for an institution to identify the critical components of the total asset/liability simulation process and operate the model in a consistent fashion that produces reliable reports is essential (Tlali, 2002: 60). Mihaltian (1998: 122) also stated that the ever-present fact of employee turnover, coupled with continual product development, requires the asset/liability manager to develop and adhere to strict standards and procedures such as the following:

- The standard chart of accounts must be maintained throughout the organization and involve all subsidiary companies.
- The input documents need standardization. Once established, these documents will streamline the entire process of data gathering and model input.
- Assumptions must be tested to be certain they are realistic and parallel actual performance.
- The asset/liability simulation model results should not simply be accepted as fact, but should be challenged. This process will make sure that the asset/liability simulation model reflects the ALCO members' best estimates and assumptions.

Internally documented procedures are critical to the asset/liability modelling process. There is no single critic that appears more frequently in audit reports than the above-mentioned issue. Documentation supplied by the vendor will and should be excellent. Bitner & Goddard (1995: 52) stated that the internal workflow must also be documented. To conclude the discussion on the modelling of an asset/liability simulation model is to say that the market conditions change frequently and it is therefore important to do these above-discussed simulations for specific dates in the future, in order to provide for the frequent changes in the market, which can lead to both market and operational risk.

Fig. 3.7 Overview of the ALM simulation process



Source: (Bessis, 2001: 195)

These asset/liability simulations are also important in the sense that the institution can provide the necessary liquidity and capital when needed, in the sense that these simulations will help the bank to correlate its inflow of funds with its outflow of funds. As Morgan (1994: 23) stated, it is important for the management of liquidity and capital,

that an income simulation must be done over extended periods, at least until most of the books mature. Figure 3.7 is an illustration of an asset/liability simulation process.

There are two significant drawbacks to the simulation methodology, namely, that it requires the projection of market rate developments over extended periods of time and it supports the illusion that gains and losses occur at the same time and that they show up on the accrual accounts (Bessis, 2001: 195). This implies that return is only defined as net interest earnings, thereby ignoring the change in the price component of the return function (Bessis, 2001: 195). Market risk in trading positions is usually measured and managed separately from ALM (Bitner & Goddard, 1995: 53).

The importance of the role played by asset/liability simulation models in the overall success of the bank is being increasingly recognized across the financial sector. This together with the realization that the asset/liability simulation process involves all the activities of the bank, transforming it from its traditional focus on interest rate measurement to the identification and measurement of other risks, for example operational risk. In other words, asset/liability simulation models can facilitate improvements in profitability at reduced risk – in doing so, providing a competitive edge. To conclude the evaluation of the role that asset/liability simulations play in operational risk management is to evaluate it in terms of the risk management process. The risk management process is a strategy that incorporates a mix of risk retention or self-insurance/ self-funding and conventional insurance above certain levels, with significant cost savings (Adelson, 1993: 24). McElravey (2001: 742) identified four basic steps in the risk management process and the importance of asset/liability simulations will be highlighted in each of them in the following sections.

3.5.7.1 Risk identification

Risk identification is the systematic identification of the risk to which an institution is or could be exposed (McElravey, 2001: 742). Asset/liability simulations could assist risk managers in the identification of a potential risk, because one of the major functions of an

asset/liability simulation is to project in- and outflows of funds by taking the risk in consideration.

3.5.7.2 Risk evaluation

Risk evaluation is the weighing-up of the identified risks in numerical terms, in order to gauge the frequency of occurrence and their potential severity to the organization (McElravey, 2001: 742). Managers can use the results of present as well as historical asset/liability simulation models to determine the frequency of risk occurrences.

3.5.7.3 Risk control

As mentioned in a previous section of this chapter, asset/liability simulation models will assist managers in their risk measurement. If, for example an operational risk is more accurately measured, the bank will be able to better control this risk because the bank will be able to make a more sufficient provision (in the form of capital) for the risk, and thus the bank will be better protected against an operational risk.

3.5.7.4 Risk financing

Matten (2000: 7) defined risk financing as the provision of funds to assist an institution to survive and recover from losses that do occur. As mentioned in a previous section of this chapter, asset/liability simulations will assist the bank in correlating its in- and outflows. If in- and-outflows are better correlated, the bank will be able to make more adequate provisions for a risk, because for each inflow there will be an outflow of funds, thus if a risk loss occurs there will be an inflow of funds to be used as risk-loss absorber.

The above-mentioned factors then concludes the discussion on the importance of asset/liability simulations in operational risk management. The aim of this discussion was to emphasize the role that ALM plays in operational risk management in terms of these asset/liability simulations.

3.6 Conclusion

The aim of chapter 3 was to present the theory of strategic asset and liability management (ALM) within the unifying theme of operational risk management. In chapter 3 it was indicated that capital is used to absorb an operational risk loss. The ALCO is responsible for the strategic management of the bank's balance sheet and as capital forms part of the bank's balance sheet, it is also the responsibility of the ALCO to manage the capital that is used as provision for an operational risk. The asset and liability committee (ALCO) is the personnel and senior management that is responsible for the implementation of an effective strategic ALM process in banks and this emphasizes the importance the ALCO plays in operational risk management.

The ALCO does not only manage the capital that is used in operational risk management, but also uses simulations (as discussed in section 3.5) to predict the impact of a potential risk event, including an operational risk event. Thus, the ALCO has a dual purpose in operational risk management. Firstly, the ALCO manages the capital that is used as buffer for an operational risk and secondly it helps to predict a potential operational risk event.

ALM is not the only way for banks to identify operational risks. Risk managers can also use the key indicators of operational risk as a means to identify, monitor, and measure operational risk. Whereas chapters 2 and 3 discussed the importance of the Basel Committee and ALM in operational risk management, chapter 4 will discuss the importance of the above-mentioned key indicators of operational risk in the management of operational risk in South African banks.

Chapter 4

Key Risk Indicators: Cornerstones for Managing Operational Risk

“Information is critical to the evaluation of risk,”

Alan Greenspan (Olsson, 2002: 132)

4.1 Introduction

Indicators are everywhere. People rely on them to monitor economic and investment performance, education results, productivity gains, economic health, even the education performance of students (Hoffman, 2002: 239). Therefore, it should be no surprise that operational risk managers have begun to use risk and performance indicators as an **early warning system** to track an institution’s level of operational risk and create a multi-dimensional risk profile. Some risk managers see risk indicators as the cornerstones of both effective measurement and management of operational risk. Herkes *et al* (2003: 4) stated that in the measurement sense, analysts use indicators as a key variable in formulae to forecast operational loss potential. Herkes *et al* (2003: 4) also stated that in the management sense, line managers are often anxious to track multiple performance indicators as a means to confirm that their products and services are performing consistently with goals and objectives.

Where and how does an institution begin a process of operational risk tracking and measurement? What is an operational risk profile and how does an institution manage it? How should a measurement methodology link to existing control functions or to line managers’ own performance indicators? Which indicators are most useful? That is, when

is it appropriate to use key performance indicators (KPIs) or when is it appropriate to use key risk indicators (KRIs)? Olsson (2002: 67) stated that all of these questions are being discussed actively in operational risk management circles. In fact, Olsson (2002: 67) affirmed that they are indicative of the various perspectives and approaches to operational risk management. The aim of chapter 4 is therefore to provide some answers to those questions, along with insight on how and where operational risk indicators are already being used in the banking industry.

4.2 Key risk indicators (KRIs) vs. key performance indicators (KPIs)

Before chapter 4 can proceed to explore and evaluate operational risk indicators in detail, however, it is important to distinguish between a key risk indicator (KRI) and a key performance (KPI) indicator. The following section will provide a short overview of a KPI in order to distinguish it from a KRI.

4.2.1 Key performance indicators (KPIs)

Key performance indicators (KPI) are high-level snapshots of a business or institution based on specific predefined measures (Herkes *et al*, 2003: 5). KPIs typically consist of any combination of reports, spreadsheets, or charts and they may include global or regional sales figures and trends over time, personnel statistics and trends, real-time supply chain information, or any thing else that is deemed critical to an institution's success (Herkes *et al*, 2003: 5). As Lopez (2002: 3) stated, a KPI application such as an executive portal can give a business executive a high-level, real-time view of the health of the institution by visually displaying vital statistical information about the institution.

In developing KPIs, a user or developer defines target performance levels, which is an essential element of the strategic planning process (see 3.4.2.3) and then decides the best way to present variance from the target (Lopez, 2002: 3). For example, a bar chart of Sales KPIs may flag regions that are under quota in red while those that are at or over quota are green. This allows the end user to see a company's strengths and possible areas

for improvement at a glance. Typical KPIs that are used in financial institutions include the following (Thirwell, 2002: 4):

- Statutory KPIs, such as GAAP or Legal Regulatory requirements.
- Profitability per business unit/customer/product.
- Exception reporting.
- Employee performance, such as asset under management or profit per customer.
- Competitiveness, such as market share.
- Cost management, such as ROA on IT or new delivering channel monitoring.
- Credit management, such as time to settlement or credit exposure.

As can be seen from the above, there are large amounts of KPIs that provide different measures of performance for an institution. Therefore, for the purpose of operational risk management, the following sections will only evaluate KPIs in a risk-return framework with specific focus on return on equity (ROE).

4.2.2 Key performance indicators (KPIs): Defined in a risk-return framework

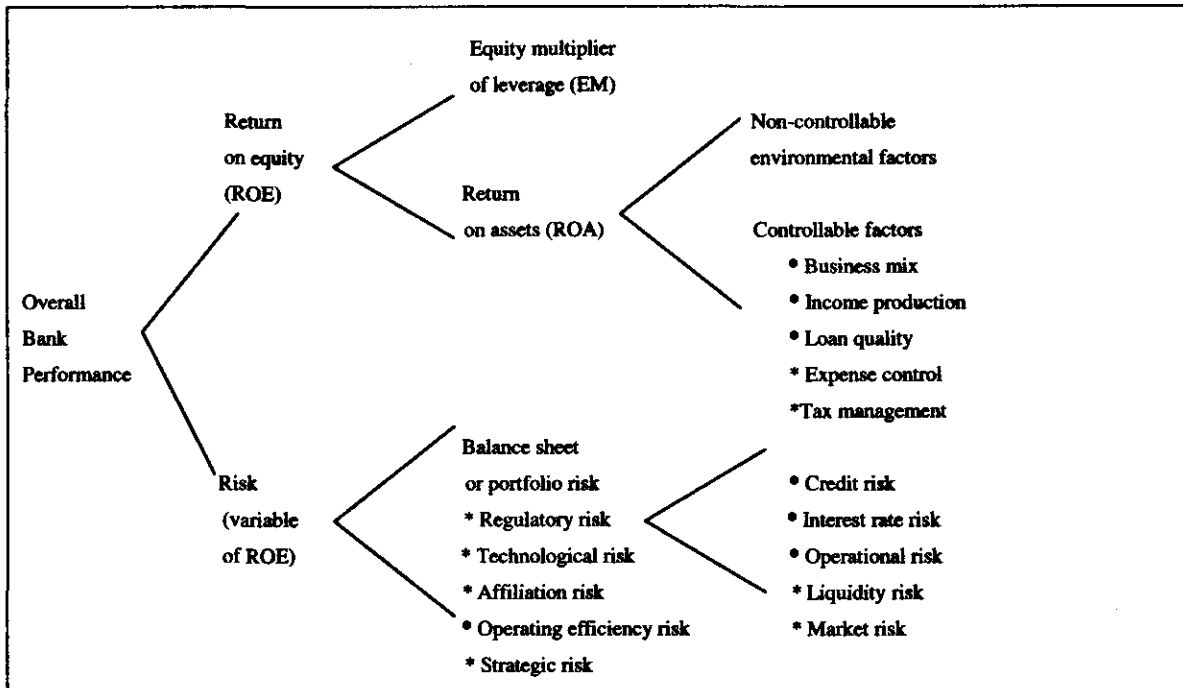
Sinkey (2001: 130) affirmed that the most eminent KPI in the risk-return framework of a bank is return on equity (ROE). As Koch and McDonald (2000: 213) mentioned, the decomposition of the ROE provides an insight regarding banking risks and returns. On the return side, ROE splits into return on assets (ROA) and the equity multiplier (EM). ROA is determined by controllable and non-controllable factors, for example the supply and demand conditions banks face and their geographic and product markets can be considered as non-controllable elements/factors. Controllable elements/factors include business mix, income production, loan quality, expense control, and tax management (Koch & McDonald, 2000: 214).

The risk component of figure 4.1 highlights the five generic risks banks face (as seen these risks are the same risks that are mentioned in figure 3.3 and also includes credit

risk, market risk, operational risk, interest rate risk, and liquidity risk, and are also provided in terms of on- and off-balance sheet activities):

- Portfolio or balance sheet risk, including the risk of off-balance sheet activities (OBSAs).
- Regulatory risk.
- Technological risk.
- Operating efficiency risk.
- Strategic risk.

Figure 4.1 A risk-return view of the overall bank performance



Source: (Sinkey, 2001: 130)

Portfolio and operational risk have the most direct effect on the short-term variability of earnings (Sinkey, 2001: 130). The key portfolio risks of banking are credit risk, interest rate risk, liquidity risk, prepayment risk, and foreign exchange risk. As Koch and McDonald (2000: 214) mentioned, these risks should determine how much capital a bank

should have on hand. In addition, the amount of capital a bank holds should depend on whether it uses OBSAs to speculate rather than to hedge. Because of the numerous risks banks face, it is convenient to have a comprehensive method to measure the exposure to these risks. The regulatory approach is to use risk-based capital requirements and CAMEL ratings, where (Sinkey, 2001: 131):

- C = capital adequacy.
- A = asset quality.
- M = management.
- E = earnings.
- L = liquidity.

The CAMEL framework has been expanded to cover systemic risk¹ with an S added to give CAMELS. Hiwatashi (2002: 4) stated that in finance, variability of earnings is a preferred measure of risk (e.g., the standard deviation of earnings per share). The following section will propose the variability of ROA, as captured by its **standard deviation**, s_{ROA} or simply S , as a comprehensive measure of a bank's risk exposure for as Herkes et al (2003: 5) puts it, the coefficient of variation (CV) of ROA, the ratio of s_{ROA} to average ROA, provides a relative measure of risk exposure. The following section will further the evaluation of a bank's KPIs by taking a more in-deep look at the most eminent KPIs in a risk-return framework.

4.2.2.1 Return on equity (ROE)

ROE is a KPI that measures profitability from the shareholder perspective (Sinkey, 2001: 131). Accounting ROE, however, should not be confused with investment profitability (or return) as measured by dividends and stock price appreciation. Accounting ROE measures bank accounting profits per rand of book equity capital (Sinkey, 2001: 131). It is generally defined by average equity or by the period-ending figure and can be

¹ Systemic risks refers to the risk or probability of breakdowns in an entire system, as exposed to breakdowns in individual parts or components, and is evidenced by co-movements (correlation) among or all the parts (Kaufman & Scott, 2003: 1).

decomposed into a leverage factor, the equity multiplier, or (EM) and return on assets (ROA), which is expressed as:

$$\text{ROE} = \text{ROA} \times \text{EM}$$

The following sections will evaluate the components of the above-stated formula in more detail.

4.2.2.1.1 Return on assets (ROA)

Return on assets (ROA) is a KPI that can be defined as net income divided by average or total assets and measures bank profits per rand of assets (Rose, 1999: 158).

4.2.2.1.2 Equity multiplier (EM)

The equity multiplier is the KPI that is the average assets divided by average equity or total assets divided by total equity – the reciprocal of the capital-to-asset ratio (Rose, 1999: 158). It provides a gauge of a bank's leverage or the rand amount of asset pyramid on the bank's base of equity capital (A/E). Sinkey (2001: 131) also stated that the equity multiplier provides the leverage that makes ROE a multiple of ROA. For example, a bank with an ROA of one percent and an equity multiplier of 10 generates an ROE of 10 percent. The EM of 10 implies an equity-to-asset-ratio of 1/10 or 10 percent, or debt to asset ratio of 90 percent. Although banks financed with either all equity or all debt does not exist in the real world, these two notions are useful for illustrating how leverage affects ROE.

First consider an all-equity bank. Its EM = 1 because assets are financed totally by equity. With EM = 1, ROE = ROA. If an all equity bank had an ROA of one percent, its ROE would be one percent. Second, consider an all-debt bank. Its EM would be undefined because division by zero is impossible, theoretically infinite leverage. As a compromise considerer a bank with a ratio of equity to assets of 4 percent. Its EM would be $0.01 \times 25 = 0.25$ or 25 percent. Therefore, from the above example it can then be seen that the EM of an all-equity bank would differ from an all-debt bank.

4.2.2.1.3 Stage two: Profit margin and asset utilization

The second stage of ROE decomposition analysis (referred to in corporate finance and accounting as *du Pont analysis*) splits ROA into two components (Koch & McDonald 2000: 215):

- Profit margin.
- Asset utilization.

As mentioned it can then be seen in the following formula:

$$\text{ROA} = \text{PM} \times \text{AU}$$

PM equals net income divided by total revenue², and AU equals total revenue divided by total average assets (Rose, 1999: 159). Rose (1999: 159) stated that by dividing ROA into these two components, it can pinpoint the variables that underlie the ROA performance. The profit margin reflects profits per rand of total revenue (sales) while asset utilization expresses total revenue (sales) per rand of assets. A bank with a 10 percent profit margin and a 10 percent asset utilization has an ROA of 1 percent. The variables and components of a ROE model are summarized in table 4.1. The ROE model contains three alternative measures of profitability (Sinkey, 2001: 131):

- Return on equity.
- Return on assets.
- Profit margins.

Because the ratios ROE, ROA and PM all have the same numerator (net income), the different denominators (i.e., average or total equity capital, average or total assets, and or total revenue) simply provide alternative perspectives on the measurement of profitability. Accounting ROE measures profitability from the owner's perspective. Its

primary shortcoming as a KPI is that ROE can be high because a bank has inadequate equity capital (Sinkey, 2001: 132). Sinkey (2001: 132) also stated that in addition to the above-mentioned; a bank with a negative book equity (book insolvency) and positive profits would show a positive return on equity. By splitting ROE into ROA and EM, this dilemma is resolved. Thus, ROA is the preferred accounting measure of overall bank risk-return performance. It measures how profitable all of the banks on balance sheet assets are employed. By splitting ROA into PM and AU, it focus on the third measure of profitability, PM, and an asset utilization, AU, or “total asset turnover.”

Table 4.1 The return on equity (ROE) model

| | | | | |
|---|---|---|---|---|
| Return on Equity = Return on Assets X Equity Multiplier | | | | |
| = ROA X EM | | | | |
| = Profit Margin X Asset Utilization X Equity Multiplier | | | | |
| = PM X AU X EM | | | | |
| $\frac{\text{Net Income}}{\text{Average Equity}}$ | = | $\frac{\text{Net Income}}{\text{Operating Income}}$ | X | $\frac{\text{Operating Income}}{\text{Average Assets}} + \frac{\text{Average Assets}}{\text{Average Equity}}$ |
| | = | $\frac{\text{Net Income}}{\text{Average Assets}}$ | X | $\frac{\text{Average Assets}}{\text{Average Equity}}$ |
| | = | $\frac{\text{Net Income}}{\text{Average Assets}}$ | | |

Source: (Compiled by the author)

Banks do not generate sales volumes greater than their total assets as do most nonfinancial institutions; therefore AU better describes the ROA ratio for a bank than asset turnover does. Given a bank’s ability to generate revenue (sales) as measured by AU, the profit margin component of the ROE model focuses on a bank’s ability to control expenses. Thus, to conclude the above section, it can be said that in a risk-return

² Total revenue equals interest revenue plus noninterest revenue.

framework of a bank, ROE can be regarded as the most eminent KPI; however, ROE is not the only KPI that is important in the evaluation of a bank's performance. The following are some examples of other KPIs that play a big part in evaluating a bank's performance (Koch & McDonald: 2000: 175-180):

- **Return to Stockholders**, which measure how well the investment in bank stock did over time.
- **Earnings per share (EPS)**, which measure the earnings per share for stockholders.
- **Market Value of Equity**, which measure what the market value of the institution's equity is at a specific time/date.
- **RAROC**, which measure the risk-adjusted return on capital.
- **RORAC**, which measure the return on risk-adjusted capital.

As mentioned, the above KPIs also play a large part in evaluating a bank's performance but will not be evaluated in detail by this study, and are only mentioned as additional KPIs to ROE and ROA.

4.2.2.2 Conclusion

In the sections, a KPI is identified as an indicator that shows the bank's overall performance at a specific time. Specific focus had been given to the ROE, ROA and EM as important KPIs in a bank and an in-deep evaluation of each has been done to assists in the distinction of a KPI from a KRI. The following section will then define a KRI in the banking sector as part of the overall objective of chapter 4.

4.2.3 Key risk indicators (KRIs) defined

Before this chapter can begin to explore KRIs in greater detail, however, it is important to place proper emphasis on the phrase "early warning systems.". As Hoffman (2002: 240) mentioned, the key challenge in dealing with risk indicators is to identify or construct

metrics that serve as predictors or “drivers” of operational risk. Unfortunately, most operational risk indicators are trailing in nature to other risk indicators, for example credit risk indicators, because not enough attention has yet been given to the development of effective operational risk indicators (Theodore, 2002:5). That is to say, operational risk indicators do a far better job of confirming recent history than they do in predicting the formation of operational risk storm clouds on the horizon. Beyond simply identifying indicators of risk, therefore, the risk manager must work hard to distil those that will prove the most useful for managing the institution’s future risk and potential, not simply measuring its recent loss potential (Hoffman, 2002: 240). Perhaps the most important of all, operational risk indicators must be prospective to be useful (Theodore, 2002: 5). Theodore (2002: 6) also mentioned that there is a lagged relationship between an indicator and the message it is sending. Take the example of an institution that is experiencing management change. During all management changes, uncertainty abounds. Employees and managers alike are left to wonder, “How will the changes affect me?” Some might stay at the institution; others are likely to leave, accepting the first attractive offer that comes along (Hoffman, 2002: 241). The difficulty with operational risk indicators, however, is that they may not identify this activity quickly enough to alert others that these departures are taking place and are presenting new risks to the institution (Hoffman, 2002: 241).

In fact, some institutions have used the turnover indicator³ quite diligently, only to find that it was not flashing a warning signal at all (Hiwatashi, 2002: 7). Hiwatashi (2002: 7) also mentioned that it was, in fact, only showing that the turnover did not look too bad. The problem with this kind of usage is that in most cases there will be a delay when the turnover indicator actually shows up in the numbers (Hiwatashi, 2002: 8). Hoffman (2002: 241) mentioned that this is precisely where there must be a predicative aspect to the indicators. For instance, banks can assume that turnover will take place. The question is how much? The challenge, then, would be to trend forward the turnover values under optimistic, expected, and worst case scenarios, considering a range of possible scenarios and associated losses.

³ More on the turnover indicator will be mentioned in a latter section of chapter 4.

Where as the above section was intended to define a KRI in the banking sector, the following section will provide a more in-deep look at KRIs by evaluating the basic classifications of KRIs.

4.2.3.1 The basics of key risk indicators (KRIs)

When using the term risk indicator, there are broadly referred to captured information that provides useful views of underlying risk profiles at various levels within an institution (Hoffman, 2002: 242). These indicators seek to quantify all aspects (both tangible and intangible) that are sought by a risk manager to enable risk-based decision-making. KRIs may be classified in a number of ways. Hoffman (2002: 242) and Hiwatashi (2002: 7-8) stated three classifications of KRIs, which include:

- Risk Indicator by type.
- Risk Indicator by risk class.
- Firm wide vs. Business-specific.

Each of the above-mentioned will then be discussed in the following sections.

4.2.3.1.1 Risk indicator by type

There are at least four types of KRIs, which include (Theodore, 2002: 10):

- Inherent risk indicators.
- Control risk indicators.
- Composite indicators.
- Model risk factors.

This study will illustrate these distinctive measure types using two general classes of risk: technology-related risks and people risks (see 2.2.1.1), such as misdeeds, mistakes, and other related actions or inactions.

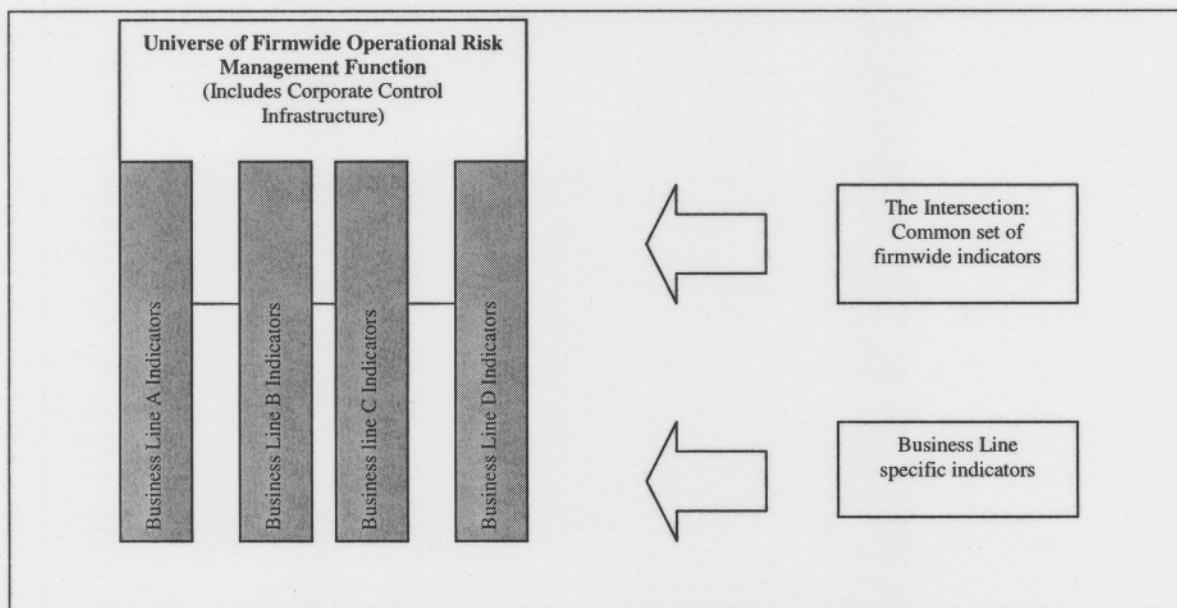
4.2.3.1.2 Risk indicators by risk class

This is the second classification of a KRI and includes a mapping of the KRI into risk classes (Theodore, 2002: 10). For consistence in the study this chapter will use people, relationships, technology/processing, physical assets, and other external risk classes. Each area implies its own set of KRIs as drivers or predictors of operational risk and loss.

4.2.3.1.3 Business-specific vs. firm wide KRIs

The third classification of a KRI categorizes KRIs by the breadth of their application across the entire institution (Theodore, 2002: 11). Business-specific KRIs are units that define an individual business type, for example trading business at a minimum would track transactions, settlements, and failed trades, whereas retail banking businesses would track numbers of customer accounts, complaints, teller shortages, etc., (Theodore, 2002: 11).

Figure 4.2 Key risk indicators: Firm wide vs. business-Specific



Source: (Hoffman, 2002: 242)

Conversely, there are also firm wide KRIs. Figure 4.2 sets the stage for the overall discussion on firm wide and business specific risk indicators throughout this chapter. Firm wide KRIs include training dollars spent, employee error rates, and customer complaints as illustrated in subsequent figures (McPail, 2003: 16). Business line-specific measures will include unique variables by business (McPail, 2003: 16).

The above section then concluded the discussion on the three different classifications of KRIs and the following section will take a more in-depth look at the different types of KRIs as mentioned in section 4.2.3.1.1.

4.3 Key risk indicators (KRIs) by type

As mentioned above, the following section will provide a more in-deep look at the different types of KRIs and will also provide some examples where possible.

