A STRUCTURED APPROACH TO OPERATIONAL RISK MANAGEMENT IN A BANKING ENVIRONMENT

by

JACOBUS YOUNG

Submitted in accordance with the requirements for the degree of

DOCTOR OF COMMERCE

in the subject

BUSINESS MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: PROF JYL CRONJE

JOINT PROMOTER: PROF GS DU TOIT

NOVEMBER 2001
I declare that A Structured Approach to Operational Risk Management in a Banking Environment is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.
# CONTENTS

LIST OF FIGURES  
LIST OF TABLES  
ACKNOWLEDGEMENTS  
EXECUTIVE SUMMARY

## CHAPTER 1: INTRODUCTION

1. Background  
   1.1. Market/Price Risk  
   1.1.1. Credit Risk  
   1.1.3. Interest-Rate Risk  
   1.1.4. Country Risk  
   1.1.5. Liquidity Risk  
   1.1.6. Legal Risk  
   1.1.7. Reputation Risk  
   1.1.8. Operational Risk  
   1.2. Problem Statement  
   1.3. Purpose of the Research  
   1.4. Approach  
   1.5. Presentation Structure of the Study

## CHAPTER 2: AN OVERVIEW OF RISK MANAGEMENT IN A BANKING ENVIRONMENT

2. Introduction  
   2.2. Risk, Risk Management and the Risk Management Process  
   2.2.1. Risk Management  
   2.2.2. Integrated Approach to Risk Management  
   2.2.2.1. Organisational Effectiveness  
   2.2.2.2. Risk Performance Management  
   2.2.2.3. Systems Technology  
   2.2.3. Risk Management Process  
   2.3. Elements of a Risk Management Process  
   2.3.1. Risk Identification  
   2.3.2. Risk Evaluation  
   2.3.3. Risk Control  
   2.3.4. Risk Financing  
   2.4. Risk Classification  
   2.4.1. Broad Groupings of Risks  
   2.4.2. Classification of Risks from the Financial Services Industry Point of View
CHAPTER 3: OPERATIONAL RISK MANAGEMENT: A LITERATURE REVIEW

3.1. Introduction
3.2. Identification of Operational Risk
3.2.1. Definition of Operational Risk
3.2.2. Underlying Operational Risk Factors
3.2.2.1. People
3.2.2.2. Systems (Technology)
3.2.2.3. Processes
3.2.2.4. External Factors
3.2.3. Methods of Risk Identification
3.2.4. Conclusion
3.3. Evaluation of Operational Risk
3.3.1. Approaches to Measuring Operational Risk
3.3.1.1. Qualitative Approaches to Measuring Operational Risk
3.3.1.2. Quantitative Approaches to Measuring Operational Risk
3.3.2. Conclusion
3.4. Control of Operational Risk
3.4.1. Operational Risk Policy
3.4.2. Internal Controls
3.4.3. Risk Reporting
3.4.4. Organisational Structure, Roles and Responsibilities
3.4.4.1. Board of Directors
3.4.4.2. Internal Audit
3.4.5. Conclusion
3.5. Operational Risk Financing
3.5.1. Risk Transfer
3.5.2. Risk Retention
3.5.3. Capital Adequacy and Operational Risk
3.5.4. Conclusion
3.6. Summary

CHAPTER 4: RESEARCH METHODOLOGY
4.1. Introduction
4.2. Research Design
4.2.1. Interviews
4.2.2. Questionnaires
4.3. Data Measuring
4.4. Pretesting for Validity and Reliability
4.4.1. Validity
4.4.2. Reliability
4.5. Data Gathering Used in this Study
4.5.1. Target Population
4.5.2. Format of the Questions
4.5.3. Choice of Measuring Scale
4.5.4. Pretesting of the Questionnaire
4.5.4.1. Validity
4.5.4.2. Reliability
4.6. Statistical Analysis
4.7. Conclusion