4.3.1 Inherent or exposure indicators

At the most basic level, the monitoring of data that are descriptive about the business is useful to provide a context, and as a means of dimensioning exposure. Thus, these inherent risk or exposure indicators provide a dimension for inherent risk exposure (Hoffman, 2002: 242). The data that support the measurement of these variables are relatively accessible across the institution, and generally inexpensive to collect (Hoffman, 2002: 242). Much of these data may already be tracked by various reporting functions within the institution and, in addition, some operational risk managers maintain this information, and apply it to risk financing and/or insurance purchasing decisions, or in satisfying requests from insurance underwriters (McPail, 2003: 17). Examples that have emerged in regulatory decisions include number of transactions, volumes of trades, value of assets in custody and value of transactions.

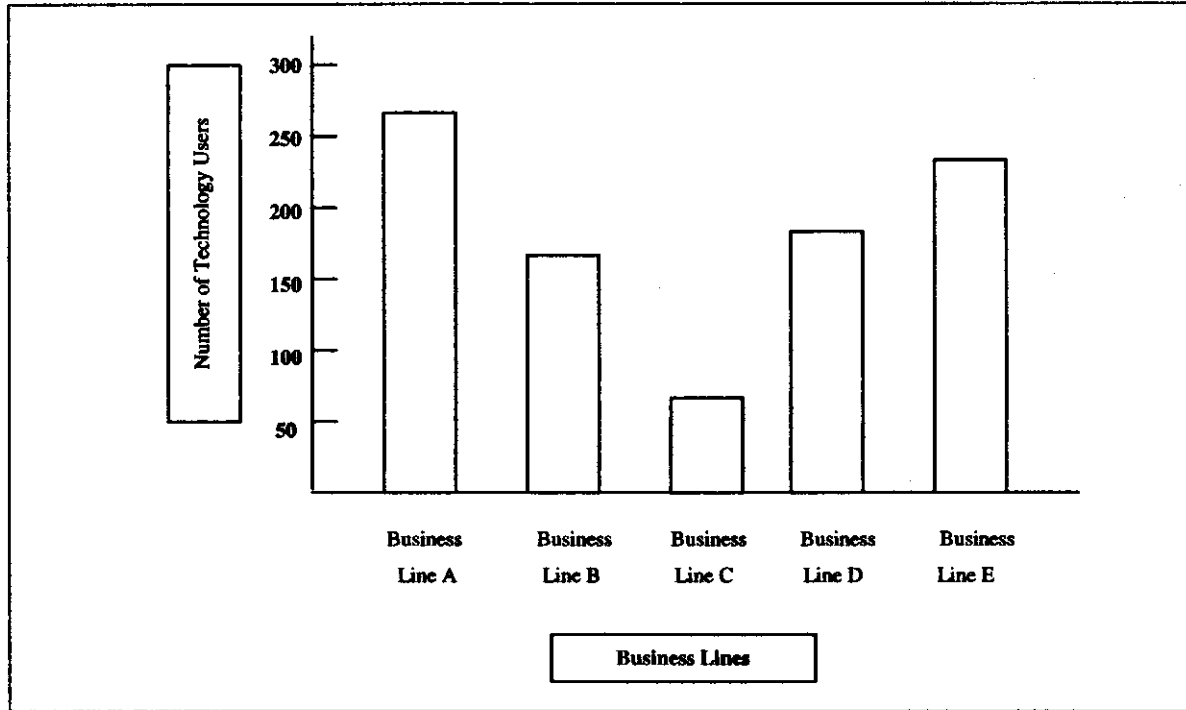
4.3.2 Individual management control risk indicators

As a second type, some institutions capture certain types of variables that are generally believed by business managers to be appropriate indicators of risk, but are not simply descriptive (Hoffman, 2002: 243). Hoffman (2002: 243) argues that instead they are representative of management's actions or inactions. These risk indicators may also already be tracked in some form by a given institution, for example some prudent managers may already monitor such indicators systematically for some classes of risks in the form of KPIs (see section 4.2.1). Existing processes may need to be modified, however, in order to collect data that represent the entire institution, and all classes of risks (Theodore, 2002: 13).

Take the example of a business unit or institution that decides to embarked on a mission of streamlining its operations by moving more management information system (MIS) data for key areas onto the Web for access over the Internet or its own intranet, as the case may be. Business functions affected may include purchasing, human resources, trading and settlement, and client services.

Total technology users requiring training is presented in figure 4.3 as a firm wide risk indicator. The strength of firm wide risk indicators lies within their comparability across the institution (Theodore, 2002: 14). Theodore (2002: 14) however, argues that users should realize that the benefit they gain in comparability and transparency across the institution may be partially offset by the generic (nonbusiness-specific) nature of these measures. In this example, inherent risk indicators (see 4.3.1), such as numbers of servers, number of technology applications, and number of business continuity plans required, provide dimensions to the technology risk profile across the institution. Similarly average transactions value, transaction volume, number of employees, and overtime serve to provide dimension to people and employee risks (Hoffman, 2002: 244).

Figure 4.3 Risk indicators: User number requiring training

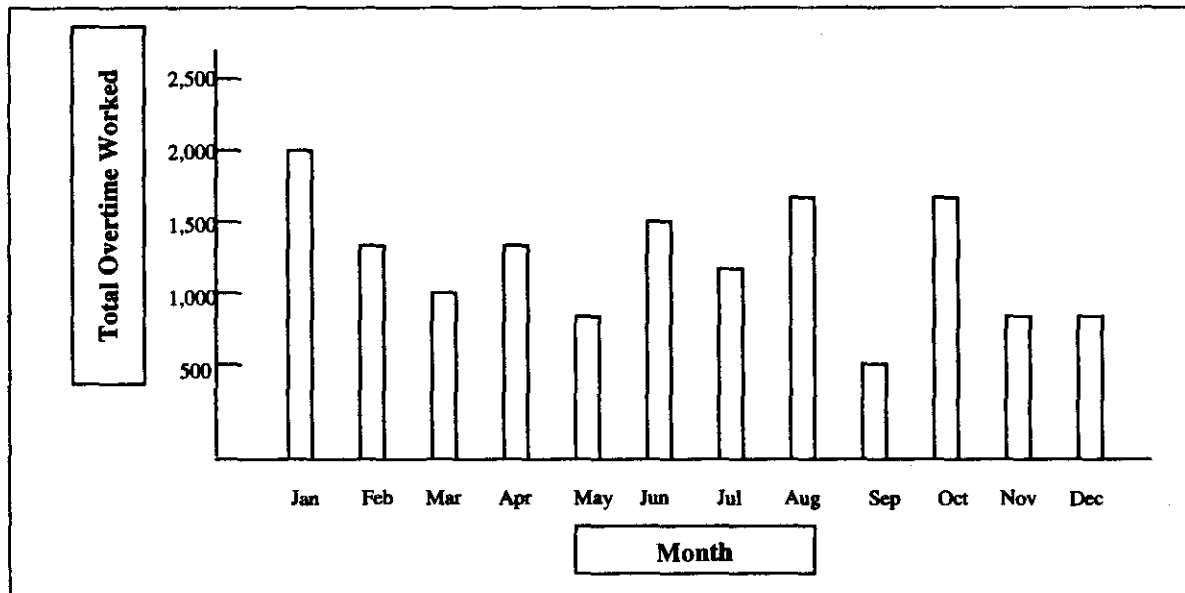


Source: (Hoffman, 2002: 244)

Technology management control risk indicators may specifically include the number of users requiring training in the new technology and will be represented as actual numbers or be weighted to reflect total employees in the department (Hoffman, 2002: 244). On the other hand, employee risk indicators may include the amount spent on training and employee appraisal completion rates (see figure 4.3). The following is an example of business-specific risk indicators in a financial institution.

As the introduction of new technology almost always requires training to maintain productivity levels, this can be an important measure to assess risk. These risk indicators may be captured in terms of any meaningful unit, for example hours, dollars (rand), or employee numbers (Theodore, 2002: 19). Theodore (2002: 19) also stated that it is critical that operational risk MIS is flexible and sophisticated enough to be able to accept data in any unit(s) entered.

Figure 4.4 Business-specific indicators: Overtime worked



Source: (Hoffman, 2002: 245)

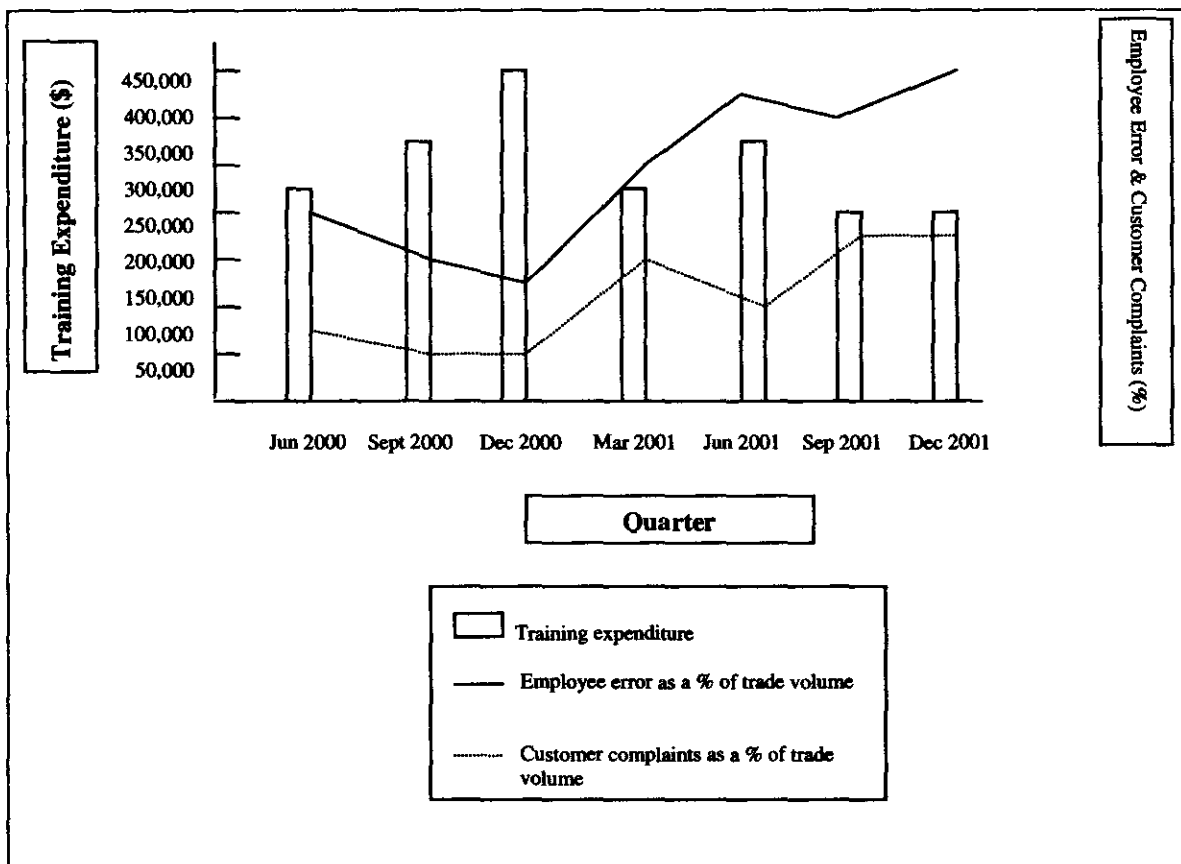
As seen in figure 4.4, this is the total overtime hours worked as a business-specific risk indicator. The analysis of business-specific indicators in isolation may prove to be only marginally beneficial (Hoffman, 2002: 245). Hoffman (2002: 245) mentioned that its intrinsic benefit might be realized when used as a variable within a group of relevant indicators (i.e., a composite).

4.3.3 Composite risk indicators

Calomaris and Herring (2002: 2-4) stated this type of risk indicators as the third and a more complex type of risk indicator. These combinations of risk indicators provide an opportunity to measure multiple dimensions of risk associated with a specific class of risk, behaviour, or business activity (Calomaris & Herring, 2002: 5). Tracking inherent risk variables (see 4.3.1) and control-oriented risk indicators together as composites, over time, can tell some very interesting stories. Figure 4.5, is an illustration of composite risk indicators.

As shown in figure 4.5, there appears to be a strong correlation between declining investment in employee training and the error rates of these employees, and the rate of customer complaints. This type of risk indicator may be considered compelling reading by management and other interested control functions. In the above case, they can show the user what is his or her optimal employee/training/performance levels is and whether performance is getting better or worse.

Figure 4.5 Composite risk indicators: Training dollars vs. employee error rate vs. customer complaints.



Source: (Hoffman, 2002: 246)

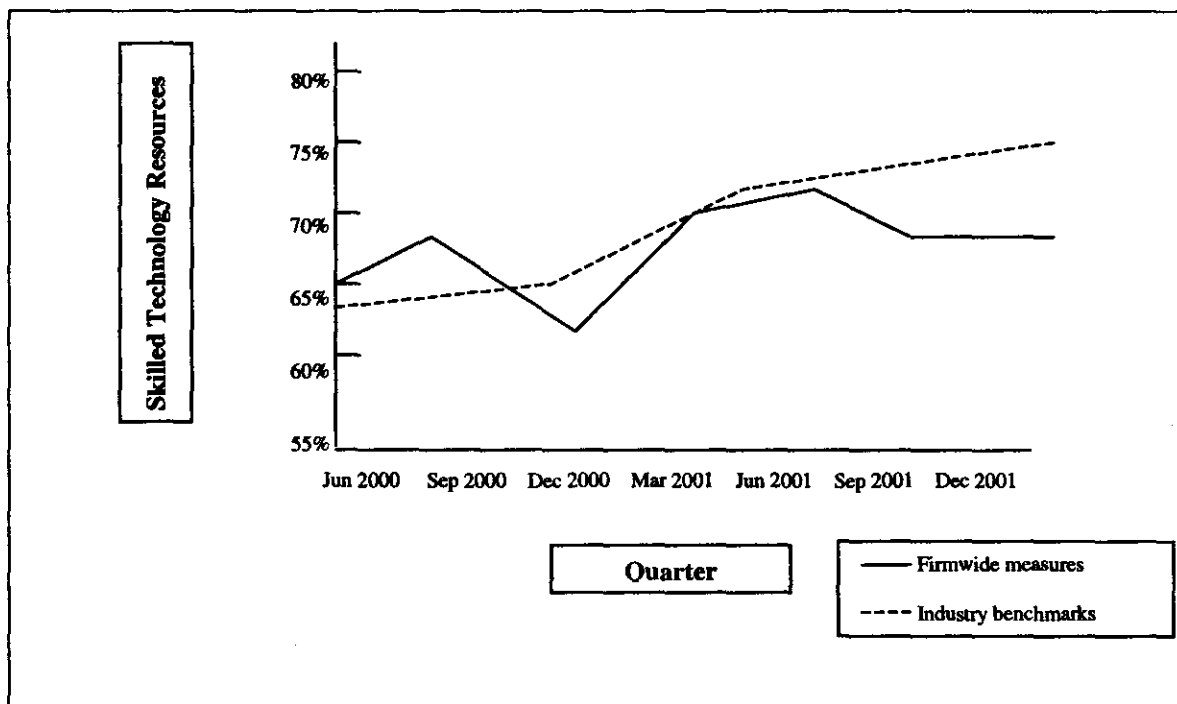
Inherent and control indicators can be combined in the context of this chapter's example of a business harnessing the power of Internet-based technologies. Thus, a composite risk indicator may track the percentage of skilled technology resources required to

support this transaction (Hoffman, 2002: 245). The percentage could then be calculated as follows (Hoffman, 2002: 245):

$$\frac{\text{Number of skilled technology resources, say 14}}{\text{Total number of technology resources, say 20}} = 70\%$$

It would also be invaluable if there were industry-benchmarking data on this risk indicator readily available to understand exactly where the institution or business unit stands relative to other industry members (see figure 4.6). In effect, a rating of seven out of ten may be more easily digested if the industry average was 7.6, for example (Theodore, 2002: 19) and (Hoffman, 2002: 246). Such an industry benchmark may point to a shortage of skilled labour within the market and would therefore provide a perspective for any intended controls. The use of industry statistics adds perspective to the rating (Hoffman, 2002: 246).

Figure 4.6 Composite risk indicators: Number of skilled technology resources vs. industry benchmark



Source: (Hoffman, 2002: 247)

The comparisons of risk indicators to industry benchmarks add additional perspective to the rating. Figure 4.6 shows that the firm wide indicator of skilled technology resources has slipped considerably below the industry benchmark and inference may be drawn from this in relation to the institution's vulnerability to technical problems. Theodore (2002: 19) mentioned that taking the concept of composite risk indicators further, risk managers can combine numerous inherent and/or control indicators to create operational risk indices, such as a new application risk index or an overall technology risk index. A further evaluation of these composite risk indicators will be done in a later section of chapter 4 and will also be included in the case study of chapter 5.

4.3.4 Operational risk model factors

Operational risk model factors are the fourth type of KRI and are essentially a subset of the previous three types of indicators (see 4.3.1 – 4.3.3) (Lopez, 2002: 4 & 16). This category implies that risk managers would not want to use all these data measures in an operational risk measurement model (Hoffman, 2002: 247). For simplicity risk managers will select certain risk drivers from those categories in order to apply the most effective ones for modelling purposes (Lopez, 2002: 17). Factor models will be derived from various underlining risk indicators that characterize a risk profile (Lopez, 2002: 17). Like composite risk indicators, operational risk model factors will also be further evaluated in a later section of chapter 4 and the case study of chapter 5. The above section then concludes the discussion on the different types of risk indicators. The following section will precede the evaluation of KRIs of operational risk by evaluating its institutional considerations.

4.3.5 Institutional considerations

Lopez (2002: 18) stated that due to their inherent flexibility, risk indicators may be captured at various levels throughout the institution. For instance, at one level risk indicators may be specifically defined and captured through different dimension across the entire institution (Lopez, 2002: 18). Alternatively, risk indicators may be engineered

to cater specifically for risks associated with the very nature of certain business-line functions, productions, personnel, and other operational environmental factors (Lopez, 2002: 19).

Thus, risk managers often think of risk indicators as either firm wide or business-specific in nature (see 4.3.2). That is in order to say that to establish a relative comparison from one business line to the next, risk managers will identify risk indicators that can be applied to any type of business line (Hoffman, 2002: 247). These are referred to as firm wide risk indicators, and as mentioned earlier, will include generic variables such as numbers of people, systems and customers (Theodore, 2002: 22). While these variables help to relate one business to the next, by making them comparable, they may become a bit generic for the individual line manager. Hoffman (2002: 249) stated that by soliciting management input into the definition of risk indicators at various levels, however, and committing management to their systematic measurement, the risk manager increases the potential for buy in and credibility to the process. In the end, the trick is to find an intersection between firm wide and business line risk indicators. (An illustration of such an intersection can be seen in figure 4.2 and 4.9).

Lopez (2002: 17) mentioned that the more successful risk indicator programs benefit from the involvement and input of several management levels and consist of a flexibility that allow for different perspectives. During the course of fin-tuning an operational risk management programme, and while seeking measures appropriate to Investment Management operations, risk managers targeted some front-line managers for response (Lopez, 2002: 19). These managers focused more on risk indicators for risks at the operations level, as have been predicted, and therefore closely resembled existing performance measures. However, when senior management, and ultimately the CEO, of the institution were interviewed, their focus was found to be more on composite indicators, such as combined key people risks within the asset management team (see chapter 3), and on drivers for relationship risks.

The above then concluded the evaluation of KRIs in terms of its institutional considerations. The following section will provide some more practical considerations regarding the definition, data collection, standards and emphasis of KRIs.

4.3.6 Practical considerations regarding definition, data collection, standards, and emphasis of KRIs

Hoffman (2002: 249) stated that the most effective operational risk management programmes will blend business line and corporate initiatives. Clearly, working closely with management from all levels within the institution is essential for the long-term commitment and credibility of the risk measurement process. Risk indicator definitions will consider the rationale for the risk indicator, description of rating or measurement criteria, and the sources of data (Herkes *et al*, 2003: 2). Once defined, procedures must be implemented to ensure the systematic collection of accurate and timely data to monitor and analyse risk indicators.

Each risk indicator may also be weighted in accordance with its significance, or predictive capabilities, to ensure accuracy and relevance throughout the various levels of the institution (Herkes *et al*, 2003: 3). Once measured, the set of risk indicators in practice must be continually validated and refined together with the management responsible. Naturally, as the business environment is subjected to continual change, underlying risk indicators may also require enhancement, to preserve integrity and their predictive capabilities (Hoffman, 2002: 249).

Hoffman (2002: 249) stated that it is natural that institutions select and define risk indicators to a large extent based on availability of appropriate data. Hoffman (2002: 249) mentioned that a word of caution is important here, however. The best institutions select risk indicators based on their predictive value first, and data availability second, not the other way around (Hoffman, 2002: 249). In any event, although data may be readily available for many variables and risk indicators, it should be noted that a full set of effective composite risk indicators would generally impose even more responsibilities

for data collection and reporting (Yam, 1998: 4). As Herkes *et al* (2003: 5) mentioned, the capture of operational loss data is becoming a fundamental feature within the risk management framework of many institutions (Herkes *et al*, 2003: 4). Analysis of operational losses (including causative factors) in combination with associated risk indicators forms the evaluation stage of the operational risk monitoring cycle and should consider whether the risk measures have been validated as relevant, including whether they were proven to bear some direct relationship to the propensity of loss.

It is the view of this study not to evaluate the above-mentioned in too much detail but rather only to provide a mere glimpse of the practical considerations regarding the definition, data collection standards and emphasis of risk indicators and it is also the view of this study that further research is still needed on the above-mentioned subject. The following section of chapter 4 will then further the evaluation of KRIs in the banking environment by taking a look at the scorecard systems that is used within banks as a means of identifying and monitoring operational risk.

4.4 Scorecards systems: The nexus of risk assessment and risk indicators

This section will evaluate the scorecard⁴ systems that are used within banks and will include two examples of how scorecards play a role as KRIs in banks. It is important to keep in mind that this discussion on scorecards is merely intended to provide a better understanding of KRIs. The continual challenge in using risk indicators, then, remains that of identifying those that are both predictors of risk and for which data are readily available (Hoffman, 2002: 250). Risk indicators that do not meet both tests are of limited value to management. Thus, capturing data remains a key focal point. But as noted already, some risk indicators can meet both tests and still be of limited value because of timeliness concerns. Hoffman (2002: 250) stated that whether the problem lies with data or timeliness, one solution is to set up a scoring system of converting softer risk assessment information into risk indicators. An example of this would involve a typical 1-3, 1-5, or 1-10 range of scoring the answers to risk assessment or self-assessment

⁴ Scorecards were briefly mentioned in section 2.5.1.2.5 as a means of identifying operational risks.

questionnaires. As mentioned this section will provide two examples of KRI scorecards and the first example will be illustrated in the following section, which was written and contributed on behalf of Dresdner Bank and its New York Branch in Hoffman (2002: 251).

4.4.1 Creating KRI scores from qualitative reviews at Dresdner Bank

As Herkes *et al* (2003: 4) mentioned, the time for quantifying qualitative operational risk data has arrived. Quantification allows for risk managers to analyse the results of operational risk exercise performed throughout an institution efficiently and identify areas where significant operational risks exists (Herkes *et al*, 2002: 4). In addition, quantification allows a risk manager to benchmark processes and controls against pre-established standards and finally, quantification proceeds to a more efficient risk capital allocation (Herkes *et al*, 2003: 5).

(Hoffman, 2002: 251) stated that to quantify the qualitative operational risk profile, a scoring mechanism must be applied and stated that there are several scoring methodologies that work well. While each has its own unique features, the commonality between scoring methodologies is that they normalise the data and it is well known that different lines of business have operational risks that are unique to each business. As such, the number of operational risks associated with each line of business will vary. Whether the number of risks associated with a particular line of business is 50 or 500, in order to compare results across lines of business, risk managers must employ a mathematical means of normalising the data (Hoffman, 2002: 251). Tables 4.2 and 4.3 are an illustration of a scoring methodology that employs data normalisation.

As Bastany (1994: 12) and Bessis (2001: 3-4) mentioned, an operational risk profile should be dynamic. It will be updated as often as new data (risk/self-assessment, KPIs, etc.) are collected (Hoffman, 2002: 250). Any significant deviations from the previous risk profile should be enlarged for possible remedial action and this remedial action would depend primarily on management's operational risk appetite and the significance

of the increase in operational risk profile if the additional exposure were accepted (Hoffman, 2002: 251).

Table 4.2 Risk subcategory – Human capital

| Question Number | Question Weight | Answer Weight | Risk Score | Scoring Legend |
|-----------------|-----------------|---------------|-------------|---------------------|
| 1 | 4 | 5 | 1.43 | 4.1 -5 Excellent |
| 2 | 3 | 3 | 0.64 | 3.1-4 Above Average |
| 3 | 2 | 4 | 0.57 | 2.1-3.0 Adequate |
| 4 | 4 | 1 | 0.29 | 1.1-2.0 Poor |
| 5 | 1 | 3 | 0.21 | 0-1 Very Poor |
| 6 | 0 | 0 | 0 | |
| 7 | 0 | 0 | 0 | |
| | 14 | | 3.14 | |

Source: (Hoffman, 2002: 250)

Table 4.3 Risk subcategory – Unauthorized activities

| Question Number | Question Weight | Answer Weight | Risk Score |
|-----------------|-----------------|---------------|-------------|
| 1 | 4 | 5 | 2.5 |
| 2 | 1 | 1 | 0.31 |
| 3 | 3 | 2 | 0.75 |
| | 8 | | 3.38 |

Source: (Hoffman, 2002: 251)

This type of consolidated risk reporting allows a risk manager to identify with ease areas where significant operational risks exist and in addition, it allows a risk manager to see how changes in processes and controls affect an area's operational risk exposure (Hoffman, 2002: 252). The risk manager's main concern when developing this type of

analysis is that he would be unable to compare, for example, a capital market operation with a custody operation. However, after running a few pilot studies, it became clear that the scoring mechanism worked effectively by giving the risk manager an accurate portrayal of an area's operational risk exposure.

It is also found that a user could easily retrofit the scoring mechanism with other types of consolidated risk reporting and analysis (Hoffman, 2002: 252). When applying the scoring mechanism to the results of the risk/self-assessment, KPIs (see 4.2), and unexpected operational incidents, the results provide line and senior management with a snapshot of an area's operational risk exposure in one consolidated report for easy analysis rather than producing several reports for grueling interpretation. It also provides the risk manager with an almost real-time measurement of the operational risk exposure that exists within the institution. The above then concludes the first example of scorecards that was successfully converted into KRIs of operational risks. The following section will provide the second example, which was written and contributed by Robert Huebner for Deutsche Bank (Hoffman, 2002: 251).

4.4.2 Converting risk scores to heat maps at Deutsche Bank

As Theodore (2002: 22) mentioned, another step in the KRI process is to create a reporting format from the risk scores. One popular graphic for this is the heat map. As mentioned, Robert Huebner contributed a heat map format on behalf of Deutsche Bank (Hoffman, 2002: 251). As shown in figure 4.7, Deutsche Bank also used a scoring approach in comparing the results of its risk assessment process, that will illustrate and position them in a heat map format for ease of aggregate reporting and clear communication (Hoffman, 2002: 251). A number of banks have recently come out in favour of combining both quantitative and quantified operational risk indicators in the form of scoring systems and scorecards (Hoffman, 2002: 251). As Hoffman (2002: 251) mentioned, Mark Lawrence of ANZ Group is such an advocate. After a review of several assessment and quantification methods, including business measures or "scalars" such as revenues, assets, benchmarking, statistical analysis, and casual modelling, ANZ settled

on an elaborate system of enterprise-wide scorecards because they “avoid many of the problems inherent in the analysis of historical data, and can be much more forward looking, by capturing the knowledge and experience of the experts who design the scorecards” (Lawrence, 2000: 10). Figure 4.7 illustrates the questionnaire that was used by Robert Huebner for Deutsche Bank.

Figure 4.7 Converting risk scores to heat maps Deutsche Bank⁵

| Overall Evaluation of Risk Category | |
|---|---------------------------------------|
| <p>Once you have read the questionnaire and answered all the questions, please place a cross in the grid next to each of the categories. Your evaluation should indicate the level of importance the risks have in your whole business division. This evaluation enables you to weigh the risk categories each against the others and to sort them in order of their potential risk impact. Please use the eight levels to make your evaluation. White means a low level of importance in the business division, black stands for a high level of importance. Any evaluation can be expressed by using the six levels in between.</p> | |
| <p>Employees The risk/exposure associated with employing staff in large, complex, multinational financial institutions.</p> | <p>← Not relevant Critical →</p> |
| <p>The risk/exposure associated with large-scale projects.</p> | <p>← Not relevant Critical →</p> |
| <p>Technology (IT) The risks/exposures associated with using technology (not just PCs and all their associated pieces (printers, network, etc.)) but also telephones Internet ATM, etc.</p> | <p>← Not relevant Critical →</p> |
| <p>Non-IT Infrastructure & Natural Disasters The risk/exposure associated with owning assets both physical and electronic.</p> | <p>← Not relevant Critical →</p> |
| <p>External The risk/exposure associated with the environment external to the bank.</p> | <p>← Not relevant Critical →</p> |
| <p>Customer Relationships The risk/exposure associated with having customers and distribution channels.</p> | <p>← Not relevant Critical →</p> |

Source: (Hoffman, 2002: 252)

The above section then concludes the discussion on how risk scores are being converted to heat maps and was illustrated with an example at Deutsche Bank. The above-mentioned examples were intended to provide some background on where operational risk indicators are presently being used with great effectiveness. The following section will provide some case examples on “back-testing” operational risk indicators in order to better understand KRIs and their use.

4.4.3 “Back-Testing” operational risk indicators and scores: Some case examples

Calomaris and Herring (2002: 5) stated that if operational risk indicators had been used effectively, risk managers could argue that the likes of Barings (see 1.1) and Sumitomo Bank might well have focussed their resources and mitigated their operational risk exposure prior to suffering their unbearable financial losses. Many people will be familiar with the circumstances surrounding the collapse of Barings Bank⁶ and the series of control deficiencies that were exposed during investigations. Hoffman (2002: 253) stated that among these findings, it became clear that the blame for Barings’ loss cannot be targeted solely at Nick Leeson⁷; it must be shared throughout the management of the bank, reflective of the poor control environment, lack of supervision and accountability, and clouded communications and reporting.

Crouhy *et al* (1998: 450) argued whether risk measures could have forewarned the fall of this major international bank. In the case of Barings Bank, the financial world is left to ponder whether the systematic analysis of appropriate operational risk indicators at the business-line level, and the firm wide level, could not have provided warning signals of the inherent and control of the operational risks of Barings Singapore, but also spurned management into action.

⁵ The same type of questionnaire that will be used in the case study of chapter 5.

⁶ More on the collapse of Barings Bank can be read in Hoffman (2002) p 172 – 174.

⁷ Nick Leeson was the manager of the Singapore Monetary Exchange (SIMEX) for Barings Bank in London (Rawnsley, 2000: 1).

For example, a sampling of relevant operational risk indicators that Barings Bank may have captured include the following (Hoffman, 2002: 253):

- **Inherent risk indicators:** *Junior and senior staff tenure individual risk indicator:* Might have highlighted the relative inexperience of the employees managing the operations from within the Singapore Office. *Product complexity composite risk indicator.* While Nick Leeson was authorised only for intraday trading in options in futures, a significant weighting is generally attributed to the derivatives trading.
- **Management control risk indicators:** *Internal Audit indicators, issues tracking, or operations benchmarking:* Much have already been written about whether the collapse of Barings Bank could have been averted if management had been forced to focus on the findings of the internal audit report on Barings Futures of August 1994. Some institutions score internal audit issues based on severity. In some systems, issues outstanding and past due for a specified period would have attracted a higher risk rating.

Crouhy *et al* (1998: 450) argues whether or not the systematic analysis of these specific operational risk indicators, in conjunction with other composite indicators, would have focussed Barings' management attention, and sparked appropriate action, is open to some conjecture. Operational risk indicators are not, by themselves, a panacea for control deficiencies (Hoffman, 2002: 253). However, it is logical that the systematic use of operational risk indicators may have mitigated some of the control weakness evident in a number of high-profile loss events.

Yam (1998: 545 – 546) mentioned that the process of capturing and analysing operational risk indicators can facilitate management ownership (see 3.4.1) of operational risks and provide a platform for the proactive management of a control environment. The investigation into the Barings Bank collapse cited poor supervision and confusion over management and supervisory responsibilities with the bank's matrix structure as major contributors to the bank's demise (Hoffman, 2002: 253). Hoffman (2002: 253) also stated that when used as a fundamental component of an overall risk management framework,

operational risk indicators can convert the previously intangible to the tangible for the line management and they can also create a proactive concern for the management of these proxies.

Yam (1998: 551) stated that in the case of Sumitomo's rogue trader, Hamanaka, there was still some uncertainty as to who had control over the activities of Hamanaka, despite reasonable sound supervision controls due to the global nature of the operations and questions. The systematic use (analysis and discussion) of operational risk indicators will reinforce management ownership of the control environment, as they seek to modify behaviour and strengthen controls (Hoffman, 2002: 255). Hoffman (2002: 255) also stated that the ability to report periodically on operational risk indicators at various levels within the institution is also important.

While proactive management of operational risk is imperative at a functional management level, the enterprise-wide risk profile should be a tool used for Board supervision. Perhaps the losses sustained by Metallgesellschaft may have been mitigated if there had been greater transparency in relation to controlling weaknesses (Yam, 1998: 551). Equally, the Barings Board may have expressed greater concern had Barings Singapore reported on operational risk indicators in comparisons to the other operations of the bank or to industry benchmarks (Hoffman, 2002: 255).

To conclude this section it can be said that, generally speaking, investment banking front office operations are dominated by fiercely competitive and performance-based cultures. Hoffman (2002: 255) stated that the remuneration policies of many banks may reward bonuses on absolute performance, despite the business line taking excessive operational risks. The use of operational risk indicators for internal or external benchmarking, or as an allocation basis for risk capital, is an effective framework in which to achieve risk based behavioural change and reward better quality earnings. The following section of chapter 4 will provide a brief overview of the implementation of a system of operational risk indicators.

4.4.4 Implementing a system of operational risk indicators

The following section will summarize how some of the best firms all around the world are taking action toward implementing and/or refining their efforts towards operational risk indicator tracking and analysis as follows (Hoffman, 2002: 255):

4.4.4.1 Identify and define

Risk managers work at all levels within the institution to begin to identify and define variables, operational risk indicators, and composite indicators (Theodore, 2002: 23). These measures should contain an appropriate hybrid blend of firm wide and business-line indicators (Hoffman, 2002: 255). This may be a significant step forward for many institutions. Hoffman (2002: 255) stated that cultural and behavioural implications should also not be taken slightly. However, as has been mentioned previously, soliciting management input from the outset will assist in establishing the credibility and longevity of the process.

4.4.4.2 Data collection, tracking and analysis

Risk managers establish enduring procedures for systematic data collection, reporting and analysis (Theodore, 2002: 25). The reporting and analysis processes are tailored to target across the various levels of the institution.

4.4.4.3 Validation of operational risk indicators

A mechanism for the periodical evaluation and update for operational risk indicators is also crucial in maintaining the longevity and management faith in the effectiveness of operational risk indicators (Theodore, 2002: 25). Hoffman and Taylor (1999: 15) stated that these measures must be responsive to the changing business environment, and should also be evaluated in the light of actual loss data, to determine predictive capabilities. As mentioned, the above section is only a brief discussion on the implementation of a system

of operational risk indicators that is used by the best and well known institutions around the world.

4.4.5 Conclusion

In keeping with the principles of operational risk management, as outline by the Basel Committee (see chapter 2), operational risk and exposure indicators should be transparent and reasonable, with any underlying assumptions clearly communicated to end users. Transparency in operational risk indicators is essential for the long-term integrity of this aspect of a risk management framework. Hoffman and Taylor (1999: 15) stated that if performance assessment such as capital allocation, is associated with their use, management will maintain a vested interest in ensuring that the operational risk indicators are responsive to risk-based behavioural improvement.

As Theodore (2002: 13 – 25) and Hoffman (2002: 255) mentioned, operational risk indicators are poised to become a critical component of effective operational risk management programmes. Successful business managers already use key performance indicators (KPIs) (see 4.2) to gauge business efficiency and profitability upsides. As can be seen throughout chapter 4, operational risk indicators simply serve as a gauge of potential downside outcomes. When applied and presented effectively, operational risk indicators should serve to identify important business vulnerabilities, or as warning lights for navigating the business clear of the dangers present in the business environment.

In addition to the above-mentioned, it can be said that as the debate continues over operational risk modelling and regulatory capital, risk measures are almost certain to help lay part of the data foundation on which to construct durable models (Hoffman & Taylor, 1999: 15). Identifying candidates for tracking operational risk indicators is only half the battle. Once a risk manager has a good lead on an operational risk indicator or two, his selection must pass some additional tests (Hoffman, 2002: 255). First and foremost, the risk manager must confirm that they are, in fact, a predictor of operational risk and that they can serve as part of an “operational risk early warning system” and/or be used in

modelling (Hoffman & Taylor, 1999: 16). Secondly, the risk manager must come up with data and/or a quantification technique (Hoffman & Taylor, 1999: 16). Thirdly, the risk manager must test his hypothesis (candidate) (Hoffman, & Taylor, 1999: 16). The risk manager is to analyse past losses and/or areas of concern in the business in order to identify causation trends. Without a qualification or measurement, a risk manager has no way to track progress of the event.

Where as section 4.1 to 4.4 have provided a theoretical discussion on the key indicators of operational risk, the following sections will provide some examples of operational risk indicators that is eminent in a Retail Bank. It is important to keep in mind that these risk indicators will only be theoretically identified in chapter 4. When identified, chapter 5 will then evaluate these risk indicators by means of a case study in a Retail Bank in South Africa.

4.5 Identifying key risk indicators (KRIs)

As mentioned in section 4.4.5, this section will provide some examples of typical operational risk indicators that is frequent visible in a bank, but before this section can begin to identify and evaluate the different examples of KRIs in more detail, the following section will first provide the basic facts that must be kept in mind when identifying KRIs.

4.5.1 Key risk indicators (KRIs): Basic facts in identifying KRIs

This section will highlight the basic facts of KRIs stated by Hoffman (2002: 255-256) and McPail (2003: 2-4):

- To identify and track predictive risk indicators and drivers of operational risk, it is important to capture both quantitative and qualitative driver data. An important aspect of identifying KRIs is to provide risk indicator reports and scores to management levels appropriate for action.

- Risk and performance indicators must be present in the best institutions and studies have shown that the most successful institutions use key performance measures. It is also important to keep in mind that different risk indicators will be used at different levels and in different areas. A business line manager will track risk indicators for his or her own business processes, whereas a corporate manager will be more interest in firm wide risk indicators or variables that can be used consistently in all areas and in all businesses, such as error rates, turnover levels, and customer complaints.
- Composite risk indicators are useful management tools. Tracking a variety of issues in a survey, for instance, and scoring the results in a weighted average over time has been shown to be a useful method of tracking management and system performance. Section 4.4 gave the example of tracking a variety of issues in a technology environment to illustrate this point. Many of the issues, such as degree of system support reliability, and credibility, for instance, are difficult issues to quantify, but can be tracked, scored, scaled, and monitored over time on a scaled basis. As an overall average, the scores, or aggregate scores, can be used as performance measures.
- The fourth point to consider when identifying KRIs is that the best risk indicator will be forward looking or predictive in order to be useful as either a modelling or management tool.
- The fifth basic aspect to consider when identifying KRIs is to keep in mind that risk indicators are generally managed by a central unit, whether in the business lines themselves or at a firm wide level. Regardless of the location, the management process should include a validation where the units being tracked or measured have an opportunity to review both input and output of the tracking system and corroborate the data against their own sources.

- The sixth factor to consider when identifying KRIs is to remember the importance of quantification. If any institution limits itself to tracking only those risk indicators that can be readily quantified neatly, it may be missing more relevant issues. Relative-ranked scoring can bridge this gap.
- Another important factor to consider when identifying KRIs is to keep the risk indicators relevant to a business. Business staff and managers should be involved in the key risk indicators that are most relevant to their risk and performance.
- To keep in mind that model factors are different is also important factor to consider when identifying KRIs. Risk indicators or factors used for modelling should be more simplified. Whereas a business or profit centre might use numerous risk indicators to track the business at hand, it can become very confusing to use all of the risk indicators in modelling.
- The last important aspect this section wants to highlight when identifying KRIs is to remember that scorecards are an effective way of combining both qualitative and quantitative risk indicators and scores fro a prospective representation of risk. Some institutions have become staunch advocates of scorecards as their primary basis of operational risk representation and for capital allocation purposes.

With the above-mentioned in mind the following section can begin to identify and evaluate the most important KRIs of operational risk in the banking environment.

4.5.2 Identifying KRIs in a Retail Bank

The identification of the KRIs of operational risk in the whole banking environment is an enormous process, therefore chapter 4 will only identify and evaluate the KRIs of a Retail Bank. To better understand the following sections, it is important to first examine the

different divisions of the banking sector. The following section will highlight the different divisions of a bank and will re-evaluate the Standardized Approach that was discussed in chapter 2 and is intended to provide some background regarding the identification of KRIs for different business lines.

It is important to keep in mind that indicators that will be discussed in the following section are business specific indicators of operational risk, and for this reason they will only be named and only a short explanation will be given where necessary. As mentioned in a previous section of this chapter, the trick with KRIs is to find the intersection between business-specific and firm wide risk indicators, therefore the following section will only evaluate the KRIs of operational risk as business specific indicators, where chapter 5 will provide them as firm wide risk indicators and will also test them in the South African banking environment.

4.5.2.1 Different divisions of a bank

Van den Brink (2002: 50) stated the following divisions of a bank:

- Investment banking:
 - Corporate Finance.
 - Trading and Sales.
- Banking:
 - Retail Banking.
 - Commercial Banking.
 - Payment and Settlement.
- Others:
 - Retail Brokerage.
 - Asset Management.

Van den Brink (2002: 50) also mentioned that the above can then be regarded as business lines and thus the Standardized Approach (2.4.4.2) is used. The Standardized Approach

(also known as the Multi-Indicator Approach) is more focused on specific business lines for example the above-mentioned, and the approach acknowledges the different character of businesses within the bank. In its consultative paper (see chapter 2), the Basel Committee suggest mapping the financial institution's businesses to predetermined business lines. The risk indicators for operational risk per business line are then also predetermined (Van den Brink, 2002: 49). The above-mentioned business lines and risk indicators describe in the Basel Document are shown in table 4.4.

Table 4.4 Business lines of a bank and risk indicators

| Business Units | Business Lines | Indicator |
|---------------------------|------------------------|------------------------------|
| Investment Banking | Corporate Finance | Gross Income |
| | Trading and Sales | Gross Income |
| Banking | Retail Banking | Annual Average assets |
| | Commercial Banking | Annual Average assets |
| | Payment and Settlement | Annual Settlement throughput |
| Others | Retail Brokerage | Gross Income |
| | Asset Management | Total Funds under management |

Source: (Van den Brink, 2002: 50)

As mentioned in chapter 2, these indicators are multiplied with a β -factor, which represents a rough estimate of the relationship between the industry's loss experience and the broad financial indicator representing the bank's activity in a given business line, calibrated to a desired supervisory sound standard. Van den Brink (2002: 50) stated that the relative weighting of each business line is describe in ranges in the consultative document of the Basel Committee.

The Basel Committee formulated the weightings in a range since it was not possible to analysis more exactly due to a lack of data. The relative weightings of the business lines

proposed by the Basel Committee are shown in table 4.5. The business lines “insurance” and “agency services” are not included in the proposal, although the final proposal is expected to include them.

The β -factor itself is calculated as follows:

$$\beta = \frac{[20\% \text{ current total MRC (\$)}] \times [\text{business line weighting (\%)}]}{\sum \text{Financial indicator for the business line from bank sample (\$)}}$$

Where MRC = minimum capital charge.

Table 4.5 Relative weightings of the business lines

| Business Lines | Range |
|-------------------------------|-----------------|
| Corporate Finance | 8 – 12 |
| Trading and Sales | 15 – 23 |
| Retail banking | 17 – 25 |
| Commercial Banking | 13 – 20 |
| Payment and Settlement | 12 – 18 |
| Retail Brokerage | 6 – 9 |
| Asset Management | 8 – 12 |
| Total | 80 – 120 |

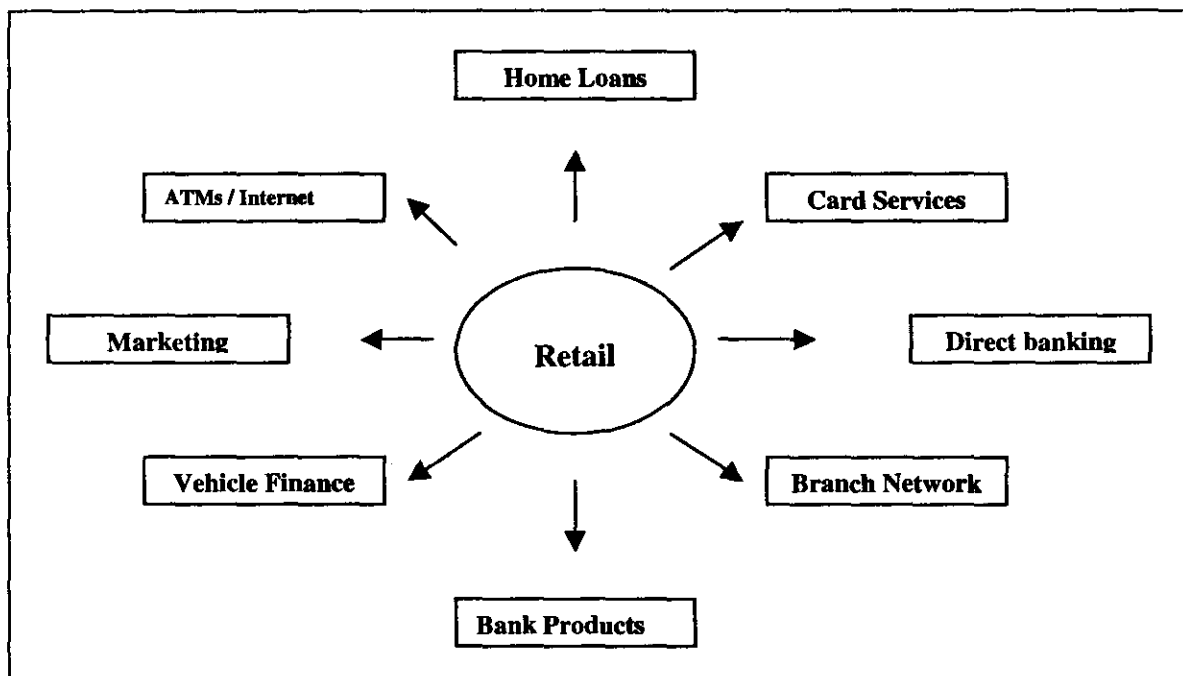
Source: (Van den Brink, 2002: 50)

As already mentioned in the beginning of this section, the above-mentioned is mere intended to provide background on the different divisions of a bank and the most eminent indicators. The Standardized Approach is also identified as the best approach to assign KRIs to the different business sectors. The following section will then firstly identify and evaluate the different elements of a Retail Bank and will then identify the KRIs of each element of a Retail Bank.

4.5.2.2 Elements of a Retail Bank

Before this study can proceed to identify and evaluate the different KRIs of a Retail Bank, it is important first evaluate the different elements of a Retail Bank. Van den Brink (2002: 51) identified the following elements of a Retail Bank, which is also illustrated in figure 4.8:

Figure 4.8 Elements of a Retail Bank



Source: (Compiled by the Author)

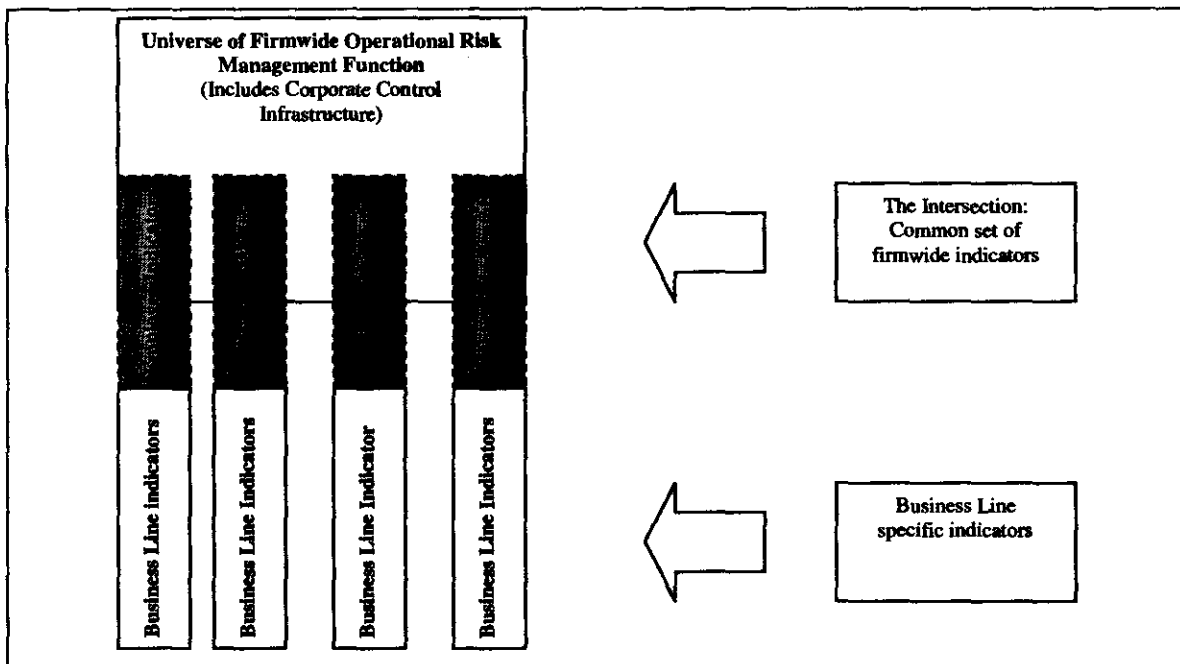
- Home Loans.
- Card Services.
- Direct banking (ATMs & Internet).
- Branch network.
- Bank Products (Current account & Savings Account).
- Vehicle Finance.
- Marketing.

- Branch Insurance.

Now that the different elements of a Retail Bank are identified, the following sections can proceed to identify and evaluate the KRIs of each of the above-mentioned elements.

4.5.2.3 KRIs of a Retail Division

Figure 4.9 Employee indicators



Source: (Hoffman, 2002: 242)

Hoffman (2002: 245) and Van den Brink (2002: 51) stated that one of the most eminent KRIs of operational risk is the employee indicator, therefore it is the view of this study to provide evaluate this indicator in more detail as an introduction to this section. To better understand the employee indicator, this section wants to refer to figure 4.2. Figure 4.2 is an illustration of the intersection of some risk indicators between different business lines. The employee indicator is regarded as the intersection, because of the fact that it is eminent in almost all the elements (business lines) of a Retail Bank. Referring to figure 4.2, figure 4.9 is an illustration of employee indicators. As mentioned, employee

indicators are the intersection between indicators in a Retail Bank as illustrated in figure 4.9.

The question now may exist which risk indicators can be regarded as employee indicators? The following nine employee risk indicators have been identified as the most renowned employee indicators of operational risk in a Retail Bank of a bank and are provided here as firm wide risk indicators:

- **Employee turnover:** Employee turnover is the rate at which new employees are leaving and joining the bank. The higher the employee turnover, the more time must be spend on training new employees.
- **Overtime worked by employees:** The more overtime an employee work, the more likely he will make a mistake, for example, if he work fifteen ours a day, the last four hours of the day he is likely to make more mistakes because of the fact that he is more tired and his concentration levels are low. The more overtime an employee work (for example till late at night, or more than fifteen ours a day), the more tired he will be the next morning and the lower his concentration levels will be the next morning and the more likely he will make a mistake
- **Vacation and absenteeism rate:** If personnel are required to take fourteen days leave per year; the risk indicator will be the personnel who have not taken their eight days leave. These personnel are then also more likely to make more mistakes then those who have taken their eight (or more than eight) days leave.
- **Number of approved positions vs. actual compliment:** In addition to the above-mentioned staff cost, the personnel manager must decide if the employment of a new employee will be beneficial for the bank, for example, he must ask himself if there will be enough funds available to pay this employee and if there will be enough work to keep the employee busy.

- **Number of temporary personnel vs. the total number of personnel:** An increase in the number of temporary personnel will increase the number of inexperienced personnel, which will increase the potential for employee mistakes, as a result of their inexperience.
- **Junior and senior staff tenure individual indicator:** This indicator highlights the relative inexperience of employees. As mentioned in 1.5, the more inexperienced employees are employed, the higher the potential will be for an employee error to occur, thus the higher the exposure to operational risk.
- **Number of transactions per staff member:** The higher the number of transactions per staff member, the more likely an employee error will occur, because it become difficult to monitor and control such a large amount of transactions per staff member, thus, the higher the exposure to operational risk.
- **Total for specific delivery failures:** For example, the number of teller shortages at a branch can also be an indication of the exposure to operational risk.
- **Technology management control risk indicator:** Include the number of employees requiring training in new technology and will be represented as actual numbers or be weighted to reflect the total number of employees in the department.

The above-mentioned are then the key employee indicators of operational risk and are eminent amongst all the different business lines of the bank. With the above-mentioned in mind, the following sections will now identify and evaluate the most renowned **KRIs of operational risk** in the different divisions of a Retail Bank.

4.5.2.3.1 Key Risk Indicators (KRIs): Home loans

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator

- **Customer complaints:** The number of customer complaints for a specific time, for example, one month. Customer complaints are an indication of how satisfied the bank's customers are.

- **Product complexity:** The more complex a bank product is, the higher the operational risk will be, because employee errors will be more likely to occur. The more complex a product, the more difficult it become to monitor and control it.

- **Application turnover time (customer satisfaction):** It must be one of the objectives of the bank to keep the application turnover time as low as possible. If the application turnover time is high, it can be an indication of operational risk.

- **Non-performance with compliance with policy:** If a bank does not comply with its policy, it can increase the exposure to operational risk.

- **Number of settlement fails:** The number of settlement fails per geographic area is also a good indication of operational risk. Settlement fails can be as a result of inadequate documentation of a certain transaction.
- **Evaluation losses:** Before a client can borrow funds from a bank he/she is thoroughly evaluated and the collateral is determined. It can happen that these evaluations are lost which in turn increases operational risk.

4.5.2.3.2 Key Risk indicators (KRIs): Card services

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator
- **Increase in the number of customers:** If there is an abnormal increase in the number of customers per a specific time, for example one month it will be more difficult to monitor and evaluate each of them and will increase the exposure to operational risk.
- **Product complexity composite risk indicator:** The more complex a product is, the more likely an employee error will occur, in other words a higher operational risk, because it is difficult to monitor and control a complex product.

- **Increase in the number of lost and stolen ATM (credit cards) cards:** The higher the number of lost and stolen cards, the higher the burden on employees, because they must provide new cards at the same rate at which they are lost, thus, it increases the exposure to operational risk.
- **Number of customer complaints:** The number of customer complaints for a specific time, for example, one month. If the number of customer complaints is high, it is an indication of an operational risk.
- **System downtime:** The longer the system is down the higher operational risk will be. It is important that the system is well defined and the bank must identify what systems are critical. The next step would be to define what a “system problem” is. If all the above-mentioned are in place then this indicator would be measurable.
- **Number of audit points outstanding:** The number of audit points outstanding could also be a good indication of the level of operational risk.
- **Total losses attributed to errors:** This will provide the bank the level and exposure to operational risk in the card division.
- **Number of accounts closed/opened:** The number of accounts that is closed in a certain time will also be an effective indicator of operational risks so will be the number of accounts opened. If there is an abnormal amount of accounts opened/closed in a specific time, it can be an indication of an operational risk.
- **Application turnover time (customer satisfaction):** It must be one of the objectives of the bank to keep the application turnover time as low as possible. If the application turnover time is high, it can be an indication of operational risk.