CHAPTER 5: STATISTICAL ANALYSIS OF RESULTS
5.1. Introduction
5.2. Demographic Data
5.2.1. Responses Received from Local and Foreign Banks
5.2.2. Different Types of Banks that Responded
5.2.3. Occupation/Positions of Persons that Completed Questionnaires
5.2.4. Experience of Persons that Completed the Questionnaires
5.3. Grouping of Questions
5.4. Statistical Analysis of the Data from the Completed Questionnaires
5.4.1. Item 1: Risk Types
5.4.2. Item 2: Operational Risk Factors and Defining Operational Risk
5.4.2.1. Primary Operational Risk Factors
5.4.2.2. Operational Risk Exposures
5.4.2.3. Definition
5.4.3. Item 3: Operational Risk Management Process
5.4.3.1. Formal Risk Management Approach
5.4.3.2. Elements of an Operational Risk Management Process
5.4.3.3. Alignment of the Operational Risk Management Processes with the Strategies and Objectives of Banks
5.4.3.4. The Operational Risk Management Process as an Integral Part of the Overall Risk Management Process
5.4.4. Item 4: Identification of Operational Risk
5.4.4.1. Risk Identification as an Ongoing Process
5.4.4.2. Methods to Identify Risks
5.4.5. Item 5: Measurement of Operational Risk
5.4.5.1. Qualitative Methods
5.4.5.2. Quantitative Methods
5.4.6. Item 6: Operational Risk Control
5.4.7. Item 7: Operational Risk Structure
5.4.7.1. Operational Risk Management Structure
5.4.7.2. Reporting Lines

Page
235
239
240
241
242
244
244
246
247
255
256
256
256
257
258
258
259
260
261
266
267
271
288
290
291
292
297
299
301
301
303
306
306
308
311
314
314
315
5.4.7.3. Responsibility for Operational Risk .......................... 317
5.4.8. Item 8: Financing of Operational Risk ....................... 321
5.4.8.1. Risk Financing Techniques .................................. 321
5.4.8.2. Basel Committee’s Proposals ............................... 324
5.5. Conclusion ......................................................... 328

CHAPTER 6: A FRAMEWORK FOR A STRUCTURED APPROACH TO
OPERATIONAL RISK MANAGEMENT IN A BANKING
ENVIRONMENT........................................................................
6.1. Introduction .......................................................... 333
6.2. Components of a Structured Approach to Operational Risk
Management ................................................................. 333
6.2.1. The Primary Risk Types of a Bank ......................... 334
6.2.2. A Formal Definition of Operational Risk .................. 334
6.2.3. The Primary Operational Risk Factors .................... 335
6.2.4. The Operational Risk Management Process ............... 337
6.2.4.1. Risk Identification ............................................. 337
6.2.4.2. Risk Evaluation ............................................... 338
6.2.4.3. Operational Risk Control ................................. 340
6.2.4.4. Risk Financing ............................................... 341
6.2.5. Operational Risk Management Structures ................. 342
6.2.6. Capital Adequacy Requirements ............................. 343
6.3. Framework for Operational Risk Management ............... 344
6.4. Conclusion .......................................................... 346

CHAPTER 7: SUMMARY, CONCLUSIONS AND
RECOMMENDATIONS...........................................................
7.1. Introduction .......................................................... 347
7.2. Summary of the Study .............................................. 347
7.3. Conclusions .......................................................... 355
7.4. Recommendations .................................................. 359

REFERENCES ........................................................................

ANNEXURES........................................................................
A: Cover Letter .............................................................. 363
B: Questionnaire on Operational Risk Management .......... 363
C: Diagnostic Questionnaire ............................................ 363
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Risk Organisational Structure</td>
<td>26</td>
</tr>
<tr>
<td>2.2</td>
<td>Risk Management Structure</td>
<td>27</td>
</tr>
<tr>
<td>2.3</td>
<td>Model for a Risk Management Process</td>
<td>32</td>
</tr>
<tr>
<td>2.4</td>
<td>Administering the Risk Management Process – A Systematic and Continuous Effort</td>
<td>34</td>
</tr>
<tr>
<td>2.5</td>
<td>Risk Exposures</td>
<td>41</td>
</tr>
<tr>
<td>2.6</td>
<td>Risk Outcomes</td>
<td>57</td>
</tr>
<tr>
<td>2.7</td>
<td>A Classification of Risk</td>
<td>58</td>
</tr>
<tr>
<td>2.8</td>
<td>Business Risk versus Consequential Risk</td>
<td>60</td>
</tr>
<tr>
<td>2.9</td>
<td>Risk Management Framework at the Royal Bank Financial Group</td>
<td>61</td>
</tr>
<tr>
<td>2.10</td>
<td>The Banking Risk Spectrum</td>
<td>63</td>
</tr>
<tr>
<td>2.11</td>
<td>Two Broad Categories of Operational Risk</td>
<td>76</td>
</tr>
<tr>
<td>3.1</td>
<td>Interconnectivity of Operational Risk Exposure Dependencies</td>
<td>88</td>
</tr>
<tr>
<td>3.2</td>
<td>Key Areas of Operational Risk</td>
<td>90</td>
</tr>
<tr>
<td>3.3</td>
<td>The Operations Risk Environment</td>
<td>108</td>
</tr>
<tr>
<td>3.4</td>
<td>Guiding Principles for Operational Risk Measurement</td>
<td>118</td>
</tr>
<tr>
<td>3.5</td>
<td>Measurement Process of Operational Risk – Risk Assessment Framework</td>
<td>120</td>
</tr>
<tr>
<td>3.6</td>
<td>Fourth Step in the Measurement Process of Operational Risk</td>
<td>123</td>
</tr>
<tr>
<td>3.7</td>
<td>Summary of Risk Reporting</td>
<td>124</td>
</tr>
<tr>
<td>3.8</td>
<td>Risk Assessment Grid</td>
<td>133</td>
</tr>
<tr>
<td>3.9</td>
<td>Example of a Risk Map</td>
<td>137</td>
</tr>
<tr>
<td>3.10</td>
<td>Loss Exceedance Curves</td>
<td>143</td>
</tr>
<tr>
<td>3.11</td>
<td>Key Risk Mitigating Decisions</td>
<td>158</td>
</tr>
<tr>
<td>3.12</td>
<td>Operational Risk Management Practices</td>
<td>160</td>
</tr>
<tr>
<td>3.13</td>
<td>Three Pillars</td>
<td>161</td>
</tr>
<tr>
<td>3.14</td>
<td>Risk-Reporting Framework</td>
<td>173</td>
</tr>
<tr>
<td>3.15</td>
<td>Risk Information Flow</td>
<td>176</td>
</tr>
<tr>
<td>3.16</td>
<td>Operational Risk Reporting Structure</td>
<td>177</td>
</tr>
<tr>
<td>3.17</td>
<td>Prerequisites when Establishing a Central Operational Risk Unit</td>
<td>179</td>
</tr>
<tr>
<td>3.18</td>
<td>Structure of a Group Risk Management Function</td>
<td>180</td>
</tr>
<tr>
<td>3.19</td>
<td>Corporate Operational Risk Organisational Model</td>
<td>181</td>
</tr>
<tr>
<td>3.20</td>
<td>Managing Operational Risk</td>
<td>185</td>
</tr>
<tr>
<td>3.21</td>
<td>Risk Financing Element of the Risk Management Process</td>
<td>197</td>
</tr>
<tr>
<td>3.22</td>
<td>The Cost of Risk</td>
<td>199</td>
</tr>
<tr>
<td>4.1</td>
<td>Diagrammatical Illustration of the Research Methodology for this Study</td>
<td>254</td>
</tr>
<tr>
<td>5.1</td>
<td>Response Rate of Foreign and Local Banks</td>
<td>257</td>
</tr>
<tr>
<td>5.2</td>
<td>Response from the Types of Banks</td>
<td>257</td>
</tr>
<tr>
<td>5.3</td>
<td>Specific Occupations/Positions of the Respondents that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Completed the Research Questionnaires</td>
<td>258</td>
</tr>
<tr>
<td>5.4</td>
<td>Years of Experience of the Respondents</td>
<td>259</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.5</td>
<td>Arithmetic Mean – Current and Recommended Classification of Primary Risk Types</td>
<td>265</td>
</tr>
<tr>
<td>5.6</td>
<td>Percentage Variance – Current and Recommended Classification of Primary Risk Types</td>
<td>265</td>
</tr>
<tr>
<td>5.7</td>
<td><em>Spearman Correlation Coefficient</em> – Correlation of Current and Recommended Classification of Primary Risk Types</td>
<td>266</td>
</tr>
<tr>
<td>5.8</td>
<td>Arithmetic Mean – Current and Recommended Importance and Implementation of Primary Operational Risk Factors</td>
<td>269</td>
</tr>
<tr>
<td>5.9</td>
<td>Percentage Variance – Current and Recommended Importance and Management of Primary Operational Risk Factors</td>
<td>270</td>
</tr>
<tr>
<td>5.10</td>
<td><em>Spearman Correlation Coefficient</em> – Correlation of Current and Recommended Implementation and Management of Primary Operational Risk Factors</td>
<td>270</td>
</tr>
<tr>
<td>5.11</td>
<td>Arithmetic Mean – Current and Recommended Recognition of People Exposure Sub-Factors</td>
<td>273</td>
</tr>
<tr>
<td>5.12</td>
<td>Percentage Variance – Current and Recommended Recognition of People Exposure Sub-Factors</td>
<td>274</td>
</tr>
<tr>
<td>5.13</td>
<td><em>Spearman Correlation Coefficient</em> – Correlation of Current and Recommended Recognition of People Exposure Sub-Factors</td>
<td>275</td>
</tr>
<tr>
<td>5.14</td>
<td>Arithmetic Mean – Current and Recommended Recognition of Process Exposure Sub-Factors</td>
<td>277</td>
</tr>
<tr>
<td>5.15</td>
<td>Percentage Variance – Current and Recommended Recognition of Process Exposure Sub-Factors</td>
<td>278</td>
</tr>
<tr>
<td>5.16</td>
<td><em>Spearman Correlation Coefficient</em> – Correlation of Current and Recommended Recognition of Process Exposure Sub-Factors</td>
<td>279</td>
</tr>
<tr>
<td>5.17</td>
<td>Arithmetic Mean – Current and Recommended Recognition of System Exposure Sub-Factors</td>
<td>281</td>
</tr>
<tr>
<td>5.18</td>
<td>Percentage Variance – Current and Recommended Recognition of System Exposure Sub-Factors</td>
<td>282</td>
</tr>
<tr>
<td>5.19</td>
<td><em>Spearman Correlation Coefficient</em> – Correlation of Current and Recommended Recognition of System Exposure Sub-Factors</td>
<td>283</td>
</tr>
<tr>
<td>5.20</td>
<td>Arithmetic Mean – Current and Recommended Recognition of External Event Exposure Sub-Factors</td>
<td>286</td>
</tr>
<tr>
<td>5.21</td>
<td>Percentage Variance – Current and Recommended Recognition of External Event Exposure Sub-Factors</td>
<td>287</td>
</tr>
<tr>
<td>5.22</td>
<td><em>Spearman Correlation Coefficient</em> – Correlation of Current and Recommended Recognition of External Event Exposure Sub-Factors</td>
<td>288</td>
</tr>
<tr>
<td>5.23</td>
<td>Arithmetic Mean – Current and Recommended Recognition and Implementation of Elements of an Operational Risk Management Process</td>
<td>296</td>
</tr>
</tbody>
</table>
5.24. Percentage Variance – Current and Recommended Recognition and Implementation of Elements of an Operational Risk Management Process