4.5.2.3.3 Key risk indicators (KRIs): Direct banking (ATMs & Internet)

- **Employee indicators** (see 4.5.2.3):
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator

- **System downtime:** The longer the system is down the higher operational risk will be. It is important that the system is well defined and the bank must identify what systems are critical. The next step would be to define what a “system problem” is. If all the above-mentioned are in place then this indicator would be measurable.

- **Physical location:** If an ATM is located in an area where crime is high, the potential for operational risks will be higher but the bank must be able to rate the ATMs in terms of their geographical area of location to effectively measure this indicator.

- **Operating turnover (ATMs):** The time people spend in queues is and indication of operational risk, in other words, the lower the operating turnover at ATMs, the higher operational risk will be. This indicator is difficult to measure.

- **The number and value of ATM transactions:** The number and value of ATM transactions will be a good indication of the exposure to operational risk.

- **Number of customer complaints:** The number of customer complaints for a specific time, for example, one month. If the number of customer complaints is high, it is an indication of an operational risk.
- **Number of ATMs:** The more ATMs there are, the more difficult it will be for the bank to monitor and effectively control them, thus a higher operational risk.

4.5.2.3.4 Key risk indicators (KRIs): Branch network

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator
- **Physical location of branches:** If a branch is located in an environment with a high crime rate the operational risk will also be higher, because it is more likely that the bank in a high crime rate environment will experience a crime than a branch in a low crime rate environment.
- **Number of customer complaints:** The number of customer complaints for a specific time, for example, one month can also indicate the exposure to operational risk. Customer complaints in an operational risk context are the complaints regarding employees and their work (efforts).

- **Inadequate intranet between banks:** If there is an inadequate intranet between branches, it will stem the flow of information between the branches and will then increase operational risk.
- **Physical losses at branches:** A large physical loss at a branch will be an indication of an operational risk, for example a loss due to “An Act of God”, for example flooding.
- **Number of transactions per staff member:** The higher the number of transactions per staff member, the more the staff member will be exposed to errors, thus, the higher the exposure to operational risk.
- **Total for specified delivery failures:** The number of teller shortages, interest write backs is examples of this indicator.

4.5.2.3.5 Key risk indicators (KRIs): Bank products (savings & current account)

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator
- **Number of settlement fails:** The number of settlement fails per geographic area is also a good indication of operational risk. A settlement failure can be as a result of the incorrect documentation of a certain transaction.

- **Number of accounting losses:** The number of accounting losses in a specific timeframe will be an effective indicator, for example the higher the amount of accounting losses, the higher the exposure will be to operational risk.
- **Number of customer complaints:** The number of customer complaints for a specific time, for example, one month. If the number of customer complaints is high, it is an indication of an operational risk.
- **Aged confirmations:** The longer the client must wait for confirmation of the deal, the higher the operational risk will be.
- **Evaluation losses:** Before a client can borrow funds from a bank he is thoroughly evaluated and the collateral is determined. It can happen that these evaluations are lost which in turn increases operational risk.
- **Volume of transactions and volume of trade:** The higher the volume of trade and transactions, the more the bank will be exposed to operational risk, because the more difficult it become to monitor and control the transactions.

4.5.2.3.7 Key risk indicators (KRIs): Marketing

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator

- **Decrease in the sale of banking products:** If there is a sudden decrease in the sales of the banking products it can be an indication of an operational risk. Any abnormal (more than usual) decrease in the sale of banking products can be an indication of a potential operational risk.
- **Lost in market share due to inadequate marketing:** A lost in market share can also be an indication of operational risks, because a loss in market share can be an indication of inadequate marketing, and this can be as a result of a high exposure to operational risk.
- **Customer satisfaction survey:** A survey can be done to provide the bank with information regarding the customer satisfaction, which can also be an indicator of the exposure to operational risk.

4.5.2.3.8 Key risk indicators (KRIs): Branch insurance

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual compliment
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator
- **Branch location:** If the branch is located in a geographic environment where, for example floods are a common occurrence, the exposure to operational risk will be higher.

- **Conditions of the branch's infrastructure:** If the branch is situated in an old building, the chances that something will happen to the building is higher and causes an increase in the exposure to operational risk.
- **Number and value of physical loss:** This indicator can be stratified into different classes of losses, for example number of accidents and vandalism. Other examples include "Acts of God", for example floods.

4.5.2.3.9 Key risk indicators (KRI): Vehicle finance

- **Employee indicators (see 4.5.2.3):**
 - Employee turnover
 - Overtime worked by employees
 - Vacation and absenteeism rate
 - Number of approved positions vs. actual complement
 - Number of temporary personnel vs. total number of personnel.
 - Junior and senior staff tenure individual indicator
 - Number of transactions per staff member
 - Total for specific delivery failures
 - Technology management control risk indicator
- **Customer satisfaction survey:** A survey can be done to provide the bank with information regarding the customer satisfaction, which can also be an indicator of the exposure to operational risk.
- **Number of customer complaints:** The number of customer complaints for a specific time, for example, one month. If the number of customer complaints is high, it is an indication of an operational risk.

- **Number of settlement fails:** The number of settlement fails per geographic area is also a good indication of operational risk. A settlement failure can be as a result of the incorrect documentation of a certain transaction.
- **Number of transactions:** The higher the volume of transactions the more difficult it become to monitor and controls them and this could increase the exposure to operational risk.

The above section then concludes the discussion on the business-specific indicators of operational risk in a Retail Bank. It is important to keep in mind that these risk indicators are not the only indicators of operational risk in a Retail Bank but it is the view of this study that they are amongst the most renowned.

4.6 Conclusion

The aim of chapter 4 was to evaluate the key risk indicators (KRIs) of operational risk in a banking environment. Chapter 4 puts great emphasis on distinguishing between a key performance indicator (KPI) and a key risk indicator (KRI) in the banking environment. A KPI is identified as an indicator that measures the performance of the bank at a specific time, whereas a KRI is identified as an indicator of a potential risk, in other words an early warning system of a potential operational risk.

All around the world banks are developing a system to identify KRIs of operational risk, because without sufficient KRIs, banks will not be able to identify potential operational risks and will be more exposed when it actually happen. Chapter 4 only aimed to provide a theoretical discussion on the key indicators of operational risk and only identified some of the most renowned KRIs as business specific risk indicators in a South African Retail Bank. Chapter 5 will discuss and evaluate the KRIs of operational risk as firm wide risk indicators and will also determine their viability in a South African Retail Bank by means of a case study.

Chapter 5

Key Indicators of Operational Risk In a Retail Bank of South Africa: A Case Study

“A risk indicator is piece of information that is a proxy for risks. The idea is that risk indicators should provide a good indication of the level of the underlining risk, while being readily available or easily calculated,” (Hoffman, 2002: 244)

5.1 Introduction

As mentioned in chapter 4, one of the main objectives for operational risk managers is to identify and evaluate the key indicators of operational risk in the banking environment. The key challenge in dealing with operational risk indicators is in identifying or constructing metrics that serve as predictors or “drivers” of operational risk. As (Theodore, 2002: 5) mentioned, most indicators are trailing in nature to other risk indicators, for example credit risk indicators, because not enough attention has yet been given to the development of effective operational risk indicators. That is to say, operational risk indicators do a far better job in confirming recent history than they do in predicting the formation of operational risk storm clouds on the horizon.

It is also important that operational risk indicators must not just be identified for specific business lines, but that they are identified across the institution as firmwide¹ operational risk indicators, in order to provide an overall view of the institution’s operational risk exposure (Van den Brink, 2002: 29). To identify and evaluate the key indicators of operational risk across all the divisions of a bank is enormous task, therefore chapter 5 only aims to identify and evaluate the key indicators of operational risk in a South African Retail Bank. It is also important to keep in mind that the

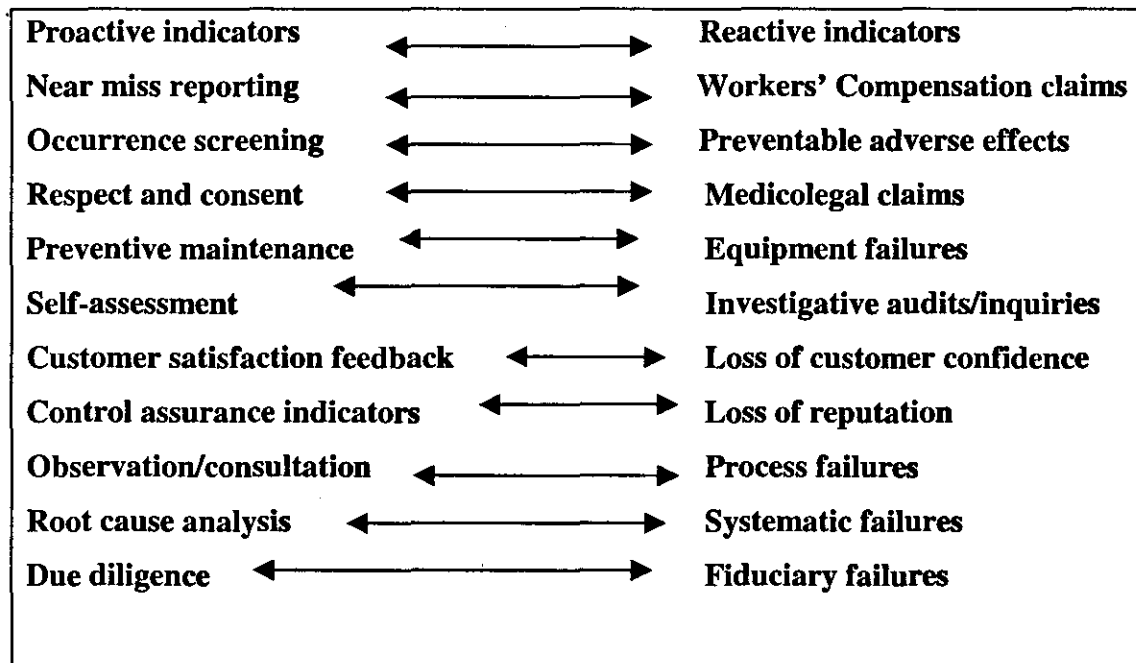
¹ Firmwide operational risk indicators are discussed in section 4.2.3

operational risk indicators identified and evaluated in chapter 5, are not the only indicators of operational risk of a Retail Bank in South Africa, but are regarded as amongst the most renowned.

5.2 Key operational risk indicators in a Retail Bank

The following section will identify the key indicators of operational risk in a Retail Bank. It is important that these indicators have some, or all of the characteristics of a typical operational risk indicator which is stated in figure 5.1, to be effective as a method of identifying an operational risk (Herkes *et al.*, 2003: 56). Typically resources are allocated to reactive indicators with little commitment or attention afforded to proactive management, therefore the focus must shift to achieving long-term substantial improvement.

Figure 5.1 Typical operational risk indicators: Retail Bank

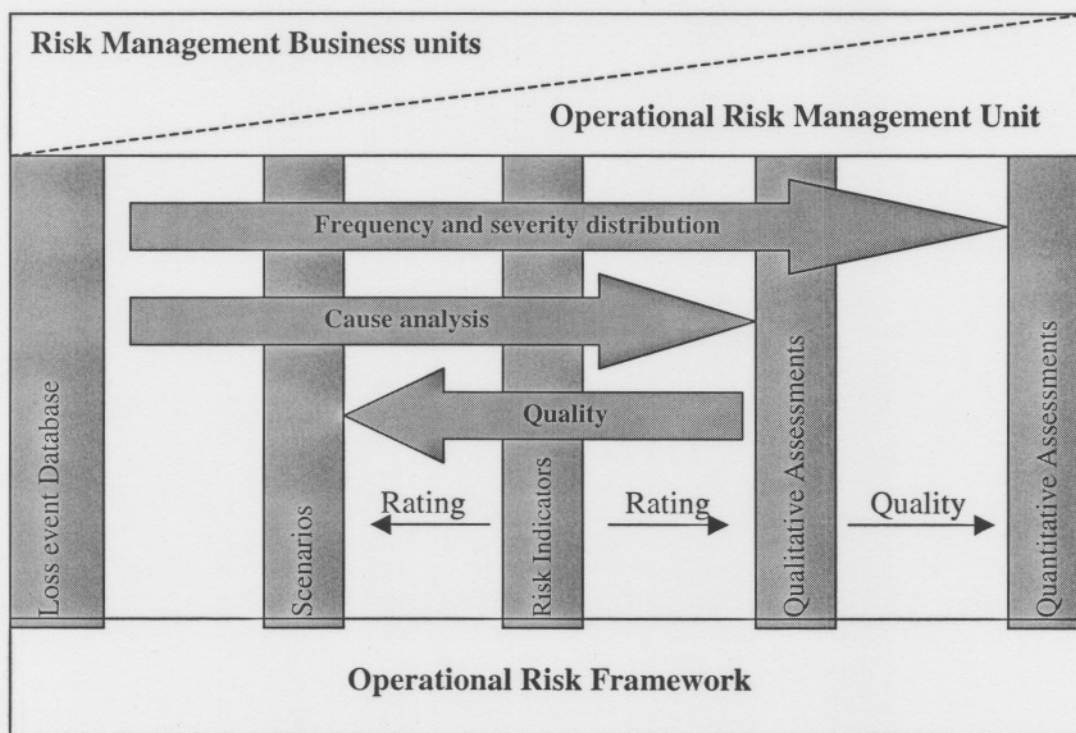


Source: (Compiled by the author)

Some indicators of operational risk in a Retail Bank were already identified in chapter 4 (see 4.5.2.3), but these indicators were identified as business specific indicators of

operational risk. The aim of this section is to provide those indicators as firm wide indicators of operational risk, in other words, as indicators that are identified in all the business lines of a Retail Bank. But, before this section can proceed to evaluate the firm wide indicators of operational risk in a Retail Bank, it is important, however to first take a look at where firm wide indicators of operational risk are situated in the integrated management system of operational risk. Figure 5.2 is an illustration of the integrated management of operational risk.

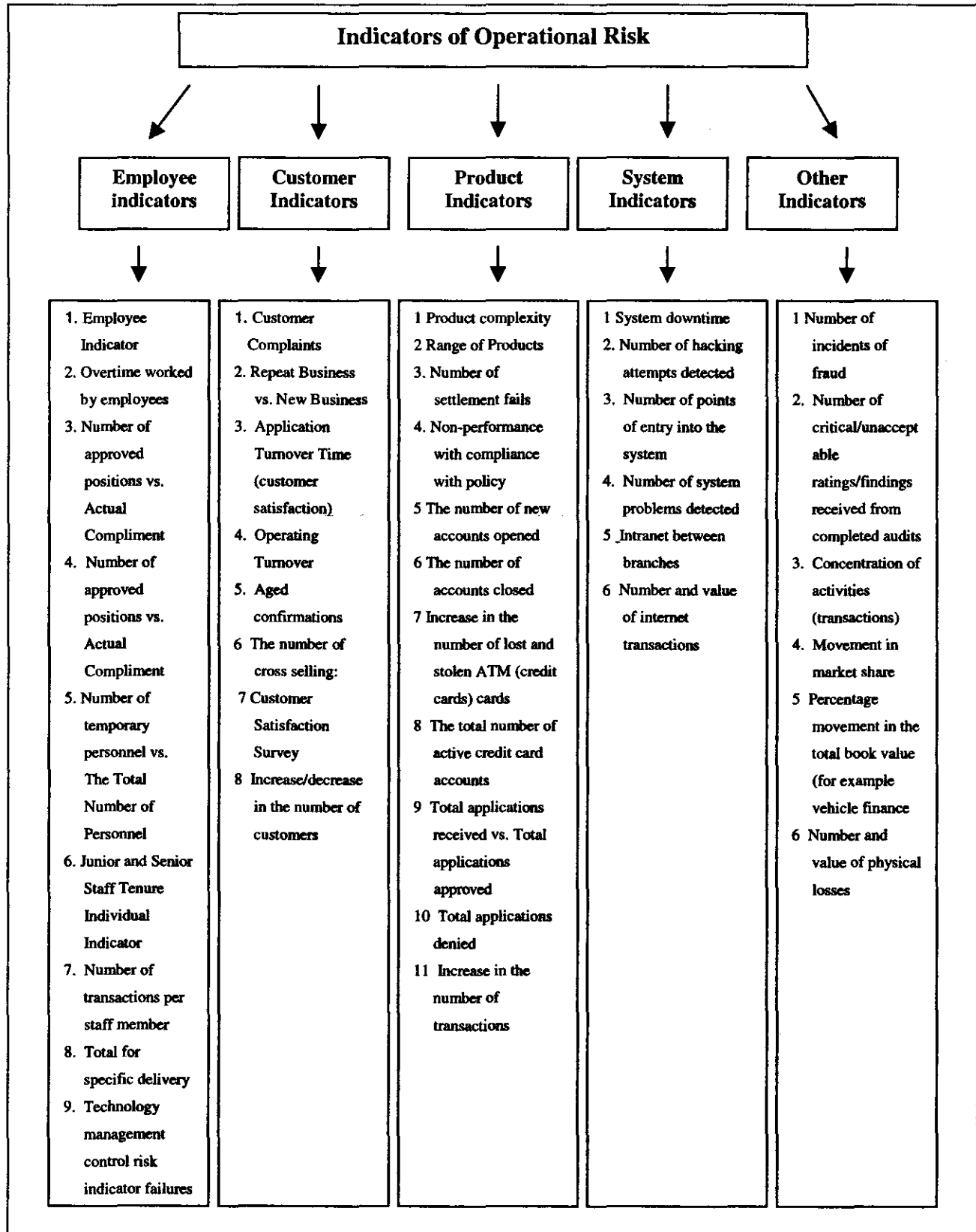
Figure 5.2 The integrated management of operational risk



Source: (PriceWaterHouse & Coopers, 2003)

As seen in figure 5.2, the risk manager must work hard to distil those indicators of operational risk that will prove the most useful for managing the institution's future risk and potential, not simply measuring its recent loss potential. Perhaps most of all, operational risk indicators must be prospective to be useful (Theodore, 2002: 5).

Figure 5.3 Indicators of operational risk: Retail Bank



Source: (Compiled by the author)

The following sections will now name and describe the different categories of operational risk indicators that were identified in chapter 4 (see 4.2.3). This study has classified operational risk indicators under five categories, which include the following:

- Employee Indicators.
- Customer Indicators.
- Product Indicators.
- System Indicators.
- Other.

Figure 5.3 is an illustration of the above-mentioned indicators of operational risk in a Retail Bank. Each of these indicators will be theoretically examined in the following section and the viability of each indicator in a Retail Bank will then be evaluated in a later section of chapter 5 by means of a questionnaire. It is important to keep in mind that some of these risk indicators were already identified and evaluated in chapter 4, but they were evaluated as business-specific risk indicators. The following section will aim to evaluate the above-mentioned risk indicators then as firm wide risk indicators.

5.2.1 Employee indicators

The following section will name and describe some of the different employee indicators of operational risk in a Retail Bank. As mentioned in chapter 4, these operational risk indicators are regarded as firm wide indicators, because they are perceptible in all of the business lines of a Retail Bank (see fig. 4.9).

5.2.1.1 Employee turnover

Employee turnover is the rate at which new employees are leaving and joining the bank. The higher the employee turnover, the more time must be spend on training new employees, and the higher the number of inexperienced employees will be and the higher the exposure to operational risk.

5.2.1.2 Overtime worked by employees

The more overtime an employee work, the more likely he will make a mistake, for example, if he works fifteen ours a day, the last four hours of the day he is likely to make more mistakes because of the fact that he is more tired and his concentration levels are lower. The more overtime an employee work (for example till late at night, or more than fifteen ours a day), the more tired he will be the next morning and the lower his concentration levels will be and the more likely he will make a mistake.

5.2.1.3 Vacation and absenteeism rate

If personnel are required to take fourteen days leave per year; the risk indicator will be the personnel who have not taken their fourteen days leave. If an employee do not take fourteen or more than fourteen days leave, he will be more likely to suffer from work related stress, tiredness, etc., which will increase the exposure to operational risk.

5.2.1.4 Number of approved positions vs. actual compliment

The personnel manager must decide if the employment of a new employee will be beneficial for the bank, for example, the personnel manager must ask himself if there will be enough funds available to pay the new employee and if there will be enough work to keep the employee busy.

5.2.1.5 Number of temporary personnel vs. the total number of personnel

An increase in the number of temporary personnel will increase the number of inexperienced personnel, which will increase the potential for employee mistakes, as a result of their inexperience. The higher the percentage of temporary personnel in an institution, the higher the exposure to operational risk (Hoffman, 2002: 244).

5.2.1.6 Junior and senior staff tenure individual indicator

This indicator highlights the relative inexperience of employees (see 4.4.3). As mentioned in 1.5, the more inexperienced employees are employed, the higher the potential will be for an employee error to occur, thus the higher the exposure to operational risk.

5.2.1.7 Number of transactions per staff member

The higher the number of transactions per staff member, the more likely an employee error will occur, because it become difficult to monitor and control such a large amount of transactions per staff member, thus, the higher the exposure to operational risk.

5.2.1.8 Total for specific delivery failures

The total for specific delivery failures include, for example, the number of teller shortages at a branch and can also be an indication of the exposure to operational risk.

5.2.1.9 Technology management control risk indicator

The technology management control risk indicator include the number of employees requiring training in new technology and will be represented as actual numbers or be weighted to reflect the total number of employees in the department. The higher the number of employees requiring training in new technology, the higher the exposure to operational risk, because not every employee is capable to handle the use of new technology in a bank (PriceWaterHouse & Coopers, 2003).

5.2.2 Customer Indicators

The following section will describe some of the most renowned customer indicators of operational risk in a Retail Bank (see fig 5.2).

5.2.2.1 Customer complaints

The number of customer complaints for a specific time, for example, one month can also indicate the exposure to operational risk. Customer complaints in an operational risk context are the complaints regarding employees and the standard of their work (efforts), in other words, the quality and effectiveness of their work

5.2.2.2 Repeat business vs. New business

The higher the number of repeat business, the lower the exposure to operational risk will be because all the necessary documentation is already in place and all the customer's details are already known so it lowers the bank's administration work. With new business the cost (risk) is higher because, for example, actions must be taken to acquire the customer's details, and thus it increases the banks administration efforts, which in turn, increases the exposure to operational risk.

5.2.2.3 Application turnover time (customer satisfaction)

As Cade (1997: 213) stated, it must be one of the objectives of the bank to keep the application turnover time as low as possible, in other words the customer satisfaction as high as possible. If the application turnover time is high and the customer satisfaction is low, it can increase the exposure to operational risk.

5.2.2.4 Customer satisfaction survey

In addition to the application turnover time, a survey can be done to provide the bank with information regarding customer satisfaction, which can also be an indicator of the exposure to operational risk. In other words, the exposure to operational risk could increase when there is a decrease in customer satisfaction.

5.2.2.5 Operating turnover

In addition to the above-mentioned indicators (see 5.2.2.3 and 5.2.2.4) of operational risk, a low operating turnover can also indicate the exposure to operational risk.

Operating turnover include, for example, how long a client must wait before he or she receives his or her statement at the end of the month.

5.2.2.6 Aged confirmations

The longer the client must wait for confirmation of a deal, the lower the operating turnover will be and the lower the customer satisfaction (also see 5.2.2.4 and 5.2.2.5), which will increase the exposure to operational risk.

5.2.2.7 The number of cross selling²

The higher the number of cross selling, the higher the exposure to operational risk.

5.2.2.8 Increase/decrease in the number of customers

If there is an abnormal increase or decrease (a more than usual decrease or increase) in the number of customers in a specific time, for example one month it can be an indication of some irregularities, which increases the exposure to operational risk.

5.2.3 Product indicators

Product indicators are the third category of operational risk indicators and will be evaluated in the following section.

5.2.3.1 Product complexity

The more complex a bank product is, the higher the operational risk will be, because the more complex a product is, the more difficult it becomes to monitor and control the product (Crouhy et al, 1998: 202).

² Cross selling is when a bank sells more than one product to the same client at the same time, for example a home loan as well as a cheque account.

5.2.3.2 Range of products

The more complex/large the range of products is, the higher the exposure to operational risk will be, because it is difficult to monitor and control a complex and large range of products. The more complex/large the range of products is the more the employees will be exposed to operational risk, because the burden on them will be higher to control and monitor such a range of products.

5.2.3.3 Number of settlement fails

The number of settlement fails per geographic area is also a good indication of operational risk. A settlement failure can be as a result of the incorrect documentation of a certain transaction (for example, a document that need a signature, or incomplete documentation).

5.2.3.4 Non-performance with compliance with policy

If a product does not comply with the bank's overall policy (Board's policy), it can also increase the exposure to operational risk.

5.2.3.5 The number of new accounts opened

An abnormal (more than usual) amount of new accounts (products) opened per month can also be an indication of a potential operational risk. The more accounts are opened in one month the more difficult it becomes for the management to monitor and control them, thus it increases the management's exposure to operational risk. Also, if there is an abnormal increase in the number of accounts opened, it will higher the burden on employees, in other words, will also increase the employee's exposure to operational risk.

5.2.3.6 The number of accounts closed

In addition to the above-mentioned, the number of accounts closed per month can also be an indication of a potential operational risk. For example, if there is an abnormal

amount of accounts closed per month it can be an indication of potential operational risk.

5.2.3.7 Increase in the number of lost and stolen ATM (credit cards) cards

The higher the number of lost and stolen cards, the higher the burden on employees, because they must provide new cards at the same rate at which the cards are lost, thus, it increases the employee's exposure to operational risk.

5.2.3.8 The total number of active credit card accounts

This will provide risk managers with insight into the exposure of operational risk faced by the card division. The higher the number of active credit cards there are, the more difficult it will become to monitor and control them. This will also increase the exposure to operational risk by the employees of a card division.

5.2.3.9 Total applications received vs. total applications approved

The total number of applications received versus the total number of applications approved can also be an indication of operational risk. The total number of applications received should be relative equal to the total number of applications approved (Serfontein, 2003).

5.2.3.10 Total applications denied

In addition to the above-mentioned indicator (see 5.2.3.10), the number of applications denied in a specific time (for example one month) could also be an indication of operational risk. If there is an abnormal (more than the usual) increase/decrease in the number of applications denied, it can increase the exposure to operational risk, or can be an indication of the exposure of operational risk.

5.2.3.11 Increase in the number of transactions

An increase in the number of transactions that, when it increases, causes an increase in the number of erroneous transactions, which in turn, increases the exposure to operational risk.

5.2.4 System indicators

System indicators are the fourth category of operational risk indicators in a Retail Bank and will be evaluated in the following sections. System indicators are usual related to the IT system, in other words related to computers, computer software, telecommunications, information systems, etc.

5.2.4.1 IT-system downtime

The longer an IT-system is down, the more likely a system-related error will occur, thus the higher the exposure to operational risk.

5.2.4.2 Number of hacking attempts detected

The number of hacking attempts per specific time frame (for example one month) could also highlight the relative exposure to operational risk. Nowadays banks rely more and more on the IT system and almost three-quarters of banks transactions are IT related. But, with an increase in the number of IT-transactions, the number of hacking attempts also increases and should therefore be one of the most significant system indicators of operational risk.

5.2.4.3 Number of points of entry into the system

In addition to the above-mentioned indicator (see 5.2.4.2), the number of points of entry into the system in a specific time (for example one month) could also be an indication of the exposure to operational risk.

5.4.2.4 Number of system problems detected

The higher the number of system problems detected in a specific time frame (for example one month), the higher the exposure to operational risk. The higher the number of system problems detected, the higher the probability of a system-related error, thus the higher the exposure to operational risk.