5.25. Spearman Correlation Coefficient – Correlation of Current and Recommended Recognition and Implementation of Elements of an Operational Risk Management Process

5.26. Arithmetic Mean – Current and Recommended Recognition of Methods for Risk Identification

5.27. Percentage Variance – Current and Recommended Recognition of Methods for Risk Identification

5.28. Spearman Correlation Coefficient – Correlation of Current and Recommended Recognition of Methods for Risk Identification

5.29. Arithmetic Mean – Current and Recommended Recognition of Qualitative Methods to Measure Operational Risk

5.30. Percentage Variance – Current and Recommended Qualitative Methods to Measure Operational Risk

5.31. Spearman Correlation Coefficient – Correlation for the Current and Recommended Qualitative Methods to Measure Operational Risk

5.32. Arithmetic Mean – Current and Recommended Recognition of Quantitative Methods to Measure Operational Risk

5.33. Percentage Variance – Current and Recommended Recognition of Quantitative Methods to Measure Operational Risk

5.34. Spearman Correlation Coefficient – Correlation for the Current and Recommended Quantitative Methods to Measure Operational Risk

5.35. Arithmetic Mean – Current and Recommended Recognition of Control Measures for Operational Risk

5.36. Percentage Variance – Current and Recommended Recognition of Control Measures for Operational Risk

5.37. Spearman Correlation Coefficient – Correlation for the Current and Recommended Control Measures for Operational Risk

5.38. Arithmetic Mean – Current and Recommended Recognition of Operational Risk Financing Techniques

5.39. Percentage Variance – Current and Recommended Recognition of Operational Risk Financing Techniques

5.40. Spearman Correlation Coefficient – Correlation for the Current and Recommended Situation Regarding Operational Risk Financing Techniques