5.4.2.5 Intranet between branches

An insufficient intranet between branches can result in the inadequate flow of information between branches. If there is an ineffective flow of information between branches, the management of these branches will be more exposed to operational risk.

5.4.2.6 Number and value of Internet transactions

The higher the number and value of internet transactions, the higher the exposure to operational risk will be, because a higher number and value of Internet transactions will result in an increase to the value at risk (VaR) of Internet transactions. The higher the number and value of internet transactions the more difficult it will become to monitor and control these transactions and thus it will increase the exposure to operational risk.

5.2.5 Other indicators of operational risk

Other indicators of operational risk are regarded the fifth category of operational risk indicators in a Retail Bank and include all the indicators that do not fall under one of the four above-mentioned categories. The following sections will evaluate and describe some of these indicators of operational risk.

5.2.5.1 Number of incidents of fraud

The number of fraud incidents can also be an indicator of operational risk. The higher the number of fraud incidents, the higher the burden on employees, thus it will also increase the employee's exposure to operational risk.

5.2.5.2 Number of critical/unacceptable ratings/findings received from completed audits

The information from completed audits regarding critical/unacceptable ratings/findings could highlight the exposure to an operational risk.

5.2.5.2 Concentration of activities (transactions)

Concentration risk – too much invested in one sector, asset class or geographic region. Yam (1998: 544) mentioned that with more activities concentrated in one sector, the higher the exposure will be for concentration risk, which will then also increase the exposure to operational risk. Yam (1998: 569) also mentioned that fifty institutions (this number include banking and non-banking institutions) failed during 2000-2002 in the USA as a result of too much activities concentrated in one sector.

5.2.5.3 Movement in market share

An abnormal (more than usual) decrease or increase in the bank's market share (for example, in vehicle finance) could highlight the exposure to operational risk.

5.2.5.4 Percentage movement in the total book value

An abnormal (more than usual) decrease or increase in total book value, which can also highlight the exposure to operational risk (for example vehicle finance).

5.2.5.5 Number and value of physical losses

The number and value of physical losses at a bank (in a specific time frame) can also be an important indicator of operational risk in a Retail Bank. Physical losses can be as a result of, accidents, vandalism, Acts of God (for example floods, hurricanes), theft, etc.

The above-mentioned sections then include a short evaluation on some of the indicators of operational risk in a Retail Bank. Part of the evaluation of these indicators is to determine their viability in a Retail Bank environment and will be done by means of handing out questionnaires. These questionnaires were handed out to some key players in operational risk management in the South African banking environment. But before this chapter can proceed and provide the results of these questionnaires, it is important to first provide a short background on how a questionnaire is designed.

5.3 Practical guidelines on designing a questionnaire

As mentioned above, questionnaires were handed out to the key players in operational risk management in the South African banking environment to analyse the viability of the above-mentioned key indicators of operational risk. This section will provide a short overview on how a questionnaire must be designed and also provide the basic elements of a questionnaire in order to better understand the designing of the above-mentioned questionnaire on the key indicators of operational risk.

Figure 5.4 is an extract of the questionnaire³ that was used in this study to determine the viability of the identified key indicators of operational risk in a Retail Bank (see 5.2).

³ The results of these questionnaire will be evaluated in a later section of chapter 5.

Figure 5.4 Questionnaire on operational risk indicators

Key Operational Risk Indicators: Retail Division of a South African Bank

Please answer the following questionnaire by indicating your choice by marking the appropriate block with a cross (X).

Note!!

It is important to keep in mind that the explanation provided for each indicator must not influence the rating of the indicator, but it is mere intended to place the indicator in its proper context. Some of the indicators may be wrongly recognized as indicators of other banking risks, for example credit risk, and it is for this reason that each indicator must be explained to distinguish it from other banking risk indicators and to place it in an operational risk context.

1. Employee Indicators:

1.1 Employee turnover: Employee turnover is the rate at which new employees are leaving and joining the bank. The higher the employee turnover, the more time must be spent on training new employees

Indicator

| | | | | | | | |
|---|---|---|---|---|---|---|--|
| | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | |

Not Important Important

1.2 Overtime worked by employees: The more overtime an employee work, the more likely he will make a mistake, for example, if he works fifteen ours a day, the last four hours of the day he is likely to make more mistakes because of the fact that he is more tired and his concentration levels are low.

Indicator

| | | | | | | | |
|---|---|---|---|---|---|---|--|
| | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | |

Not Important Important

1.3 Vacation and absenteeism rate: If personnel are required to take fourteen days leave per year, the risk indicator will be the personnel who haven't taken fourteen days leave. (If an employee do not take fourteen or more than fourteen days leave, he will be more likely to suffer from work related stress, tiredness, etc.)

Indicator

| | | | | | | | |
|---|---|---|---|---|---|---|--|
| | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | |

Not Important Important

1.4 Number of approved positions vs. Actual Commitment: The personnel manager must decide if the employment of a new employee will be beneficial for the bank, for example, he must ask himself if there will be enough funds available to pay this employee and if there will be enough work to keep the employee busy.

Indicator

| | | | | | | | |
|---|---|---|---|---|---|---|--|
| | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | |

Not Important Important

Source: (Compiled by the author)

5.3.1 Background on designing a questionnaire

The following section will provide a short overview on the effective construction/designing of a questionnaire. The same guidelines were used to design the above-mentioned questionnaire (see fig 5.4).

5.3.1.1 The purpose of a questionnaire

Steenkamp (1984: 3) stated that the first thing to consider when designing a questionnaire is to highlight the purpose/aim of the questionnaire. It is also important to distinguish between the purpose/aim of the questionnaire and the purpose/aim of the study (research). The main aim of a questionnaire must be therefore to acquire information from the public, or in other words, "its function is measurement" (Oppenheim, 1966: 24). One of the biggest problems with a questionnaire is that there is not always a well-defined purpose/aim, and many questionnaire-users do not always know what they want to achieve with a questionnaire (Oppenheim, 1966: 24).

Steenkamp (1984: 3) also stated that it is important that every questionnaire must have a proper problem statement, because if there is not a problem statement, it will not be necessary to design a questionnaire, in other words, the question must be asked that what does the researcher want to achieve with his or her questionnaire? As Oppenheim (1966: 3) stated, "we cannot judge a questionnaire as good or bad, efficient or inefficient unless we know what job it was meant to do". Therefore, a good questionnaire always starts with a thorough evaluation of its purpose/aim; in other words, a questionnaire must provide answers to a problem statement.

5.3.1.2 The environment of the respondent

Steenkamp (1984: 4) stated that the second important thing to consider when designing a questionnaire is to evaluate the environment of the respondent. It is important to keep in mind that facts that are familiar to the person, who is constructing the questionnaire, will not always be familiar to the respondent (Steenkamp, 1984: 4). The person that is constructing a questionnaire must ensure that the subject, concepts, and idea are known to all the respondents in his sample.

5.3.1.3 Data gathering

The third important fact to consider when designing a questionnaire is that basic principles must be set regarding the manner in which data is gathered (Steenkamp, 1986: 5). When designing a questionnaire, it is important that the personnel responsible for designing the questionnaire must know whether the questionnaire will be done over the telephone, by mail, via the Internet or by means of personal interviews. Steenkamp (1986: 5) stated that the technique of data gathering is direct related to the development of a questionnaire. The above-mentioned sections were intended to provide some background regarding the designing/development and construction of a questionnaire; the following section will provide a short overview on the typology of a questionnaire.

5.3.2 The typology of a questionnaire

Steenkamp (1984: 6) stated that there are four basic reasons for the use of a questionnaire (types of questionnaires), which is illustrated in figure 5.5 and include the following:

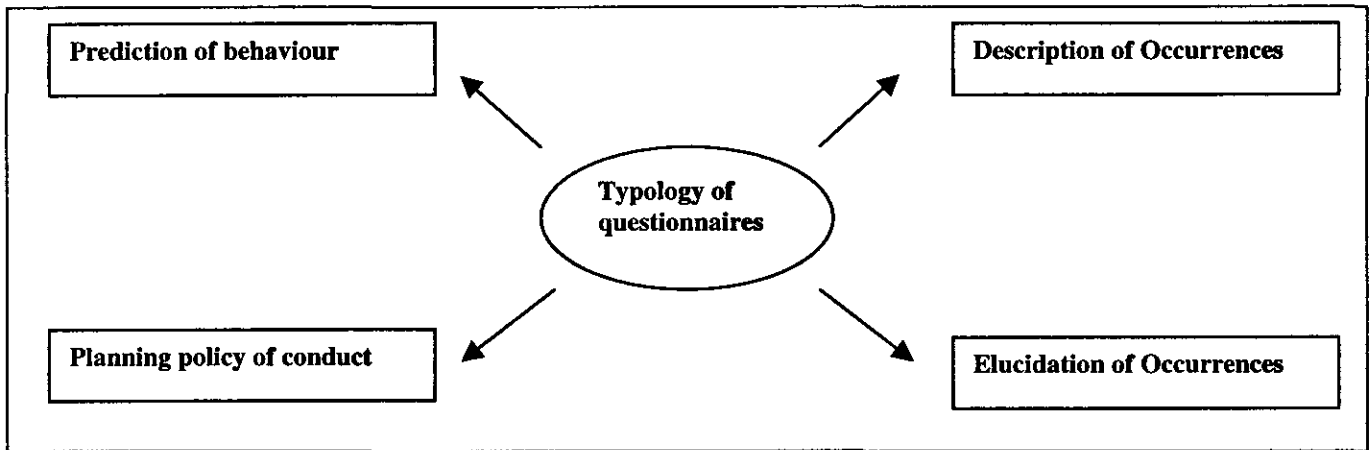
- Description of occurrences.
- Elucidation of occurrences.
- Planning the policy of conduct.
- Prediction of behaviour.

5.3.2.1 Description of the occurrences

The first and maybe the most common reason for designing a questionnaire is the need for an explanation of a specific situation or occurrence (Oppenheim, 1966: 8-9). There are two factors that play a fundamental role in this, which is categorising and establishing the frequencies of incidents/occurrences. The type of data that is gathered is regarded as sociographical data, for example the need to know the number of people using a bus services, the number of people living in houses or in apartments,

the number of people that is depended on health organisations, or the number of children per family of a specific population group, etc.

Figure 5.5 The typology of a questionnaire



Source: (Steenkamp, 1984: 5)

5.3.2.2 Elucidation of occurrence

When a particular situation, feature or process needs to be declared in a society, the researcher is depended on a theoretical approach, which will lead to a specific hypothesis⁴, which is the second most common reason for designing a questionnaire (Steenkamp, 1984: 8). Referring back to the bus-example (see 5.3.2.1), the person who is conducting the research need more than just the amount of people and more than just an evaluation of the their sex, age, etc. A questionnaire that is based on elucidation is not so different from those that are based on description, except that more variables are used and that the question and answer possibilities may be more focussed on specific behaviour patterns.

With a questionnaire that is based on elucidation it is important to place proper emphasis on the motivations, views, and attitudes of the researcher and also on the people in his survey sample. This will focus the attention on the third type of questionnaire, which is a questionnaire that is based on the development/planning of the psychological policy.

5.3.2.3 Planning/determining of the policy

A questionnaire that aims to obtain information based on changing policies or behaviours can be regarded as social-psychological questionnaires and is the third type of questionnaire (Steenkamp, 1984: 9). Social psychology plays an important role, because the planning of psychological policies is based on attitudes and the view of the public regarding the given situation. When designing a questionnaire that aims to determine the attitudes and behaviour of the public by focussing on the views, reactions and behaviour of an individual, it is moving the attention of the questionnaire more forward towards the Psychological environment⁵.

5.3.2.4 Predicting of behaviour

These types of questionnaires are often called test, which include I.Q.-, ability-, adaptation capability-, and other similar psychometric test (Steenkamp, 1984: 9). It sometimes takes years to develop such a questionnaire, because with these questionnaires⁶ every answer must be almost complete and must provide accurate data regarding the respondent's I.Q, adaptation capability, and ability.

The above sections were only intended to provide a short background on the designing of a questionnaire, the following section will continue the discussion on the design of a questionnaire by evaluating the question content and phrasing.

5.3.3 Question content and phrasing

The following aspects of question content and phrasing have to be considered when designing a questionnaire (Martins et al, 1996: 216):

- The question must be kept as concise as possible. The fewer the words, the more evident the core of the question.

⁴ A hypothesis can be defined as a proposal that there is a specific connection between two or more than two compositions (Steenkamp, 1984: 8)

⁵ The social psychologists that played an integral role in developing this type of questionnaire include, Thurstone, Allport, Likert, Osgood, and Coombs (Steenkamp, 1984: 9).

- The answer required has to be definitive.
- In survey conducted amongst all levels of the population the questions should be worded in such a way that even the less sophisticated and less educated can understand them (see 5.3.1.2).
- It is important that the questions are simple.
- Leading questions must be avoided. A leading question is one that prompts a desired answer.
- It is important to ensure that the respondent has the relevant information and is able to answer the question. Respondents have been known to answer questions even when they have no opinions on the subject.
- Questions that may embarrassed the respondent must be avoided as far as possible. In such questions it is advisable to use a third-party approach to the problem by citing a hypothetical situation with imaginary characters.

Martins et al (1996: 219) mentioned that an understanding of the above-mentioned issues is essential if the question is to be framed successfully without oversimplifying or omitting certain aspects. In addition to the above-mentioned, Martins et al (1996: 219) stated that the questions, besides from not being mathematically testable in exclusion from the survey, are also influenced by grammar, word choice, length and punctuation and also by its position in the questionnaire. Finally, the question stands or falls by whether it elicits the information required in the survey, and it is here that pre-testing plays a key role (Loubser & Gilmour, 1991: 4). The following section will further the discussion on the development/designing of a questionnaire by evaluating the question sequence of a questionnaire.

5.3.4 Question sequence of the questionnaire

Loubser and Gilmour (1991: 4) stated that structured questions have the advantage that a good interviewer will read the questions aloud in their exact wording and sequence in the questionnaire. Thus all the respondents are asked the same questions in exactly the same order. By arranging the questions logically and observing other sequencing rules the researcher enhances the standard of interviewing, helps the

⁶ Examples on these types of questionnaires can be seen in Van den Berg (1983) and Van den Berg &

interviewer and induces a logical and harmonious flow of thought in the questionnaire.

Martins et al (1996: 219-220) sated that the following points must receive thorough consideration:

- The first question should be simple and interesting, its main intention being to put the respondent at ease and motivate him to react to the succeeding questions without suspicion.
- It is important to indicate which respondents have to answer which questions.
- Ensure a logical sequence of questions.
- Position sensitive questions or questions on embarrassing subjects as near to the end of the questionnaire as possible.
- Questions requiring classification information, such as those on age, income and marital status, may also be sensitive and should also be as near as possible to the end of the questionnaire.
- It is important to ensure that structured answers to a question do not provide respondents with answers to questions lower down in the questionnaire.

Particularly in questionnaires designed for opinion surveys it may be worthwhile to consider the following sequence of questions, suggested long ago by the famous Gallup (1947: 201) and are still valid:

- Questions to ascertain the extend of the respondent's previous thinking, if any on the subject.
- Open-ended questions to derive the respondent's general feelings on the subject.
- Questions, often multiple choice, aimed at electing specific information.
- Questions aimed at discovering the reasons for the views given in answers to the above-mentioned.
- Questions to determine how strongly held those views are.

Vorster (1982).

The above section then concludes the discussion on the question sequence of a questionnaire. The following section will continue the discussion on the development/designing of a questionnaire by evaluating its question/respond format.

5.3.5 The question format of a questionnaire

Martins et al (1996: 220) stated that structured questions with structured or unstructured responses are most commonly used in marketing research. The questionnaire that is used in this study is based on a structured question/structured response format, therefore the following section will evaluate the designing of a questionnaire that is based on a structured question/structured response format. Martins et al (1996: 220) stated seven types of structured questions, which include the following:

- Dichotomous questions.
- Multiple-choice questions with single answers.
- Multiple-choice questions with multiple answers.
- Checklists.
- Rankings.
- Grids.
- Scaled questions.

The following section will provide a short overview on the above-mentioned types of structure questions.

5.3.5.1 Dichotomous questions

The dichotomous question is a question which offers only two fixed alternative answers to choose from, for example Yes/No, Male/Female, Agree/Disagree (Martins et al, 1996: 221).

5.3.5.2 Multiple-choice questions with single answers

The multiple choice or multichotomous question is also a fixed-alternative question but it offers more than two fixed-alternative answers (Steenkamp, 1984: 12). Response is restricted to one of the given alternatives. These types of questions are used when information is classified into fairly fixed categories, or when the respondent's thoughts are deliberately channelled in a certain direction. Figure 5.6 is an example of multiple-choice question with a single answer.

Figure 5.6 Multiple-choice questions with single answers

| | |
|---------------------|--------------------------|
| 1. How old are you? | (Please tick) |
| Under 20 | <input type="checkbox"/> |
| 20 – 29 | <input type="checkbox"/> |
| 30 – 39 | <input type="checkbox"/> |
| 40 and over | <input type="checkbox"/> |

Source: (Martins et al, 1996: 221)

5.3.5.3 Multiple-choice questions with multiple answers

Steenkamp (1984: 14) and Martins et al (1996: 222) stated that this type of question allows for more than one response. Figure 5.7 is an illustration of an example of a multiple-choice question with multiple answers.

Figure 5.7 Multiple-choice questions with multiple answers

| | |
|--|--------------------------|
| 1. Which of the following brands of cigarettes have you ever smoked? | (Please tick) |
| Ransom select | <input type="checkbox"/> |
| Peter Stuyvesant | <input type="checkbox"/> |
| Rembrandt van Rijn | <input type="checkbox"/> |
| Lexington | <input type="checkbox"/> |

Source: (Martins et al, 1996: 222)

5.3.5.4 Checklists

A checklist typically lists a product's or person's attributes, which the respondent is, required to rate in terms of given criteria that have to be related in accordance with their importance or applicability (Martins *et al*, 1996: 222). Usually a checklist is complete with the aid of a prompt card⁷.

5.3.5.5 Rankings

In the rank order method the respondent is asked to rank a set of items in terms of a given criterion (Steenkamp, 1984: 15). For example, the interviewer gives the respondent a list and says: "here is a list of motorcar characteristics that motorists have mentioned to use. Please rank them in what you consider their order of importance, marking the most important as 1, etc." Respondents may be inclined to rate characteristics near the top of the list higher than those lower down. To obviate this each characteristic may be shown on a separate card. Macfarlane Smith (1972: 77) suggests limiting the number of characteristics to six, whereas Oppenheim (1966: 98) suggested a maximum of ten.

5.3.5.6 Grids

Martins *et al* (1996: 223) stated grids as the sixth type of structured questions that is commonly used in questionnaires. A grid is a simple and straightforward means of collecting information quickly and analysing it in various ways. Figure 5.8 is an illustration of a grid questionnaire. The overall frequency tabulation will immediately show for example which foods were eaten at each meal and whether a specific kind of food was eaten at one or more meals. In this way the researcher can explore the use of particular items without the respondent knowing which they are. Here, for example, we may be interested in the respondent's eating habits only in so far as eggs are concerned.

⁷ A prompt card is a card, which lists the possible answers to a question.

Figure 5.8 Grids

Which of the following types of food did you eat yesterday at each meal?

| Meals | Bread | Mutton | Bacon | Pork | Beef | Eggs | Fish | Cheese | Chicken |
|-----------|-------|--------|-------|------|------|------|------|--------|---------|
| Breakfast | | | | | | | | | |
| Dinner | | | | | | | | | |
| Supper | | | | | | | | | |
| Other | | | | | | | | | |

Source: (Martins et al, 1996: 223)

5.3.5.7 Scaled questions

Steenkamp (1984: 17) stated that this type of question the respondent is required to mark a point on the scale. It has the advantage that the response is recorded in the right of the page and a number of aspects are listed on the left, as illustrated in figure 5.4. There are five basic types of scaled questionnaires, which include the following (Martins et al, 1996: 224):

- Graphic rating scale.
- Semantic different scale.
- Stapel scale.
- Likert scale.
- Thurstone scale.

It is also important to mention that the questionnaire that is used in this study is also based on this type of questionnaire. This section then conclude the discussion on the different types of questionnaires and their characteristics, the following section will provide a short discussion on the importance of pre-testing.

5.3.6 Pre-testing

Pre-testing is essential if the researcher is to be satisfied that the questionnaire he has designed will perform its various functions in the interview situation (Martins *et al*, 1996: 232). Writing about the necessity for trying out a questionnaire beforehand and also for tabulating the answers to questionnaires, Churchill (1992: 357) mentioned that: “the researcher who avoids a questionnaire pre-test and tabulation of replies is either naïve or a fool. The pre-test is the most inexpensive insurance the researcher can buy to assure the success of the questionnaire and the research project”.

Obviously aspects that have been tested successfully in previous questionnaires need not to be retested (Churchill, 1992: 357). However when the questionnaire’s layout, the sequins of questions, the words, the branching instructions and the degree of difficulty of the questions, are new, everything must be tested. The pre-test must be administered among respondents who correspond to those among whom the survey is to be carried out. Great care must be taken that all strata of the target population are represented in terms of intellectual ability, training, knowledge of the subject and attitude of it (Churchill, 1992: 357). Martins *et al* (1996: 233) also stated that it is important to tabulate the results obtained in the pre-test. In this way the researcher can ascertain how the final tables will look and whether the information is really that needed to resolve the problem.

So far this chapter has proceeded from the point of view that the designer of the questionnaire has *carte blanche*⁸. However, the design process may start with a questionnaire drafted by the client, or the client may submit questions for inclusion in the questionnaire, or clients commissioning a multi-client or omnibus survey may all submit a certain number of questions for inclusion in the questionnaire. In such instances the researcher will probably suggest any adjustments he deems necessary and submit them to the client for approval (Martins *et al*, 1996: 233). Or at some stage, possibly just before the pre-test, he may submit the draft questionnaire to the client for comment and then make any changes agreed upon by both parties. A copy of the final questionnaire may also be submitted to the client as a matter of courtesy

⁸ *Carte blanche* means to start with a clean piece of paper.

(Martin et al, 1996: 233). Martin et al, (1996: 233) stated that there are no hard and fast rules, however, and in the most instances these matters are specified in the proposal for the study.

5.3.7 Conclusion

Section 3.5 was intended to provide some background on the designing and development of a questionnaire. It is important to realize, that when designing a questionnaire that questionnaires come in many shapes and sizes, depending on the information required, the target group and the survey method. To conclude this section it is important to state the three related goals with the designing of a questionnaire, which is (Martin et al, 1996: 233):

- All questionnaires are designed to achieve three related goals: maximise the relevance and accuracy of the data collected.
- To ensure the participation and cooperation of target responses.
- To facilitate the collection and analysis of the data.

To conclude this section it is important to state that the questionnaires that were used for this study were handed to operational risk managers in the specific business areas of a South African Retail Bank. The questionnaires used in this study are also different from the one used by Robert Heubner (see section 4.4.2). Robert Heubner used a 5 point Likert scale this study however will use a 7 point Likert scale.

5.4 Results of questionnaires on KRIs in a Retail Bank

As mentioned in a previous section, this section will provide the results of the questionnaires that were handed out to certain key role players in operational risk management in a Retail Bank. This chapter has identified some of the most renowned key indicators of operational risk (see section 5.2) and the aim of this section is to provide the viability of each of the identified indicators. The results of the questionnaires will be provided by means of rating the indicators between 1 and 7, where 1 is an indication of an indicator that is not important to operational risk

management in a Retail Bank and where 7 is an indication of an indicator that is very important or relevant to operational risk management in a Retail Bank. The results will also be given in terms of the average rating and the standard deviation. A standard deviation (SD) is an indication of how the results deviate from the average. **A high average and a small standard deviation is an indication of an indicator that is of high importance/relevance to operational risk management in a Retail Bank, whereas a small average and large standard deviation is an indication of a risk indicator that is of little to no importance to a Retail Bank.**

5.4.1 Employee indicators⁹

The following section will provide the results of some of the most renowned employee indicators of operational risk (also see section 5.2.1).

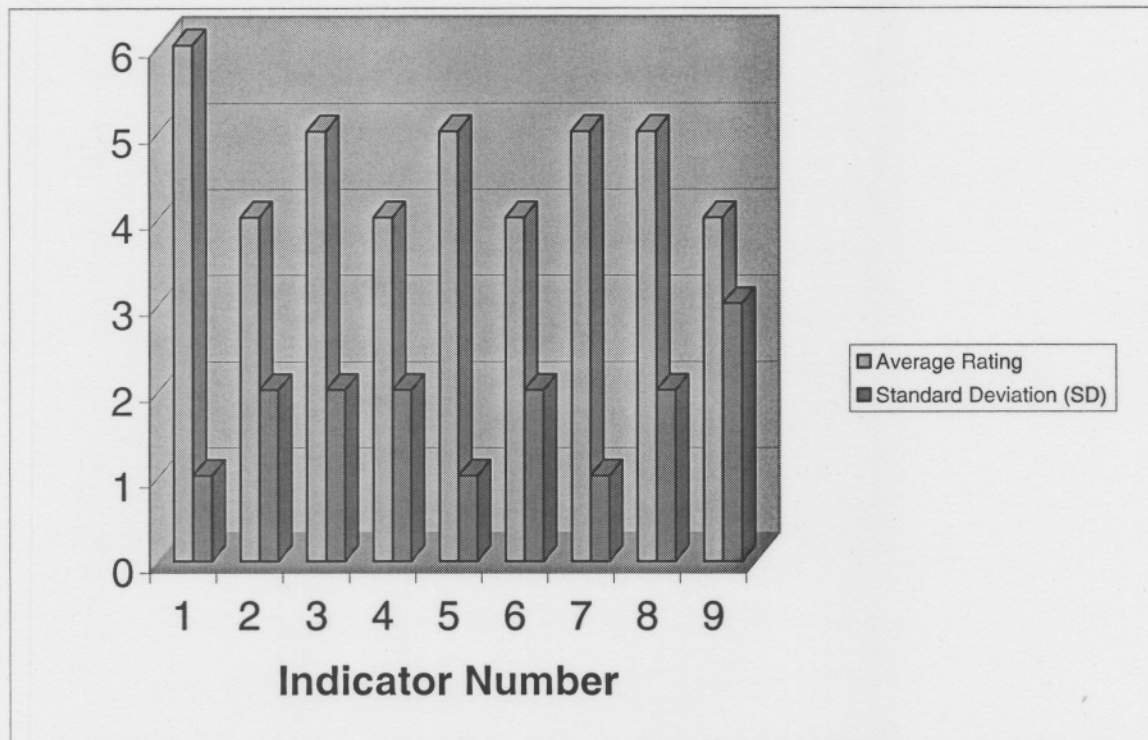
Table 5.1 Ratings of employee indicators¹⁰

| Indicator | Average Rating | Standard Deviation (SD) |
|---|-----------------------|--------------------------------|
| 1. Employee turnover | 6 | 1 |
| 2. Overtime worked by employees | 4 | 2 |
| 3. Vacation and absenteeism rate | 5 | 2 |
| 4. Number of approved positions vs. actual compliment | 4 | 2 |
| 5. Number of temporary personnel vs. Total number of personnel | 5 | 1 |
| 6. Junior/Senior staff tenure indicator | 4 | 2 |
| 7. Number of transactions per staff member | 5 | 1 |
| 8. Total for specific delivery failures | 5 | 2 |
| 9. Technology management control indicator | 4 | 3 |

Source: (Appendix: 207)

⁹ A thorough evaluation of employee indicators has been done in section 5.2

Figure 5.9 Ratings: Employee indicators



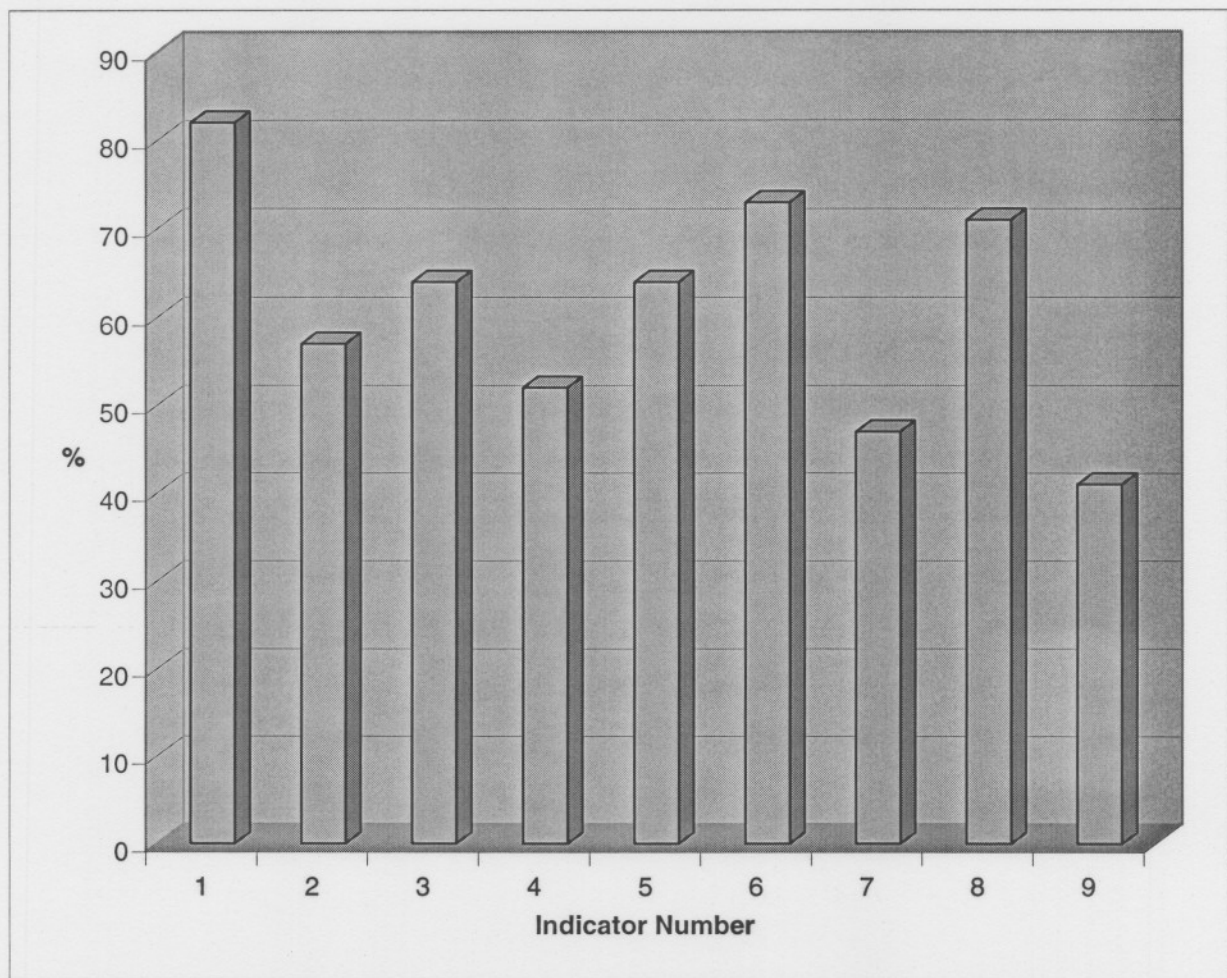
An average between 5 and 7 and standard deviation of $SD \leq 2$ is an indication of an indicator that is very important to operational risk management in a Retail Bank. From table 5.1 it can be seen that indicator 1, employee turnover, with an average of 6 and a SD of 1 is the most important employee indicator. The technology management and control indicator is the least important indicator, with an average of 4 and a SD of 3. Other relevant indicators include indicators 3, 5, 7 and 8 all with an average of between 5 and 7 and a SD of not more than 2. Figure 5.9 is an illustration of the average and the SD of each of the employee indicators.

As already mentioned in a previous section of this chapter, seventeen questionnaires were handed out to evaluate the importance of the indicators identified in section 5.2. Out of the seventeen questionnaires, 82 percent rated employee turnover as the most renowned employee indicators of operational risk in a Retail Bank. Figure 5.10 is an illustration of the importance of each indicator. A rating of 5 or more than 5 is an indication of an important indicator, therefore figure 5.10 is an illustration of how

¹⁰ The complete version of the results on employee indicators can be seen in the appendix.

many times an indicators has scored a rating of 5 or more than 5 out of the seventeen questionnaires.

Figure 5.10 Percentage rating: Employee indicator



The above section then concludes the discussion of the results on the employee indicators of operational risk. The following section will provide the results of the customer indicators of operational risk in a retail bank.

5.4.2 Customer indicators

Table 5.2 is an illustration of the ratings of the customer indicators of operational risk in a Retail Bank.

Table 5.2 Ratings of customer indicators

| Indicator | Average Rating | Standard Deviation (SD) |
|---|-----------------------|--------------------------------|
| 1. Customer complaints | 6 | 1 |
| 2. Repeat business vs. new business | 4 | 2 |
| 3. Application turnover time (customer satisfaction) | 5 | 1 |
| 4. Customer satisfaction survey | 5 | 2 |
| 5. Operating turnover | 4 | 2 |
| 6. Edged confirmations | 4 | 3 |
| 7. The number of cross selling | 5 | 1 |
| 8. Increase/decrease in the number of customers | 5 | 2 |

Source: (Appendix: 207)

From the above table it can be seen that indicator 1, customer complaints is the most relevant customer indicator of operational risk in a Retail Bank with an average of 6 and a SD of 1. The least relevant customer indicator of operational risk in a Retail Bank is indicator 6, aged confirmations with an average of 4 and a SD of 3. As mentioned, for an indicator to be relevant/important it must have an average of more than 5 and a SD of not more than 2. Other important/relevant customer indicators include indicators 3,4, 7 and 8 all with an average of more than 5 and a SD of not more than 2. Figure 5.11 is an illustration of the average rating and SD of each of the customer indicators.

As done in section 5.4.1, figure 5.12 will provide an illustration of the number of times an indicator has scored a rating of 5 or more than 5, and is illustrated in terms of a percentage, in other words how many times out of the seventeen a indicator has scored a rating of 5 or more than 5 (seventeen is the number of questionnaires the were handed out).

Figure 5.11 Ratings: Customer indicator

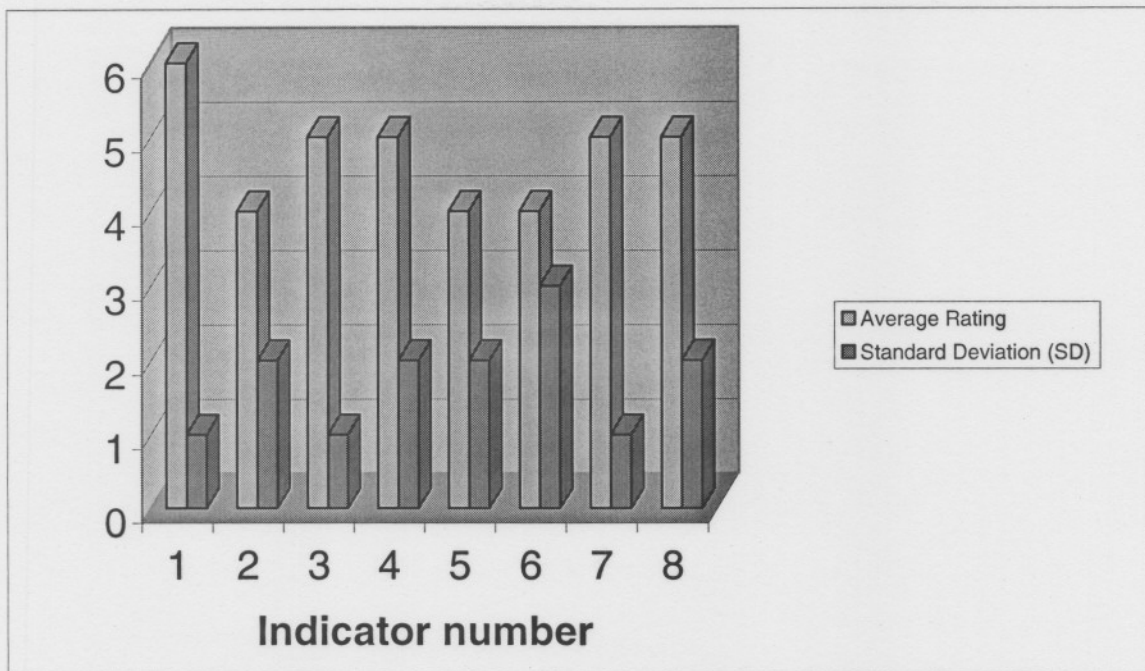
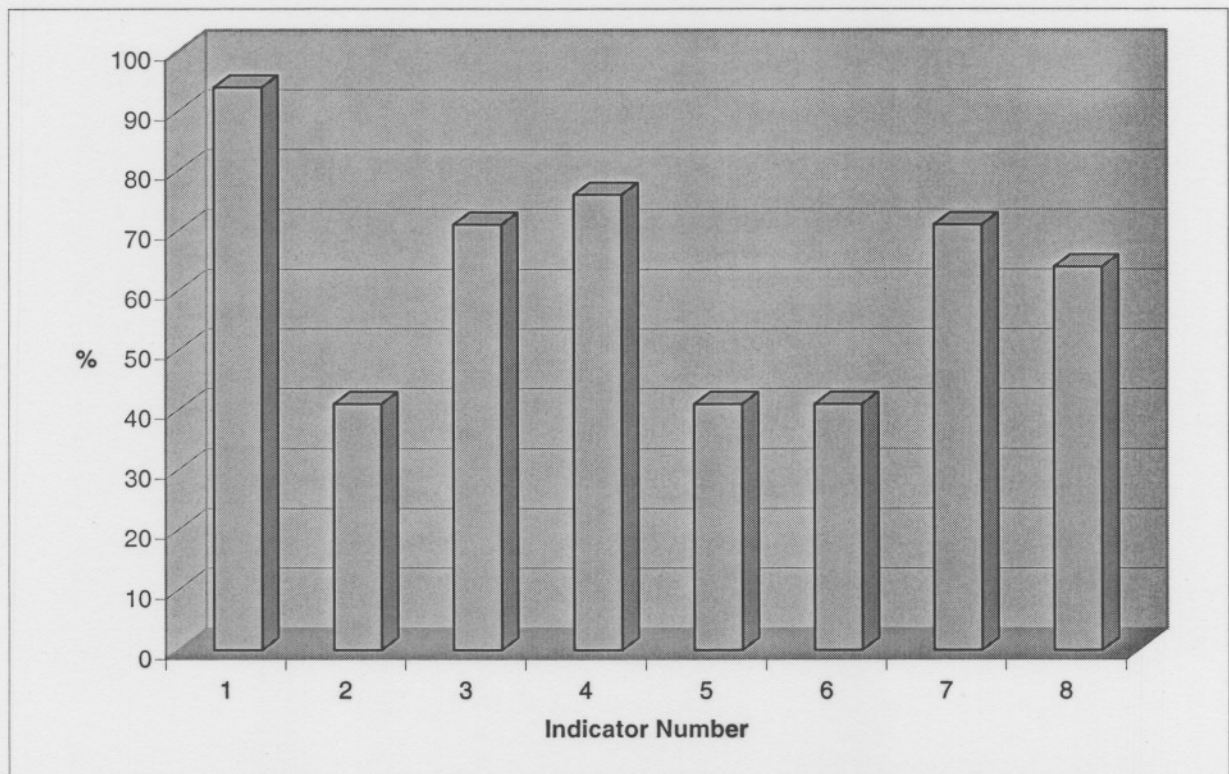


Figure 5.12 Percentage Rating: Customer indicator



5.4.3 Product indicators

Table 5.3 is an illustration of the ratings of the product indicators of operational risk in a retail bank.

Table 5.3 Ratings of product indicators

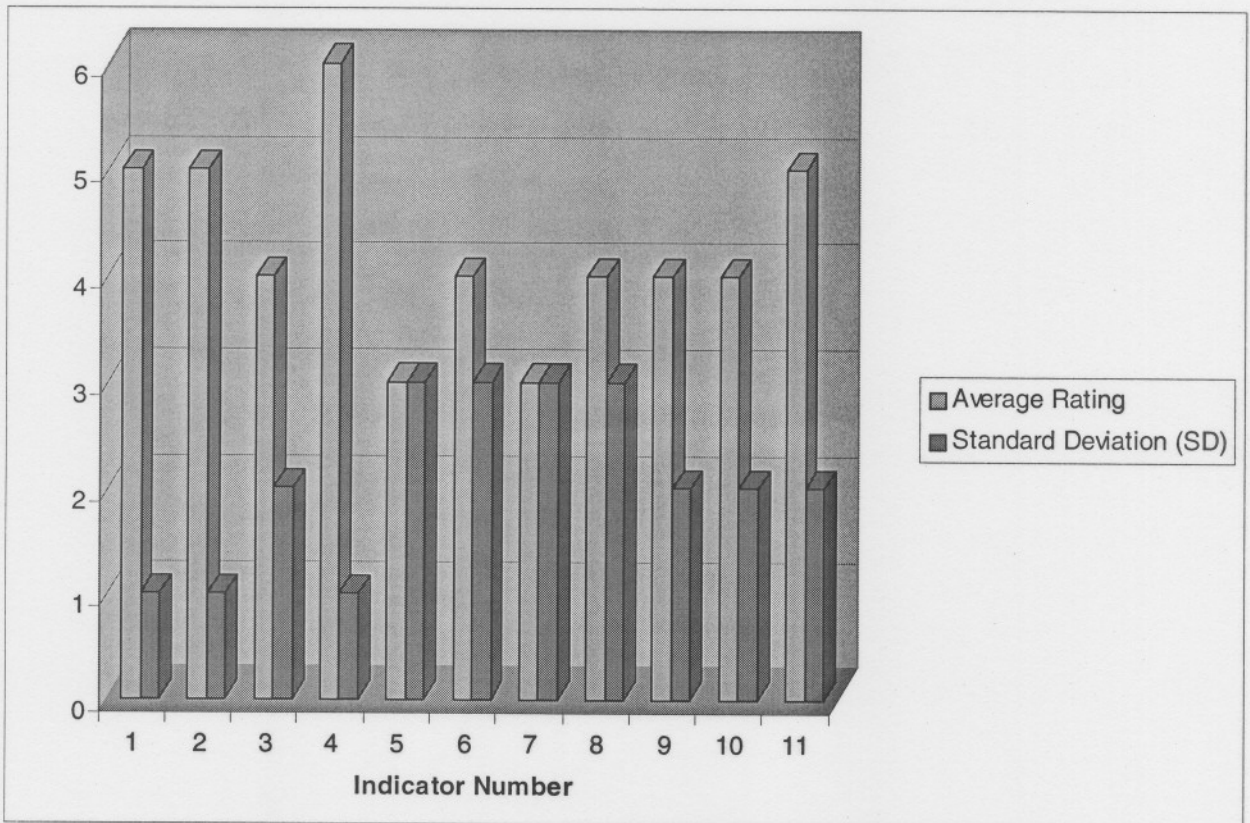
| Indicator | Average Rating | Standard Deviation (SD) |
|---|-----------------------|--------------------------------|
| 1. Product complexity | 5 | 1 |
| 2. Range of products | 5 | 1 |
| 3. Number of settlement fails | 4 | 2 |
| 4. Non-performance with compliance with policy | 6 | 1 |
| 5. Number of new accounts opened | 3 | 3 |
| 6. Number of accounts closed | 4 | 3 |
| 7. Increase in the number of lost/stolen ATM cards | 3 | 3 |
| 8. Number of active credit card accounts | 4 | 3 |
| 9. Total applications received | 4 | 2 |
| 10. Total applications denied | 4 | 2 |
| 11. Increase/decrease in transactions | 5 | 2 |

Source: (Appendix: 207)

From the above table it can be seen that indicator 4, non-performance with compliance to Board policy is the most relevant/important product indicator of operational risk in a Retail Bank, with an average of 6 and a SD of 1. The least relevant product indicator is indicator 7, the number of lost and stolen ATM cards, with an average of 3 and a SD of 3. As already mentioned in the previous sections, for an indicator to be relevant/important it is important that it's average rating must be 5 or more than 5 with a SD of not more than 2. Other important product indicators of operational risk in a Retail Bank include indicators 1, 2 and 11 each with an average

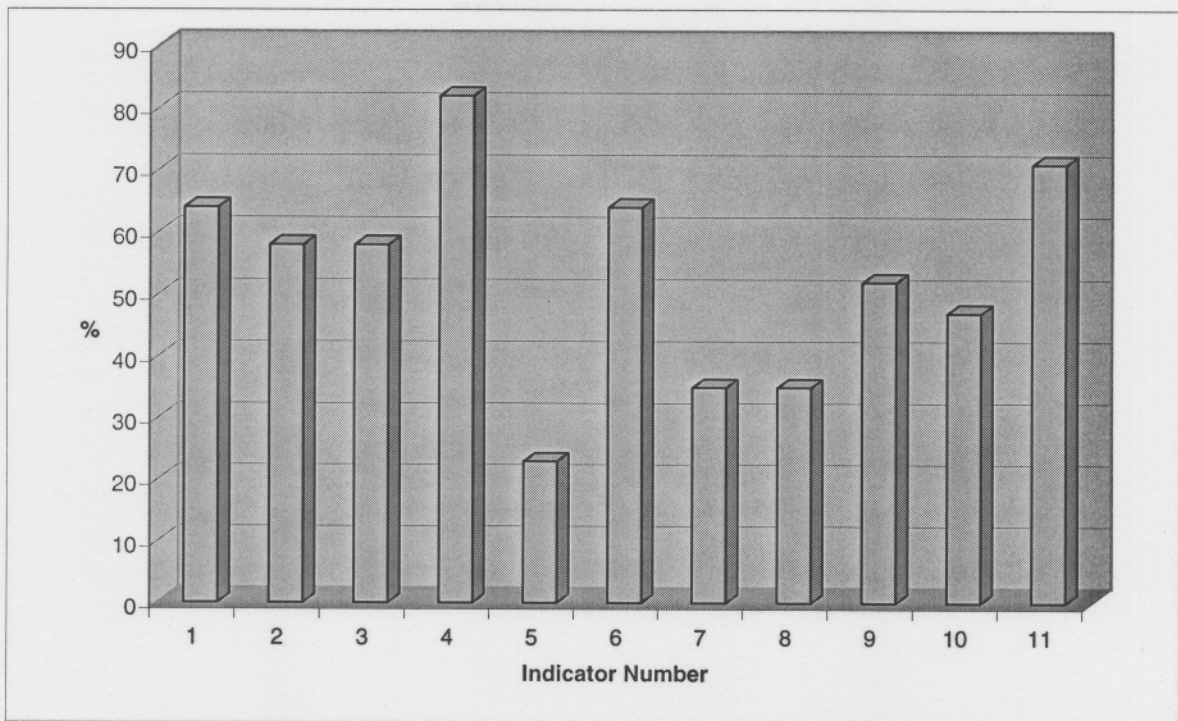
of 5 and a SD of not more than 2. Figure 5.13 is an illustration of the average and SD of each of the product indicators.

Figure 5.13 Ratings: Product indicators



As done in section 5.4.1 and 5.4.2, figure 5.14 is an illustration of how many times an indicator as scored a rating of 5 or more than 5. As seen in figure 5.14, indicator 4, non-performance with compliance with the board policy has scored a percentage of 82% out of the seventeen questionnaires a rating of 5 or more than 5, which makes it the most renowned product indicator. Other indicators with a high percentage includes indicators 1, 5 and 11 each with a percentage higher than 60.

Figure 5.14 Percentage rating: Product indicator



The above section then concludes the discussion on the results on product indicators, the following section will evaluate and discuss the results of the system indicators.

5.4.4 System indicators

Table 5.4 Ratings of system indicators

| Indicator | Average Rating | Standard Deviation (SD) |
|--|----------------|-------------------------|
| 1. IT System Downtime | 6 | 1 |
| 2. Number of Hacking attempts | 5 | 1 |
| 3. Number of points of entry | 5 | 2 |
| 4. Number of system problems | 6 | 1 |
| 5. Insufficient intranet | 4 | 2 |
| 6. Number and value of internet transactions | 4 | 3 |

Source: (Appendix: 207)

It can be seen from table 5.4 that indicator 1, IT system downtime and indicator 4, the number of system problems detected are the most renowned system indicators of operational risk identified in a Retail bank. As mentioned, for an indicator to be recognized as an important indicator, it must have an average rating of 5 or more than 5 and a SD of not more than 2. Both of the above-mentioned indicators fulfil these requirements. Other important indicators include indicators 2, 3, and 4 all with an average rating of 5 or more than 5 and with a SD of not more than 2. The least important system indicator is indicator 6, the number and value of Internet transactions, with an average rating of 4 and with a SD of more than 2.

Figure 5.15 is an illustration of the average rating and SD of each of the identified system indicators of operational risk.

Figure 5.15 Ratings: System indicators

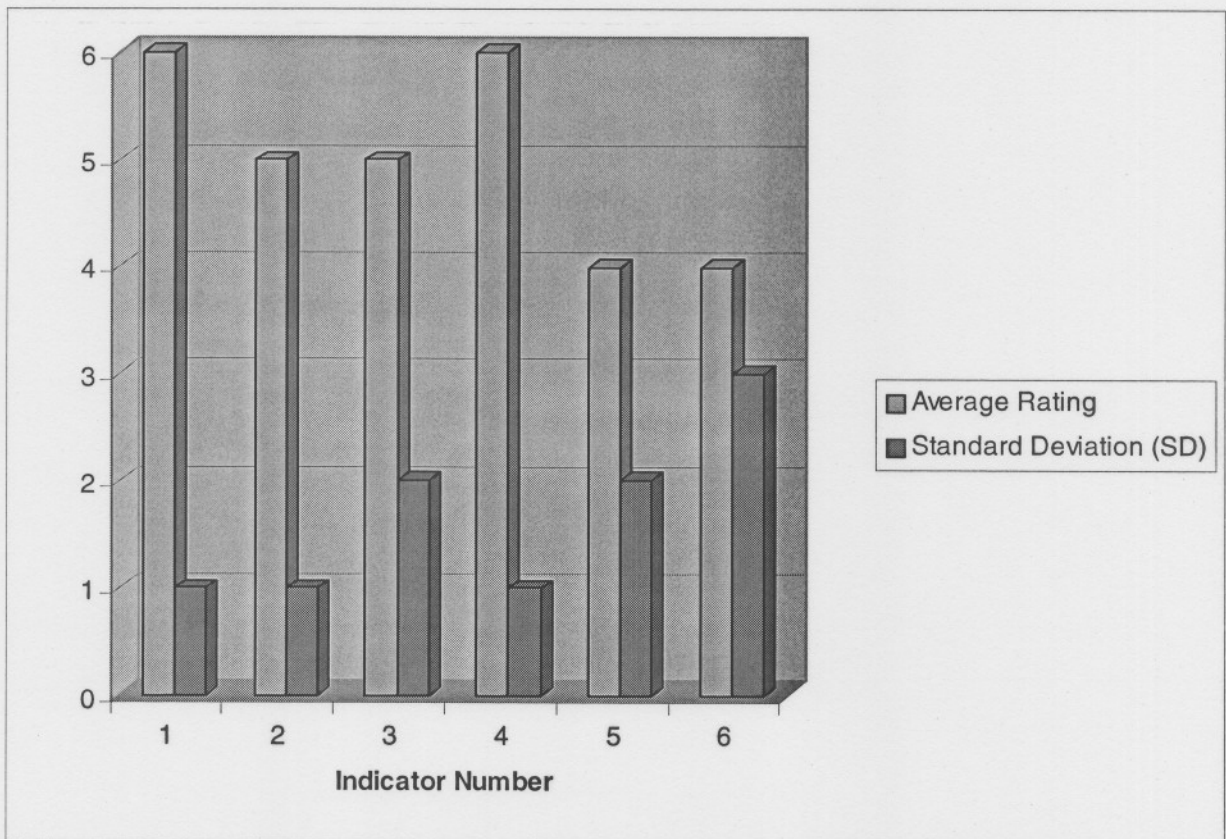
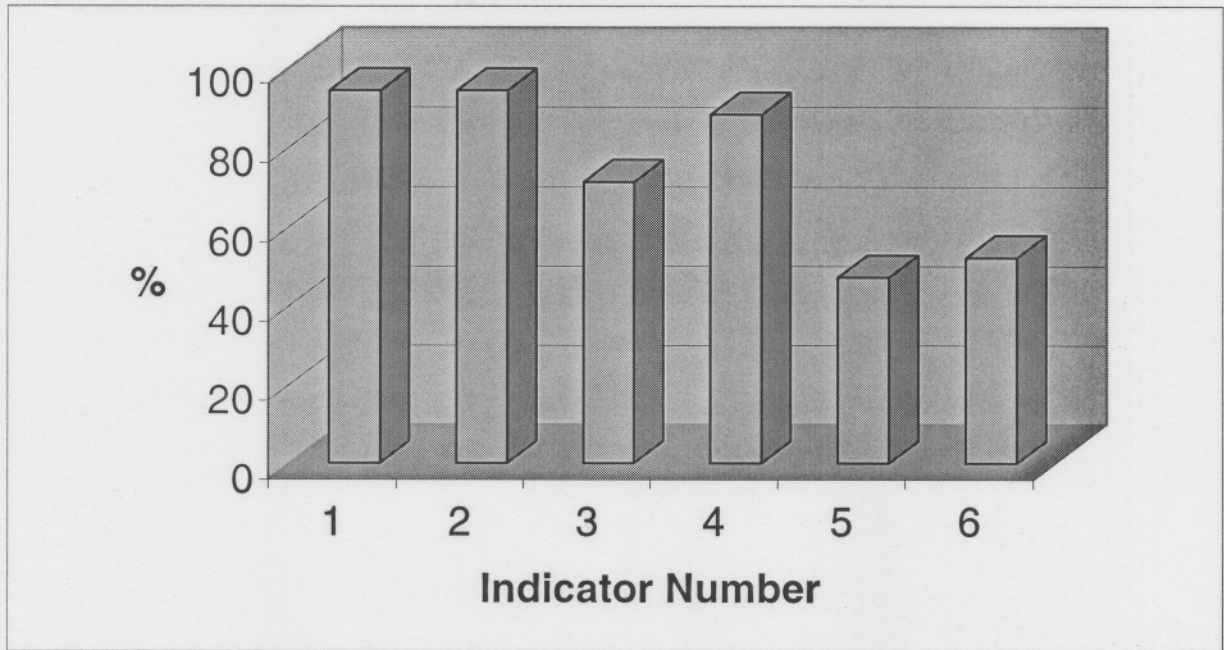


Figure 5.16 is an illustration of how many times a system indicator has scored a rating of 5 or more than 5 out of the seventeen questionnaires. For an indicator to be viable in operational risk management it is important that it has a rating of 5 or more than 5.

Figure 5.16 Percentage rating: System indicator



From the above figure it can be seen that indicator 1, IT system downtime and indicator 2, number of hacking attempts have scored the most times a rating of 5 or more than 5, which makes them the most renowned system indicators identified by chapter 5. The above then concludes the evaluation of the results of system indicators, the following section will evaluate and discuss the results of the other indicators of operational risk identified by chapter 5 (see section 5.2).

5.4.5 Other indicators of operational risk

As mentioned this section will evaluate and discuss the other indicators of operational risk identified by chapter 5, in other words, all the indicators that do not fall under employee, customer, product, or system indicators. Table 5.5 is an illustration of the average rating and SD of each of these indicators.