5.41. Arithmetic Mean – Current and Recommended Recognition of the Approaches to Assess Capital for Operational Risk

6.1. Framework of a Structured Approach to Operational Risk Management in a Banking Environment
LIST OF TABLES

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>The Nature of the Three Risk Perceptions</td>
<td>40</td>
</tr>
<tr>
<td>2.2</td>
<td>Risk Types</td>
<td>64</td>
</tr>
<tr>
<td>3.1</td>
<td>Causes and Effects</td>
<td>83</td>
</tr>
<tr>
<td>3.2</td>
<td>Causes and Events</td>
<td>84</td>
</tr>
<tr>
<td>3.3</td>
<td>Types of Operational Failure Risks</td>
<td>86</td>
</tr>
<tr>
<td>3.4</td>
<td>A Summary of Risks</td>
<td>94</td>
</tr>
<tr>
<td>3.5</td>
<td>Sources of Information in the Measurement Process of Operational Risk</td>
<td>120</td>
</tr>
<tr>
<td>3.6</td>
<td>Five-point Likelihood Continuum</td>
<td>121</td>
</tr>
<tr>
<td>3.7</td>
<td>Example of a Risk Assessment Report</td>
<td>122</td>
</tr>
<tr>
<td>3.8</td>
<td>Scale to Determine Impact</td>
<td>127</td>
</tr>
<tr>
<td>3.9</td>
<td>Scale to Determine the Likelihood of Occurrences</td>
<td>128</td>
</tr>
<tr>
<td>3.10</td>
<td>Potential Losses and Possible Causes of Risk</td>
<td>145</td>
</tr>
<tr>
<td>3.11</td>
<td>Sources of Loss Data</td>
<td>146</td>
</tr>
<tr>
<td>3.12</td>
<td>Common Measures</td>
<td>148</td>
</tr>
<tr>
<td>3.13</td>
<td>Applications and Limitations of Each Tool</td>
<td>152</td>
</tr>
<tr>
<td>3.14</td>
<td>Operational Risks Mapped to Mitigating Factors</td>
<td>154</td>
</tr>
<tr>
<td>3.15</td>
<td>Characteristics of Effective Controls</td>
<td>157</td>
</tr>
<tr>
<td>3.16</td>
<td>Risk Mitigation Practices and Tools</td>
<td>159</td>
</tr>
<tr>
<td>3.17</td>
<td>Example of Business Units, Business Lines and Indicators</td>
<td>212</td>
</tr>
<tr>
<td>4.1</td>
<td>Target Population for the Research</td>
<td>240</td>
</tr>
<tr>
<td>4.2</td>
<td>Likert-Type Scale to Measure the Response</td>
<td>243</td>
</tr>
<tr>
<td>4.3</td>
<td>Reliability Test of the Questionnaire</td>
<td>247</td>
</tr>
<tr>
<td>4.4</td>
<td>Measures of Central Tendency and Dispersion Permissible with Each Type of Measurement Scale</td>
<td>250</td>
</tr>
<tr>
<td>5.1</td>
<td>Grouping of Questions</td>
<td>260</td>
</tr>
<tr>
<td>5.2</td>
<td>Response – Current and Recommended Rating of the Primary Risk Factors of Operational Risk</td>
<td>267</td>
</tr>
<tr>
<td>5.3</td>
<td>Response – Current and Recommended Recognition of People Exposure Sub-Factors</td>
<td>271</td>
</tr>
<tr>
<td>5.4</td>
<td>Response – Current and Recommended Recognition of Process Exposure Sub-Factors</td>
<td>276</td>
</tr>
<tr>
<td>5.5</td>
<td>Response – Current and Recommended Recognition of System Exposure Sub-Factors</td>
<td>280</td>
</tr>
<tr>
<td>5.6</td>
<td>Response – Current and Recommended Recognition of External Event Exposure Sub-Factors</td>
<td>284</td>
</tr>
<tr>
<td>5.7</td>
<td>Response – Current and Recommended Adoption of a Formal Definition of Operational Risk by Banks</td>
<td>289</td>
</tr>
<tr>
<td>5.8</td>
<td>Response – Current and Recommended Recognition of the Importance of a Formal Risk Management Process</td>
<td>291</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.9.</td>
<td>Response – Current and Recommended Recognition of the Importance and Implementation of the Elements of an Operational Risk Management Process</td>
<td>293</td>
</tr>
<tr>
<td>5.10.</td>
<td>Response – Current and Recommended Alignment of an Operational Risk Management Process with Strategies and Objectives</td>
<td>298</td>
</tr>
<tr>
<td>5.11.</td>
<td>Response – Current and Recommended Rating of Operational Risk Management as an Integral Part of the Overall Risk Management Process</td>
<td>300</td>
</tr>
<tr>
<td>5.12.</td>
<td>Response – Current and Recommended Recognition of the Importance of Risk Identification as an Ongoing Process</td>
<td>302</td>
</tr>
<tr>
<td>5.13.</td>
<td>Response – Current and Recommended Recognition of Methods for Risk Identification</td>
<td>303</td>
</tr>
<tr>
<td>5.14.</td>
<td>Response – Current and Recommended Recognition of Qualitative Methods to Measure Operational Risk</td>
<td>306</td>
</tr>
<tr>
<td>5.15.</td>
<td>Response – Current and Recommended Recognition of Quantitative Methods to Measure Operational Risk</td>
<td>309</td>
</tr>
<tr>
<td>5.16.</td>
<td>Response – Current and Recommended Recognition of Control Measures for Operational Risk</td>
<td>312</td>
</tr>
<tr>
<td>5.17.</td>
<td>Response – Current and Recommended Structure for Operational Risk Management</td>
<td>315</td>
</tr>
<tr>
<td>5.18.</td>
<td>Response – Current and Recommended Recognition of Reporting Lines between the Risk Manager and the CEO</td>
<td>316</td>
</tr>
<tr>
<td>5.19.</td>
<td>Response – Current and Recommended Situation Regarding the Involvement of Internal Audit in the Management of Operational Risk</td>
<td>318</td>
</tr>
<tr>
<td>5.20.</td>
<td>Response – Current and Recommended Involvement of the Board of Directors in the Management of Operational Risk</td>
<td>319</td>
</tr>
<tr>
<td>5.21.</td>
<td>Response – Current and Recommended Involvement of Business Managers in the Management of Operational Risk</td>
<td>320</td>
</tr>
<tr>
<td>5.22.</td>
<td>Response – Current and Recommended Recognition of Risk Financing Techniques</td>
<td>322</td>
</tr>
<tr>
<td>5.23.</td>
<td>Response – Current and Recommended Awareness of the Basel Proposals by Banks</td>
<td>325</td>
</tr>
<tr>
<td>5.24.</td>
<td>Response – Current and Recommended Recognition of the Approaches to Assess Capital for Operational Risk</td>
<td>326</td>
</tr>
<tr>
<td>5.25.</td>
<td>Response – Current and Recommended Recognition of the Essentiality of a Minimum Capital Requirement for Operational Risk</td>
<td>327</td>
</tr>
<tr>
<td>6.1.</td>
<td>Sub-factors of the Main Underlying Risk Factors of Operational Risk</td>
<td>336</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

I am indebted to and thank sincerely the following persons for their assistance in completing this study:

Prof. Tom Cronje for his valuable suggestions and stimulating guidance.

Prof. Gawie du Toit for his guidance and support.

Everyone at Standard Bank of South Africa who supported me throughout this study.

All those members of the various banks for their willingness to share their experience and viewpoints on this subject with me.

My family, Salomé, Linda and Donovan for their support and understanding throughout this study.

JACKIE YOUNG
NOVEMBER 2001
EXECUTIVE SUMMARY

Operational risk was identified as one of the primary risk types that a bank faces. Neglected for many years, there is a growing awareness in the banking industry that the management of operational risk is crucial for their future existence. The effective management of operational risk, however, requires a structured approach. This study, therefore, investigates the management of operational risk by way of a literature study and empirical research in order to develop a framework for a structured approach to operational risk management in banking.

The framework comprises the primary risk factors of operational risk, namely: people, processes, systems and external events, as well as a definition of operational risk. The operational risk exposures that apply to the aforementioned primary risk factors are identified. It, furthermore, illustrates that operational risk management is an ongoing process that consists of risk identification, risk evaluation, risk control and risk financing and addresses the methods that could be applied in the management process.

As operational risk management in the banking industry is still in a development stage it is believed that this study could assist banks with establishing formal operational risk management processes.