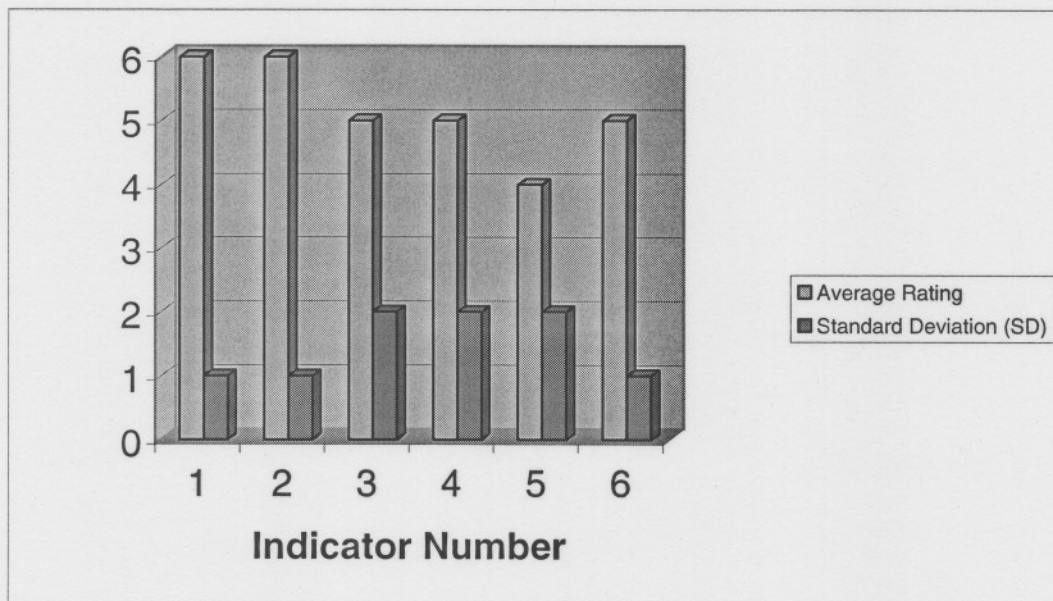
Table 5.5 Ratings of the other indicators of operational risk

| Indicator | Average Rating | Standard Deviation (SD) |
|---|----------------|-------------------------|
| 1. Number of incidents of fraud | 6 | 1 |
| 2. Number of critical/unacceptable ratings received from completed audits | 6 | 1 |
| 3. Concentration of activities | 5 | 2 |
| 4. Movement in market share | 5 | 2 |
| 5. Percentage movement in total book value | 4 | 2 |
| 6. Number and value of physical losses | 5 | 1 |

Source: (Appendix: 207)

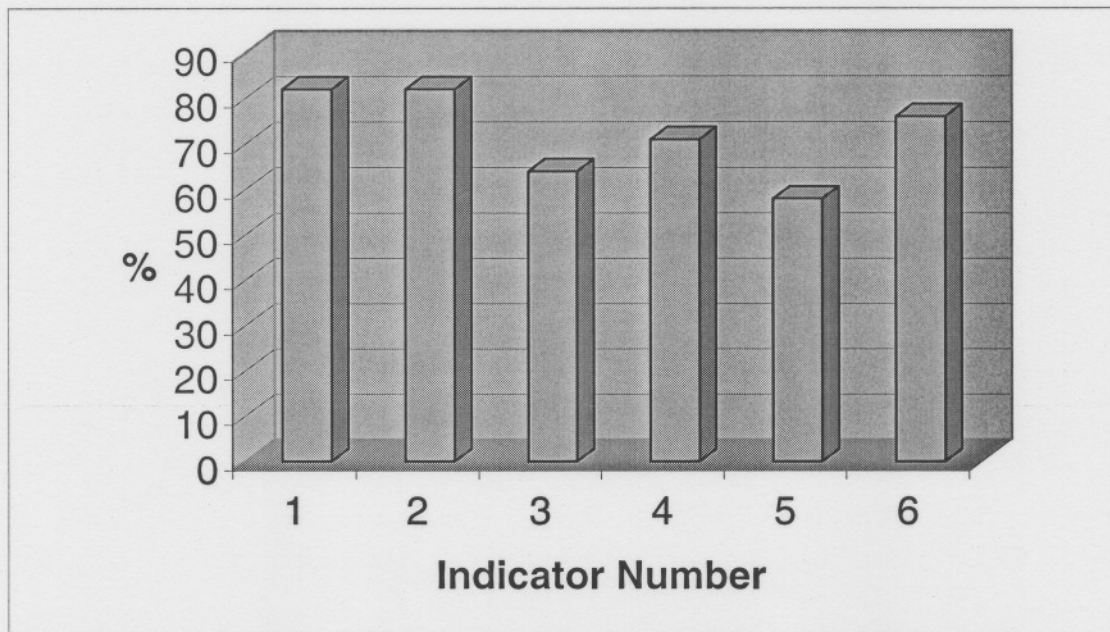
It can be seen from table 5.5 that indicators 1, the number of accidents of fraud and indicator 2, number of critical/unacceptable ratings received from completed audits are the most renowned, both with an average rating of 6 and a SD of not more than 2. Figure 5.17 is an illustration of the average rating and SD of the above-mentioned indicators.

Figure 5.17 Ratings: Other indicators of operational risk



As already mentioned in a previous section of chapter 5, for an indicator to be important in operational risk management, it must score a rating of 5 or more than 5, therefore the figure 5.18 is an illustration of how many times an indicator has scored a rating of 5 or more than 5.

Figure 5.18 Percentage rating: Other indicators of operational Risk



As seen in the figure 5.17, both indicators 1 and 2, the number of accidents of fraud and the number of critical/unacceptable ratings received from completed audits have scored a percentage of more than 80, which make them the most renowned other indicators of operational risk in a Retail Bank.

5.4.6 Overall results

To conclude the evaluation and discussion on the results of the questionnaires that were handed out to determine the viability of the identified indicators of operational risk in a Retail Bank, the following section will provide the overall results of the five different categories of operational risk indicators. Table 5.6 is an illustration of the overall average and SD of the five different categories of operational risk indicators.

Table 5.6 Overall ratings

| Indicator | Average Rating | Standard Deviation (SD) |
|------------------------|----------------|-------------------------|
| 1. Employee Indicators | 5 | 2 |
| 2. Customer Indicators | 5 | 2 |
| 3. Product Indicators | 6 | 2 |
| 4. System Indicators | 5 | 2 |
| 5. Other Indicators | 5 | 2 |

Source: (Appendix: 207)

From the above table it can be seen that the overall results (working on averages) are basically the same, except for product indicators with a higher average rating, which make it the most renowned category of operational risk identified by chapter 5. Figure 5.19 is an illustration of the above-mentioned results.

Figure 5.19 Overall ratings

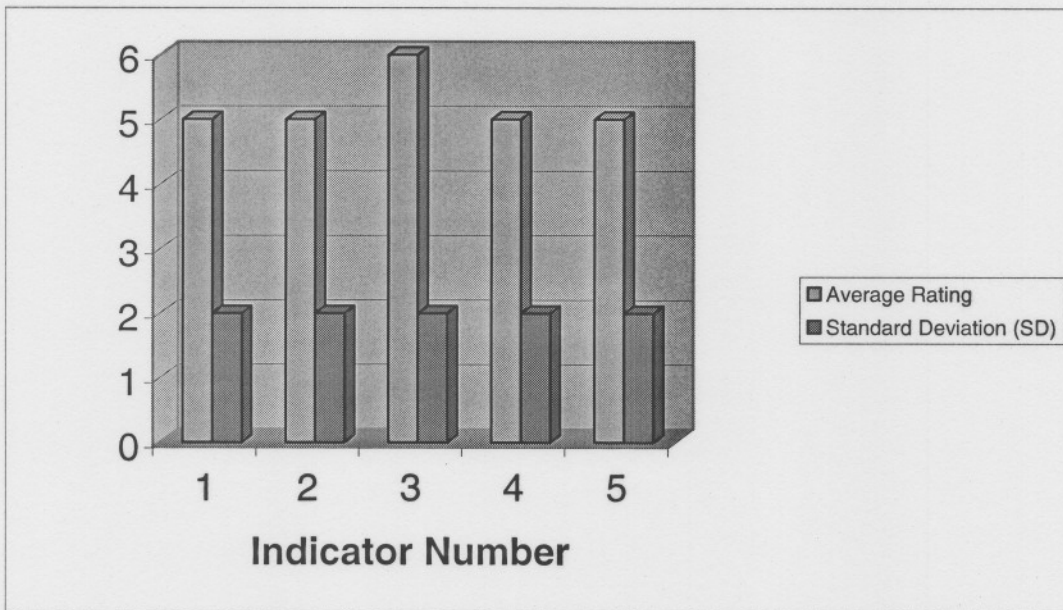
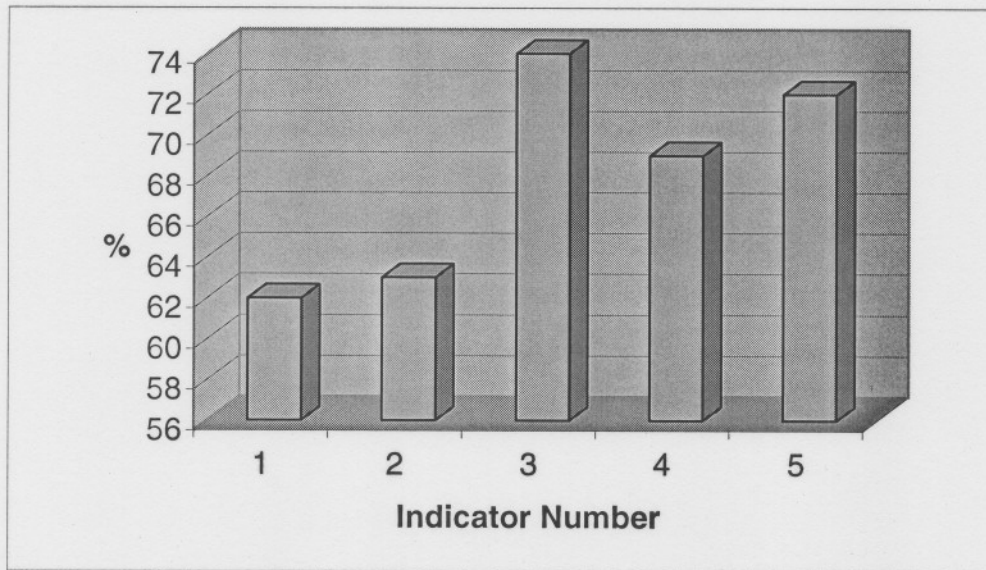


Figure 5.20 is an illustration of the overall results of how many times an indicators as scored a rating of 5 or more than 5.

Figure 5.20 Overall percentage rating



As seen in figure 5.20, indicator 3, product indicator has scored the most times a rating of 5 or more than 5, and for an indicator to be important it has to score a rating of five or more than 5, therefore product indicators is the most renowned indicator of operational risk in a Retail Bank identified by chapter 5 and employee indicators are the least important.

5.5 Conclusion

The aim of chapter 5 was to identify some of the most renowned firm wide risk indicators of operational risk in a South African Retail Bank and to determine their viability in operational risk management by handing out questionnaires. By handing out these questionnaires it was determined that product indicators is the most renowned and employee indicators the least important category of operational risk indicators in a South African Retail Bank. It is important to remember that the indicators evaluated in chapter 5 are not the only indicators of operational risk in South African Retail Bank, but are regarded as amongst the most renowned. Chapter 5 had also provide a thorough evaluation and discussion on how to effectively design and construct a questionnaire. Chapter 6 will conclude the study and will also make recommendations regarding operational risk management in South African banks.

Chapter 6

Conclusion

“The greatest risk of all is to take no risk at all,” (Olsson, 2002: xiii)

6.1 Introduction

The main goal of this research was to evaluate the management of operational risk in South African banks. The study firstly investigated The Basel Committee’s proposals for operational risk management and secondly the role of the banks asset and liability management (ALM) in operational risk management in banks in South Africa. The study further provide a theoretical as well as a practical evaluation of the key indicators of operational risk and also identified some examples of key indicators of operational risk in South Africa banks. The first objective of this research was to determine a single definition of operational risk and to discuss the existing as well as possible methods to quantify and measure operational risk in banks in South Africa. The second objective was to investigate the viability of capital provisions as a way of managing operational risk in South Africa, in other words the feasibility of the New Basel Capital Accord on South African banks.

In order to reach the goal and the objectives, the literature was reviewed and in-depth interviews were held with current experts and relevant parties in the South African risk management environment. A case study was also done on a Retail Bank in South Africa to identify and evaluate some key indicators of operational risk in South African banks by means of questionnaires. The next section draws certain conclusions based on both the literature survey (chapters 2, 3, 4 and 5) and the results of the interviews as well as the questionnaires (as discussed in chapter 5).

6.2 Conclusions

As mentioned in the introduction, one of the main objectives of this study was to provide an evaluation of the definition of operational risk. The finding was that it is almost impossible to provide a single definition of operational risk, because of the fact that operational risk can take so many forms. In chapter 2 a single definition of operational risk is constructed based on eight other published definitions. This definition define operational risk as *“the risk of an external or internal loss resulting from a range of possible events, which include a human or employee error, a disruption in the work environment, a breakdown of processes, a malfunction in the information system and or a computer system failure due to ineffective technology”*. It is important to keep in mind that the above-mentioned definition is not intended to be the decisive definition of operational risk, but is merely intended to guide the reader of this study to better understand the nature of operational risk.

Regarding the Basel Committee’s proposals (chapter 2), it has done some fundamental work on operational risk management in the past few years, and the most outstanding was the issuing of a Capital Accord, which guides banks to make capital provisions for operational risks. It has been established that the Basel Capital Accord is widely adopted around the world. Consequently, from the viewpoint of being competitive, it is to the advantage of a bank to adhere to the prescriptions of the Basel Capital Accord. However, to stay relevant, the Basel Capital Accord was due for a review. The Basel Committee released a proposal to replace the existing Basel Capital Accord with a more risk-sensitive framework. The new framework intends to improve safety and soundness in the financial system by placing more emphasis on bank’s own internal control and management, the supervisory review process, and market discipline.

The work on operational risk is in the development stage, but three different approaches of sophistication (basic indicator, standardized, and advanced measurement) have been put forward. The Basel Committee expects operational risk on average to constitute approximately 15% of the overall capital charge under the new framework. The Basel

Committee has stated that its goal is not to raise the aggregate regulatory capital inclusive of operational risk. Whether this is a realistic goal, is one of the issues debated by the interested parties through their comments on the proposed new Basel Capital Accord. Even the choice of definition will greatly affect the resulting capital charge. A big concern is that even the Advanced Measurement Approach will lead to excessive regulatory capital. In addition, there are concerns about the cost of compliance. What is clear though, is that an explicit capital requirement for operational risk will have a definite impact on capital adequacy. The magnitude of this impact will be largely determined by the approach applied to calculate the operational risk capital requirement. Which approach a bank will be allowed to use, will in turn largely depend on the quality of operational risk management and measurement.

As mentioned, another the objective of this research was to present the theory of asset and liability management (ALM) within the unifying theme of operational risk management. It was indicated that capital is used to absorb an operational risk loss. The Asset and Liability Committee (ALCO) is responsible for the strategic management of the bank's balance sheet and as capital forms part of the bank's balance sheet, it is also the responsibility of the ALCO to manage the capital that is used as provision for an operational risk. The asset and liability committee (ALCO) is the personnel and senior management that is responsible for the implementation of an effective strategic ALM process in banks and this emphasizes the important role that the ALCO plays in operational risk management in South African banks

The ALCO does not only manage the capital that is used in operational risk management, but also uses simulations (as discussed in chapter 3) to predict the impact of a potential risk event, including an operational risk event. Thus, the ALCO has a dual purpose in operational risk management. Firstly, the ALCO manages the capital that is used as buffer for an operational risk and secondly it helps to predict a potential operational risk event.

ALM is not the only way for banks to identify operational risks. Risk managers can also use the key indicators of operational risk as a means to identify, monitor, and measure operational risk. Chapter 4 puts great emphasis on distinguishing between a key performance indicator (KPI) and a key risk indicator (KRI) in the banking environment. A KPI is identified as an indicator that measures the performance of the bank at a specific time, whereas a KRI is identified as an indicator of a potential risk, in other words an **early warning system** of a potential operational risk.

All around the world banks are developing a system to identify KRIs of operational risk, because without sufficient KRIs, banks will not be able to identify potential operational risks and will be more exposed when it actually happen. The key challenge in identifying the key indicators of operational risk is to find the intersection between the business specific and firmwide risk indicators, in other words to identify the indicators that are viable not just for a specific business line or division, but are also viable for the institution as a whole.

Unfortunately, most operational risk indicators are trailing in nature to other risk indicators, for example credit risk indicators, because not enough attention has yet been given to the development of effective operational risk indicators. That is to say, operational risk indicators do a far better job of confirming recent history than they do in predicting the formation of operational risk storm clouds on the horizon. Beyond simply identifying indicators of risk, therefore, the risk manager must work hard to distil those that will prove the most useful for managing the institution's future risk and potential, not simply measuring its recent loss potential.

It is also important to mention that the indicators identified in chapter 4 and 5, is not the only indicators of operational risk, therefore, this study only aimed to provide a theoretical discussion on the key indicators of operational risk and only identified some of the most renowned KRIs in a South African Retail Bank. As mentioned the viability of the indicators identified in this study were tested in a South African Retail Bank by means of a questionnaire and the finding was that that there are five basic categories of

operational risk indicators, which include employee, customer, product, system and “other” risk indicators. The “other” risk indicators refer to those indicators that do not fall under employee, customer, product, or system indicators. The results of the questionnaires also indicated that product indicators are the most renowned and employee indicator the least important category of operational risk indicators in a Retail Bank in South Africa. To conclude this study the following key recommendations can be made:

- When defining operational risk, it is important that the definition include all four levels of operational risk, which include people, processes, technical, and technology.
- To be able to determine how much capital must be allocated specifically for operational risk, it must be possible to measure operational risk.
- For ALM to play a role in operational risk management in South African banks it is important that the standard chart of accounts must be maintained throughout the organization and involve all subsidiary companies and that the assumptions must be tested to be certain they are realistic and parallel with actual performance.
- The asset/liability simulation model results should not simply be accepted as fact, but should be challenged. This process will make sure that the asset/liability simulation model reflects the ALCO member’s best estimates and assumptions.
- For risk indicators to be effective as predictors of operational risk, risk managers must distinguish between a key risk indicator (KRI) and a key performance indicator (KPI).
- Operational risk indicators must be identified and constructed metrics that serve as predictors or “drivers” of operational risk.
- Operational risk indicators must not just be identified for specific business lines, but must be identified for the institution as a whole as firmwide operational risk indicators.
- Operational risk must not just be managed by a central unit, it is also the responsibility of every business unit in a bank to manage their own operational risk and also to provide other business units with information regarding operational risks.

6.3 Further Research

As South Africa is regarded as a third-world country, it is the view of this study that the international definition of operational risk published by the Basel Committee is not sufficient enough for operational risk management in South Africa, therefore much more research is necessary on operational risk in South Africa to find a single definition of operational risk to be appropriate for the management of operational risk in South African banks. It is also the view of this study that there is not enough theoretical background on the key indicators of operational risk in South African banks, and not enough has yet been done to identify them, therefore much more research is necessary to identify and evaluate the most renowned key risk indicators of operational risk in the South African banking environment.

Appendix 1

Interviews

DWYER, S. 2003. Standard Bank

EDWARDS, G. 2003. ABSA

SERFONTEIN, G. 2003. Standard Bank

POTTAS, A. 2003. ABSA

YOUNG, J. 2003. Standard Bank

Appendix 2

Questionnaire on the Key Indicators of Operational risk

Please answer the following questionnaire by indicating your choice by marking the appropriate block with a cross (X).

Note!!

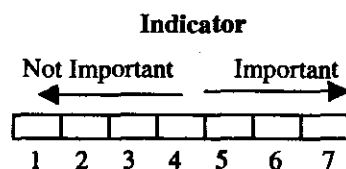
It is important to keep in mind that the explanation provided for each indicator must not influence the rating of the indicator, but it is mere intended to place the indicator in its proper context. Some of the indicators may be wrongly recognized as indicators of other banking risks, for example credit risk, and it is for this reason that each indicator must be explained to distinguish it from other banking risk indicators and to place it in an operational risk context.

The key indicators of operational risk will be evaluated in the following order:

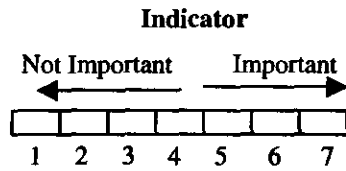
- Employee indicators
- Customer Indicators
- Product Indicators
- System Indicators
- Other indicators of operational risk

1. Employee Indicators:

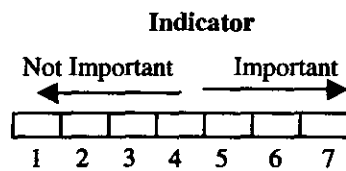
1.1 Employee turnover: Employee turnover is the rate at which new employees are leaving and joining the bank. The higher the employee turnover, the more time must be spend on training new employees



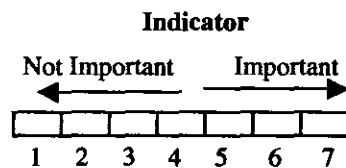
1.6 Junior and Senior Staff Tenure Individual Indicator: This indicator highlights the relative inexperience of employees. As mentioned in 1.5, the more inexperienced employees are employed, the higher the potential will be for an employee error to occur, thus the higher the exposure to operational risk.



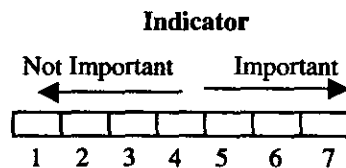
1.7 Number of transactions per staff member: The higher the number of transactions per staff member, the more likely an employee error will occur, because it become difficult to monitor and control such a large amount of transactions per staff member, thus, the higher the exposure to operational risk.



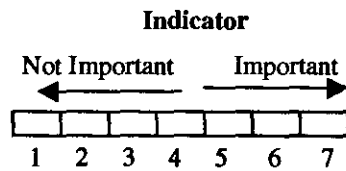
1.8 Total for specific delivery failures: For example, the number of teller shortages at a branch can also be an indication of the exposure to operational risk.



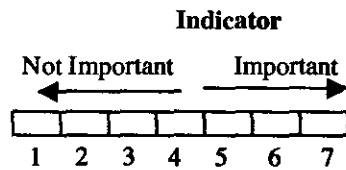
1.9 Technology management control risk indicator: Include the number of employees requiring training in new technology and will be represented as actual numbers or be weighted to reflect the total number of employees in the department.



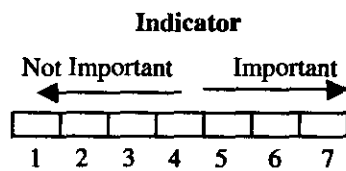
2.5 Aged confirmations: The longer the client must wait for confirmation of a deal, the lower the operating turnover will be (also see 2.4), which will increase the exposure to operational risk.



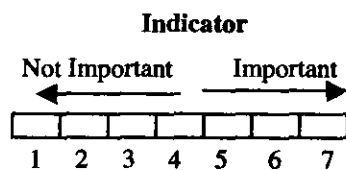
2.6 The number of cross selling: The higher the number of cross selling, the higher the exposure to operational risk.



2.7 Customer Satisfaction Survey: A survey can be done to provide the bank with information regarding the customer satisfaction, which can also be an indicator of the exposure to operational risk. In other words, the exposure to operational risk could increase when there is a decrease in customer satisfaction.

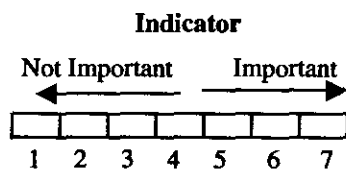


2.8 Increase/decrease in the number of customers: If there is an abnormal increase or decrease in the number of customers per a specific time, for example one month it can be an indication of some irregularities, for example operational risks.

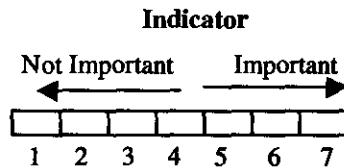


3. Product Indicators

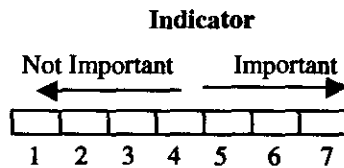
3.1 Product complexity: The more complex a bank product is, the higher the operational risk will be, because employee errors will be more likely to occur.



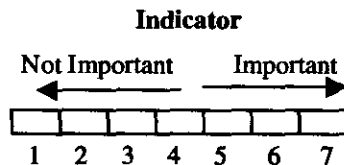
3.2 Range of Products: The more complex/large the range of products is, the higher the exposure to operational risk will be, because it is difficult to monitor and control a complex and large range of products.



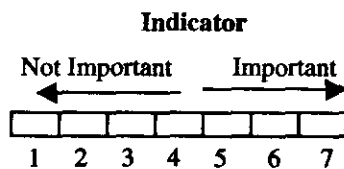
3.3. Number of settlement fails: The number of settlement fails per geographic area is also a good indication of operational risk. A settlement failure can be as a result of the incorrect documentation of a certain transaction.



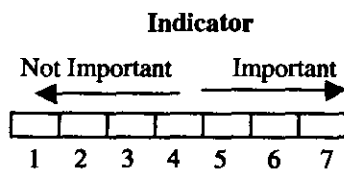
3.4. Non-performance with compliance with policy: If a product does not comply with the bank's overall policy (Board's policy), it can also be an indication of a possible operational risk.



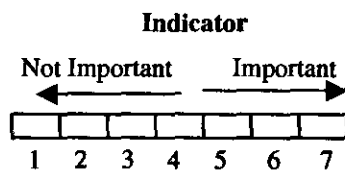
3.5 The number of new accounts opened: An abnormal (more than usual) amount of new accounts (products) opened per month can also be an indication of a potential operational risk. The more accounts are opened in one month the more difficult it become for the management to monitor and control them, thus there is an increase in the exposure to operational risk.



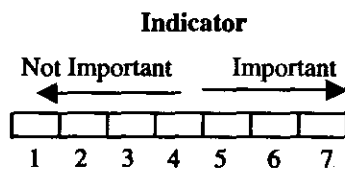
3.6 The number of accounts closed: As with the number of new accounts opened, the number of accounts closed per month can also be an indication of a potential operational risk. For example, if there is an abnormal amount of accounts closed per month it can be an indication of potential operational risk.



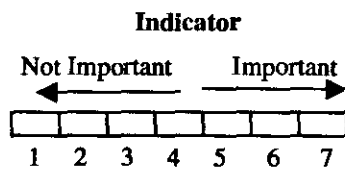
3.7 Increase in the number of lost and stolen ATM (credit cards) cards: The higher the number of lost and stolen cards, the higher the burden on employees, because they must provide new cards at the same rate at which they are lost, thus, it increases the exposure to operational risk.



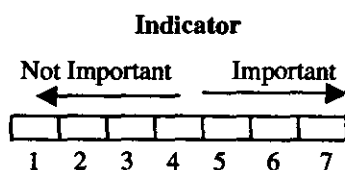
3.8 The total number of active credit card accounts: This will provide risk managers with insight into the exposure of operational risk faced by the card division.



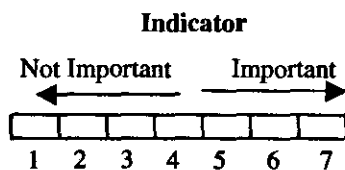
3.9 Total applications received vs. Total applications approved: The total number of applications received versus the total number of applications approved can also be an indication of operational risk.



3.10 Total applications denied: In addition to the above-mentioned indicator (see 3.9), the number of applications denied in a specific time frame (for example one month) could also be an indication of operational risk.

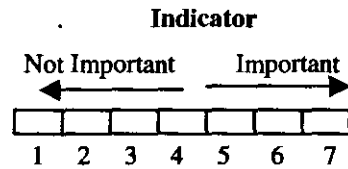


3.11 Increase in the number of transactions: An increase in the number of transactions that, when it increases, causes an increase in the number of erroneous transactions, which in turn, increase the exposure to operational risk.

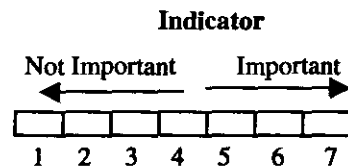


4. System Indicators

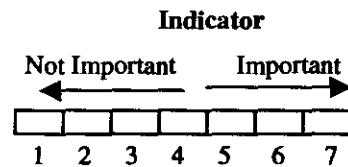
4.1 System downtime: The longer an IT-system is down, the more likely a system-related error will occur, thus the higher the exposure to operational risk will be.



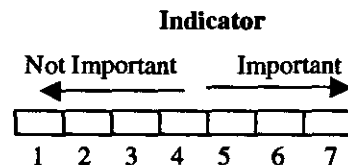
4.2 Number of hacking attempts detected: The number of hacking attempts per specific time frame (for example one month) could also highlight the relative exposure to operational risk.



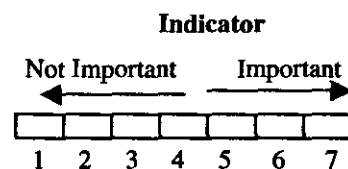
4.3 Number of points of entry into the system: In addition to the above-mentioned indicator (see 4.2), the number of points of entry into the system per specific time frame (for example one month) could also be an indication of the relative exposure to operational risk.



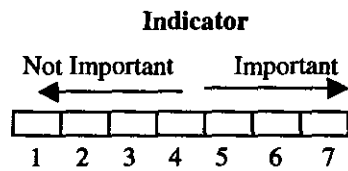
4.4 Number of system problems detected: The higher the number of system problems detected per specific time frame (for example one month), the higher the exposure to operational risk. (The higher the number of system problems detected, the higher the probability of a system-related error)



4.5 Intranet between branches: An insufficient intranet between branches can result in the inadequate flow of information between branches. This can then result in the ineffective management of branches.

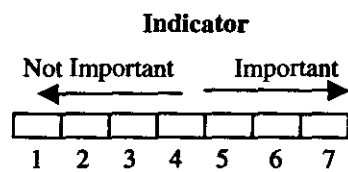


4.6 Number and value of internet transactions: The higher the number and value of internet transactions, the higher the exposure to operational risk will be, because a higher number and value of internet transactions will result in an increase to the value at risk (VaR) of internet transactions.

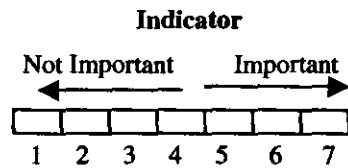


5. Other Indicators of Operational Risk:

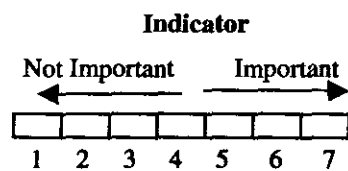
5.1 Number of incidents of fraud: The higher the number of fraud incidents the higher the burden on employees, thus it increases the exposure to operational risk.



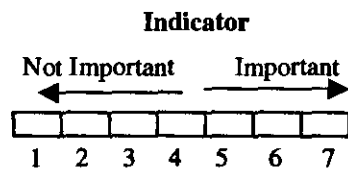
5.2 Number of critical/unacceptable ratings/findings received from completed audits: The information from completed audits regarding critical/unacceptable ratings/findings could highlight the exposure to an operational risk.



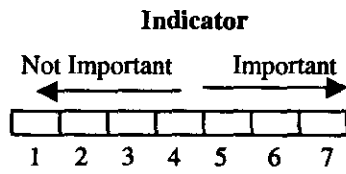
5.3 Concentration of activities (transactions): Concentration risk – too much invested in one sector, asset class or geographic region.



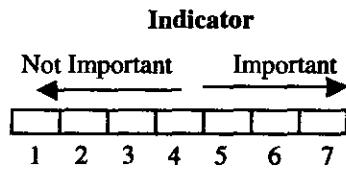
5.4 Movement in market share: An abnormal (more than usual) decrease or increase in the bank's market share (for example, in vehicle finance) could highlight the exposure to operational risk.



5.5 Percentage movement in the total book value (for example vehicle finance): An abnormal (more than usual) decrease or increase in total book value, which can highlight the exposure to operational risk.



5.6 Number and value of physical losses: The number and value of physical losses at a bank (in a specific time frame) for example, accidents, vandalism, Acts of God (for example floods), etc. could indicate the exposure to operational risk.



Additional comments:

.....

.....

.....

.....

.....

.....

.....

.....

Appendix 3

Results of the Seventeen Questionnaires

| |
|--------------------------------|
| Number of questionnaire |
|--------------------------------|

| |
|---------------------------|
| Number of question |
|---------------------------|

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|
| 1.1 | 7 | 6 | 6 | 6 | 5 | 7 | 6 | 7 | 6 | 5 | 5 | 6 | 3 | 4 | 5 | 5 | 4 |
| 1.2 | 6 | 5 | 4 | 3 | 6 | 1 | 7 | 7 | 6 | 3 | 2 | 4 | 6 | 5 | 4 | 3 | 4 |
| 1.3 | 6 | 4 | 5 | 2 | 5 | 7 | 5 | 6 | 6 | 3 | 3 | 6 | 5 | 6 | 5 | 3 | 4 |
| 1.4 | 6 | 6 | 6 | 5 | 5 | 1 | 6 | 3 | 4 | 4 | 4 | 5 | 2 | 4 | 7 | 3 | 5 |
| 1.5 | 4 | 7 | 7 | 5 | 6 | 7 | 4 | 5 | 7 | 2 | 3 | 4 | 5 | 5 | 5 | 3 | 4 |
| 1.6 | 6 | 5 | 6 | 5 | 3 | 6 | 5 | 4 | 5 | 6 | 6 | 5 | 3 | 5 | 5 | 4 | 2 |
| 1.7 | 4 | 5 | 5 | 5 | 4 | 1 | 4 | 2 | 4 | 6 | 5 | 4 | 5 | 5 | 3 | 5 | 3 |
| 1.8 | 6 | 4 | 5 | 5 | 6 | 1 | 5 | 5 | 6 | 6 | 6 | 5 | 3 | 5 | 5 | 5 | 6 |
| 1.9 | 6 | 5 | 5 | 5 | 5 | 2 | 4 | 3 | 3 | 3 | 3 | 2 | 7 | 4 | 3 | 3 | 6 |
| 2.1 | 7 | 7 | 7 | 6 | 6 | 7 | 6 | 6 | 7 | 6 | 6 | 7 | 6 | 4 | 7 | 7 | 5 |
| 2.2 | 6 | 4 | 5 | 6 | 5 | 1 | 6 | 2 | 6 | 2 | 4 | 4 | 7 | 4 | 3 | 3 | 3 |
| 2.3 | 6 | 3 | 4 | 7 | 7 | 1 | 6 | 3 | 7 | 6 | 6 | 6 | 7 | 6 | 6 | 4 | 2 |
| 2.4 | 6 | 7 | 6 | 6 | 6 | 1 | 6 | 1 | 5 | 6 | 5 | 2 | 7 | 6 | 5 | 5 | 2 |
| 2.5 | 5 | 3 | 3 | 7 | 6 | 1 | 6 | 2 | 7 | 6 | 5 | 6 | 2 | 4 | 2 | 4 | 1 |
| 2.6 | 3 | 5 | 5 | 5 | 5 | 1 | 4 | 3 | 3 | 3 | 2 | 1 | 7 | 6 | 7 | 2 | 4 |
| 2.7 | 7 | 5 | 6 | 6 | 6 | 5 | 5 | 6 | 4 | 7 | 6 | 6 | 2 | 4 | 7 | 7 | 3 |
| 2.8 | 7 | 4 | 4 | 7 | 6 | 7 | 5 | 6 | 3 | 6 | 6 | 5 | 6 | 5 | 2 | 7 | 2 |
| 3.1 | 6 | 6 | 6 | 6 | 7 | 2 | 4 | 5 | 5 | 6 | 6 | 6 | 6 | 4 | 3 | 3 | 2 |
| 3.2 | 7 | 6 | 6 | 6 | 6 | 1 | 4 | 6 | 3 | 5 | 4 | 6 | 7 | 4 | 6 | 3 | 4 |
| 3.3 | 5 | 6 | 6 | 5 | 5 | 1 | 4 | 3 | 5 | 6 | 7 | 1 | 4 | 4 | 3 | 6 | 5 |
| 3.4 | 7 | 6 | 6 | 4 | 7 | 7 | 5 | 4 | 5 | 6 | 6 | 6 | 7 | 5 | 6 | 5 | 2 |
| 3.5 | 3 | 5 | 5 | 6 | 3 | 1 | 4 | 4 | 3 | 2 | 3 | 3 | 7 | 3 | 2 | 2 | 2 |
| 3.6 | 6 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 2 | 2 | 1 | 6 | 6 | 5 | 1 | 6 | 2 |
| 3.7 | 1 | 7 | 7 | 3 | 6 | 1 | 6 | 2 | 5 | 1 | 1 | 4 | 5 | 3 | 4 | 1 | 3 |
| 3.8 | 4 | 5 | 6 | 5 | 4 | 1 | 5 | 4 | 2 | 3 | 2 | 3 | 5 | 5 | 4 | 1 | 2 |
| 3.9 | 5 | 6 | 6 | 5 | 6 | 1 | 4 | 5 | 2 | 3 | 1 | 5 | 5 | 4 | 4 | 5 | 2 |
| 3.1 | 5 | 3 | 4 | 5 | 6 | 1 | 4 | 5 | 3 | 1 | 1 | 5 | 5 | 4 | 7 | 1 | 6 |
| 3.11 | 4 | 6 | 6 | 6 | 3 | 1 | 4 | 6 | 6 | 6 | 6 | 4 | 7 | 6 | 7 | 5 | 6 |
| 4.1 | 7 | 7 | 7 | 7 | 6 | 7 | 5 | 6 | 7 | 7 | 7 | 6 | 7 | 6 | 2 | 7 | 6 |
| 4.2 | 7 | 6 | 7 | 7 | 7 | 1 | 5 | 6 | 6 | 6 | 5 | 6 | 7 | 6 | 5 | 6 | 6 |
| 4.3 | 3 | 6 | 6 | 7 | 5 | 1 | 5 | 2 | 2 | 5 | 4 | 5 | 5 | 6 | 5 | 2 | 6 |
| 4.4 | 7 | 7 | 7 | 6 | 7 | 6 | 4 | 6 | 7 | 6 | 6 | 6 | 7 | 6 | 3 | 6 | 6 |
| 4.5 | 6 | 7 | 7 | 3 | 6 | 1 | 3 | 2 | 5 | 4 | 2 | 5 | 5 | 4 | 6 | 1 | 1 |

| | | | | | | | | | | | | | | | | | |
|------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.6 | 3 | 7 | 7 | 3 | 6 | 1 | 5 | 2 | 3 | 3 | 6 | 5 | 7 | 3 | 5 | 1 | 6 |
| 5.1 | 7 | 5 | 6 | 6 | 7 | 7 | 4 | 6 | 7 | 7 | 7 | 6 | 7 | 2 | 5 | 7 | 7 |
| 5.2 | 7 | 7 | 7 | 6 | 7 | 7 | 6 | 5 | 7 | 7 | 4 | 6 | 6 | 5 | 5 | 5 | 4 |
| 5.3 | 6 | 6 | 6 | 7 | 7 | 1 | 6 | 2 | 5 | 5 | 4 | 6 | 7 | 4 | 3 | 5 | 4 |
| 5.4 | 5 | 6 | 6 | 6 | 5 | 1 | 5 | 6 | 5 | 6 | 2 | 6 | 7 | 4 | 6 | 4 | 3 |
| 5.5 | 4 | 6 | 6 | 6 | 6 | 1 | 5 | 6 | 4 | 2 | 5 | 6 | 7 | 4 | 5 | 2 | 4 |
| 5.6 | 6 | 3 | 4 | 6 | 6 | 7 | 7 | 6 | 6 | 6 | 3 | 6 | 7 | 2 | 4 | 6 | 7 |

References

ADELSON, M.H. 1993. Asset based commercial paper: understanding the risks - moody investors services. Standard financial report, April.

ALLEN, L. & CEBENOYAN, A.S. 1991. Bank acquisitions and ownership structure: theory and evidence: *Journal of banking and finance* 15 (2): 425-448. April.

BANK FOR INTERNATIONAL SETTLEMENTS (see BIS):

BIS, Basel Committee on Banking Supervision. 1998. Operational risk management, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2001h. Potential modification to the Committee's proposals, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2000d. A new capital adequacy framework, Pillar 3 (Market Discipline), Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2000d. Range of practices of banks internal ratings based system, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2000d. Credit ratings and complementary sources of credit quality information, Working Paper no. 3 August, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2000e. Summary of responses received on the report 'Credit risk modelling, current practices and applications, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision .2000f. Best practice for credit risks management, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2000g. Principles for the management of operational risk, Basel, Switzerland, May.

BIS, Basel Committee on banking supervision. 2001a. Consultative document, a proposal for New Basel Capital Accord, Basel Switzerland.

BIS, Basel Committee on Banking Supervision.2001b. Supporting document: the International Rating Based Approach. BIS, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2001c. Supporting document. Pillar 3 (market discipline) BIS, Basel Switzerland.

BIS, Basel Committee on Banking Supervision. 2001d. Quantitative impact study, Basel, Switzerland, April.

BIS, Basel Committee on Banking Supervision. 2001d. Public disclosure by banks, results of the survey of the 1999 disclosure, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2001f. Update on the New Basel Capital Accord, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2001g. Results on the second quantitative impact study, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2001h. Potential modification to the Committee's proposals, Basel, Switzerland.

BIS, Basel Committee on Banking Supervision. 2002a. Public disclosure by banks: results of the survey of the 2000 disclosure survey, Basel, Switzerland,

BIS, Basel Committee on Banking Supervision. 2002b. Basel Committee reaches agreement on the New Capital Accord issues, Basel, Switzerland, 10 July.

BIS, Basel Committee on Banking Supervision. 2003a. Third consultative document on the New Basel Capital Accord, Basel, Switzerland. 29 April.

BANKING COUNCIL OF SOUTH AFRICA. 2001. Submission to the Basel Committee on Banking Supervision: comments on the consultative package of the New Basel Accord, June, Pretoria.

BARBOUR, D., NORTON, J.J. & PENN, G. 1991. Capital adequacy concerns: Basel Supervisors Committee, US and UK. (*In Norton, J.J. & Spellman, P.R. eds. Asset securitization: international financial and legal perspectives. Oxford: Basil Blackwell, p. 270-318.*)

BARCKLEYS, P.L.C 2001. Submission to the Basel Committee on Banking Supervision: comments on the second consultative package of the New Basel Capital Accord: [Available on the Internet:] <http://www.bis.org>, [Date of access: 14 April 2003].

BASTANY, A. 1994. Credit risk management. (*In DAS, ed. Risk management and financial derivatives: A guide to the mathematics. New York: McGraw & Hill. p.697-713*)

BESSIS, J. 2001 Risk management in banking, 2nd ed, Chichester, UK: Wiley.

BITNER, W.J, & GODDARD, R.A. 1995. Successful asset and liability Management, A Guide To the Future Beyond Gap, New York, USA, Willey.

BLISS, P.R, FLANNERY, M.J. 2001. Market discipline in the governance of U.S. bank holding companies: monitoring vs. influencing Federal Reserve Bank of Chicago, Chicago. (Working paper no. 2000-03.)

BOTHA, M. 1999. Asset and liability management: Applications for value at risk, (Thesis – M.Comm) Potchefstroom, South Africa: P.U for CHE

CALOMARIS, C & HERRING, R. 2002. The Regulation of operational risk in investment management companies, Perspective 8 (2): 1 – 20, Investment, September. [Available on the Internet:] <http://www.ici.org> [Date of Access: 22 July 2003]

CA-RATINGS. 2000. SA banks, security firms and money market funds. Issue 4/2000. Johannesburg, December.

CADE, E. 1997. Managing banking risks, Cambridge, UK: Woodhead.

CEBENOYAN, A.S., COOPERMAN, E.S., REGISTER, C.A & HUDGINS, S.C. 1993. The relative efficiency of stock versus mutual S&Ls: A stochastic cost frontier approach. *Journal of Financial Services Research* 2nd ed, p151-170.

CHURCHILL, G.A. 1992. Basic marketing research: 2nd ed, Fort Worth, UK: Dryden Press.

COLE, R.A & EISENBEIS, R.A. 1996. The role of principle – agent conflicts in the 1980's thrift crises. Federal Reserve Board, finance and economics discussion series, division of monetary affairs, Chicago, USA, working paper 95-27.

CROSSE, H & HEMPEL, G.H. 1999. Management policies for commercial banks. 3rd ed, Englewood Cliffs, New Jersey, USA: Prentice-Hall.

CROUHY, M, GALAI, D & MARK, R. 1998. Key steps in building consistent operational risk management and measurement, operational risk in financial institutions, West Sussex, UK: Wiley.

CRUZ, M.G. 2002. Modelling and measuring and hedging operational risk. West Sussex: Wiley.

DE BEER, J.A. 2002. The Impact of the new proposed framework and credit risk management policies of South African banks, (Thesis – D.Comm) Bloemfontein, South Africa: University of the Free State.

DEMPSEY, A & PIETERS, H.N. 1996, Inleiding tot finansiële rekeningkunde, Pretoria, South Africa: Butterworth.

FABOZZY, F.J & KONISHI, A. 1996. Introduction, the handbook of asset and liability management: State-of-the-art investment strategies, risk controls and regulatory requirements. Revised ed, Chicago, USA: Irwin.

FALKENA, H.B., FOURIE, L.J & KOK, W.J. 1995. The South African financial system. Goodwood, South Africa: South Book Publishers.

FISHER, H. 1930. The use of multiple measurements in taxonomic problems, annals of Eugenics. 7, p. 178 – 188.

GALLUP, R. 1947. Qualitative measurement of public opinion: the quintamensional plan of questionnaire design, American Institute of Public Opinion: 201.

GARDNER, M.J., MILLS, P.L & COOPERMAN, E.S. 2001. Managing financial institutions, an asset and liability management approach, 4th ed: Dryden Press.

GARDNER, M.J & MILLS, P.L. 1997. Managing financial institutions: an asset and liability approach, 3rd ed, Sea Hamber Drive, Orlando, USA: The Dryden Press.

HIWATASHI, J. 2002. Solutions on measuring operational risk, capital markets news, Federal Reserve Bank of Chicago, USA, September: [Available on the Internet:] <http://www.chicagofed.org/publications> [Date of access: 22 July 2003]

HERKES, R., GEGINAT, M & BORYSIK, M. 2003. Operational risk: how to create and use models of the Advanced Measurement Approach: [Available on the Internet:] <http://www.riskpartner.lu.dos8> [Date of access: 14 July 2003].

HOFFMAN, D.G. 2002. Managing operational risk: 20 firm wide best practice strategies, Chicago, USA: Wiley.

HOFFMAN, D.G, & TAYLOR, D. 1999. Avoiding signal failure, *operational risk special report, risk*, November.

HUSSAIN, A. 2000. Managing operational risk in financial markets, Oxford, UK: Butterworth-Heinenmann.

JACKSON, P., MAUDE, D.J & PERRAUDEN, W. 1997. Bank capital and value-at-risk, *Journal of derivatives*, 4 (2).

JARROW, R.A, & VAN DEVENTER, D.R. 1999. Assets and liability management, a synthesis of new methodologies, London, UK: Risk Book Publishers.

KARACADAG, C & TAYLOR, M.V. 2000. A new capital adequacy framework: institutional constraints and incentive structures. IMF working paper no. 00/93. IMF. Washington, D.C., USA. April.

KAUFMAN, G.G & SCOTT, K.E. 2003. What is systematic risk, and do bank regulators retard or contribute it? *Independent Review*, 10861653, 7 (3), September.

KING, J.L. 2000. Operational risk: measurement and modelling, Chichester, UK: Wiley.

KOCH, T.W & McDonald, S.S. 2000. Bank Management, 4th ed, Orlando, USA: Dryden Press.

KOCH, T.W. 1997. Bank Management, International ed, University of South Carolina, South Carolina, USA: Dryden Press.

KROON, J. 2000. Entrepreneurskap, begin jou eie onderneming, PU for CHE, Potchefstroom, South Africa: Porton.

KUPIEC, P.H & NICKERSON, D. 2001. Assessing systematic risk exposure under alternative approaches for capital adequacy. Prepared for the Bank of England, May25.

KUPIEC, P.H & NICKERSON, D. 2001. Assessing systematic risk exposure under alternative approaches for capital adequacy. Prepared for the Bank of England, October 12.

LAWRENCE, M. 2000. Marking the cards of ANZ, Operational Risk: A Risk Special Report, p. S9 – S10, November.

LOPEZ, J.A. 2002. What is operational risk? FRBSF economic letter, January: [Available on the Internet:] [http://www. Frbsf.org/publications](http://www.Frbsf.org/publications) [Date of access: 22 July 2003].

LOUBSER, M & GILMOUR, B. 1991. Questionnaire design: research for marketing, (*In* Macfarlane Smith, J. Interviewing in market and social research, London: 18(2): 4-15)

MACFARLANE SMITH, J. 1972. Questionnaire design and attitude measurement, London: Heinemann.

MAITZ, J & SMITH, K. 2001. Operational risk. Mr. Maitz & Smith was speaking for the CSC Financial Services Institute at the Centre for the Study of Financial Innovation in February.

MANKIW, N.G. 2000. Macroeconomics, fourth edition. New York, USA: Worth Publishers.

MARE, D. 1995. The ALCO Process, *ALCO Update*, 7 (3), September.

MARSHALL, C.L. 2001. Measuring and managing operational risk in financial institutions: tools, techniques, and other resources. Singapore: Wiley.

MARTINS, J.H., LOUBSER, M & DE J VAN WYK, H. 1996. Marketing research: A South African approach, Pretoria, South Africa: Unisa Press.

MATTEN, C. 1998. Managing banking capital: capital allocation and performance measurement, Chichester, UK: Wiley.

MATTEN, C. 2000. Managing banking capital: capital allocation and performance measurement, 2nd ed, Chichester, UK: Wiley.

McELRAVEY, J.N. 2001. Securities backed by credit card receivables. (*In* Fabiozzy, F.J ed. The Handbook of fixed income securities. 6th ed, New York: McGraw & Hill. p. 739-756)

McPAIL, K. 2003. Managing operational risk and payment clearing and settlement systems, Bank of Canada Working Paper, February. [Available on the Internet:] <http://bankofcanada.ca> [Date of Access: 22 July 2003]

MEDOVA, E.A & KYRIACOU, M.N. 2002. Measuring extremes in operational risk management, (*In Dempster, M.A.H. ed. Risk management: value at risk and beyond*, Cambridge, UK: Cambridge University Press)

MIHALTIAN, P.A. 1998. Additional considerations for effective asset and liability modelling. *Bank Asset/Liability management*, October.

MORGAN, J.P. 1994. Riskmetrics technical document, 4th ed, April.

OLSSON, C. 2002. Risk management in emerging markets: how to survive and prosper, New York, USA: Prentice Hall.

ONG, M.K. 1998. Integrating the role of risk management in ALM. (*In Gardner, C, ed. 1998. asset and liability management: A Synthesis of new Methodologies*, London, UK: Risk Books).

OPPENHEIM, A.N. 1966. Questionnaire design and attitude measurement, London, UK: Heinemann.

PLATT, R.B. 2000. Controlling interest rate risk: new techniques and applications for money management, New York, USA: Wiley.

PRICEWATERHOUSE & COOPERS. 2003. About us: industries, financial Services, and risk management. [Available on the Internet:] <http://www.pwcglobal.com> [Date of access: 9 September 2003].

RAGHAVEN, C. 2001. New proposals for bank capital adequacy standards unveiled. *South-North Development Monitor (SUNS)*, January 16. [Available on the Internet:] <http://www.twinside.org.sg/title/adequacy.htm> [Date of access: 13 March 2003].

RAWNSLEY, J. 2000. Total risk, Nick Leeson and the fall of Barings Bank. [Available on the Internet:] <http://www.tebubbleburst.co.uk/nickleeson> [Date of access: 4 August 2003].

REUTERS. 2002a. SA's FirstRand to acquire Saambou. *Mail & Guardian online*, April 3. [Available on the Internet:] <http://www.news24.com/News24/Home> [Date of access: 17 March 2003].

REUTERS. 2002a. More bank mergers seen, April 23. [Available on the Internet:] <http://www.news24.com/News24/Finance> [Date of access: 17 March 2003].

ROSE, P. S. 1999. Commercial bank management, 4th ed, Singapore: McGraw & Hill.

SAAYMAN, A. 2002. Securitization as a liquidity source for small banks in South Africa, (Thesis – D.Comm), Potchefstroom, South Africa: P.U for CHE.

SARGENT, P.C. 1995. Commercial mortgage securitization (*In* Norton, J.J., Pupler, M.S, & Spellman, T.R eds. International asset securitization, London, UK: Lloyds of London Press)

SCOTT, E. 1999. Risk Management and insurance, Boston, USA: Irwin/McGraw & Hill.

SINKEY, J.F. 2001. Commercial bank financial management in the financial services Industry, 6th ed, Cape Town, South Africa: Pearson Education.

STEENKAMP, C.S. 1984. Praktiese riglyne vir vraelyskonstruksie, Pretoria, Suid-Afrika: Raad vir Geesteswetenskaplike Navorsing,

STYGER, P. 1997a. What should the board of directors know about asset and liability management. *ALCO Update*: 9 (1).

STYGER, P. 1998a. Basel, tydskuur en waarde op risiko. Potchefstroom, South Africa: PU vir CHO. (Inougurele Rede Nr 150.)

STYGER, P. & BOTHMA, F. 1998. The ALCO Policy Document. *ALCO Update*: 10 (2).

THEODORE, S. 2002. Bank operational risk management, more than just an exercise in capital allocation and data gathering: Moody Investors Services, June. [Available on the Internet:] <http://www.moody's.com> [Date of access: 22 June 2003].

THIRWELL, J. 2002. Time performance indicators monitoring financial institutions. [Available on the Internet:] <http://metamatrix.com/infomatrix> [Date of access: 22 June 2003]

THORNHILL, W.T. 1993. Risk management for financial institutions: Applying cost effective controls and procedures, New York, USA: Bankers Publishers.

TLALI, J.K. 2002. Asset and liability management at a Central Bank, (Thesis – M.Comm) Potchefstroom, South Africa: P.U for CHE.

UBS. Submission to the Basel Committee on banking supervision. 2001. Comments on the second consultative package of the New Basel Accord. June. [Available on the Internet:] <http://www.bis.org>. [Date of access: 14 April 2003].

VAN DEN BERG, A.R. 1983. 'n Oorsig oor skakelingsteorie en skakelingstegnieke, referaat aangebied tydens 'n seminar oor skakeling, Pretoria: RGN.

VAN DEN BERG, A.R. & VORSTER, J.F. (red). 1982. Basiese psigometrika, Pretoria, South Africa: RGN.

VAN DEN BRINK, G.J. 2002. Operational Risk: The new challenge for banks. New York, USA: Pulgrave

VIVIERS, G.H. 2003. The Saambou Crises and the Impact on Other Banks, *Writing for the Financial Mail*, February.

VORSTER, Q., JOUBERT, W.A., KOEN, M & KOORNHOF, C. 1997. Beskrywende rekeningkunde. Agste Uitgawe, Pretoria, South Africa: Juta.

WILLIAMSON, D.P. 1963. Environmental guidance and support for small businesses. Written for small business development, department of environmental consideration, Alaska, 54.

YAM, J. 1998. The impact of technology on the financial development in East Asia, *Journal of International Affairs*, Columbia University in the City of New York, USA, Spring 1998, 51, no. 2.