The framework demarcates the area of operational risk properly and provides insight into all the activities that should be performed in the operational risk management process, but the following issues still require further research:
• The practical implementation of methods for the quantification of operational risk and determining a capital charge for it;
• The effect of the requirements of corporate governance on banks as it relates to the management of operational risk; and
• The interaction between operational risk and the other primary risk types to ensure an effective, enterprise-wide risk management process.

The framework that has been developed could also be applied to any other enterprise as operational risk management is not unique to banks and the basic principles are generic.
CHAPTER 1

INTRODUCTION

1.1. Background

Risk management in any organisation is a critical requirement for success. The importance thereof is also emphasised in modern banking environments. As such, the Annual Report of Standard Bank Investment Corporation (1998:51) states that risk management is vital to the bank and that it is a dynamic and an evolving area for which processes are constantly evaluated and reviewed to align it with international initiatives and best practices.

A bank provides financial services to its customers. To accomplish this, banks have established independent risk management functions to monitor and control risk on a daily basis.

The Basel Committee (1998c:17-25) provides examples of possible risks a bank may face, namely:

- Market/Price risk;
- Credit risk;
- Country risk;
- Liquidity risk;
- Interest-rate risk;
- Legal risk;
- Reputation risk; and
- Operational risk.
1.1.1. Market/Price Risk

Price risk is described as the risk of a decrease in the value of a financial portfolio as a result of adverse movement in market variables such as prices, currency exchange rates and interest rates. According to the Comptroller’s Handbook (1994:10), market risk is the exposure arising from adverse changes in the market value (the price) of an instrument or portfolio of instruments. Such exposures also refer to changes in the market value of derivative instruments due to movements, which occur in market factors such as underlying interest rates, equity prices and commodity prices or in the volatility of these factors.

It is clear from the above that price risk and market risk are synonymous terms and will be dealt with as such during the course of this research.

It is also evident from the above that price risk exists whenever a bank takes trading, banking and investment positions. Major exposure to price risk occurs in formal financial and over-the-counter markets, both in South Africa and internationally (Standard Bank Annual Report 1999:52).

Independent price risk management departments that monitor the two main factors, namely exposure to trading and interest-rate risks, exist in all banking groups.

1.1.2. Credit Risk

In the area of lending, credit risk arises through the provision of loans and contracts to support a client’s obligations. In trading activities, credit risk results from the possibility that the party with whom the bank is trading will be unable to fulfil its contractual obligation on or before the settlement date (Standard Bank Annual Report 1998:53). Falkena et al. (1989:77) state that credit risk is the risk
that a counterparty to a financial transaction will fail to perform according to the
terms and conditions of the contract. The actual loss suffered can, however, be
minimised through, for example, hedging, third party insurance, and recoveries
from the defaulter’s assets.

According to the Comptroller’s Handbook (1994:20), credit risk is the risk of
loss due to a counterparty’s unwillingness or inability to fulfil its financial
obligations.

A bank’s general approach to managing credit risk is, firstly, by way of overall
credit policy guidelines. These guidelines cover compliance with prescribed
sanctioning authority levels, avoidance of a high concentration of credit risk and
a regular review of credit limits. Secondly, counterparty creditworthiness is
evaluated and limits are set before credit is granted (Standard Bank Annual
Report 1998:53). Thirdly, loans are managed on an ongoing basis in order to
monitor excesses, arrears and large credit exposures.

All banks have specialised credit departments that manage this type of risk.

1.1.3. Interest-Rate Risk

Van Greuning and Bratanovic (2000:177) state that all financial institutions face
interest-rate risk. When interest rates fluctuate, a bank’s earnings, expenses and
the economic value of its assets are affected. Liabilities and off-balance-sheet
positions also change. The net effect of these changes is reflected in a bank’s
overall income and capital. Interest-rate risk is by nature a speculative type of
financial risk since interest rate movements can result in profits or losses.

Broadly speaking, interest rate risk management comprises various policies,
actions and techniques that a bank can use to reduce the risk of diminution in its
net equity resulting from adverse changes in interest rates (Van Greunin & Bratanovic 2000:177).

Alessandrini (1999:42) states that interest rates are known to fluctuate over the business cycle and that one could argue that interest-rate risk depend on the general state of the economy.

According to Buchanan (2000:1), interest-rate risk is a standard component of bank ratings since interest rates affect different areas of a bank’s finances, including net interest margins and the value of fixed-rate loan portfolios.

Van Greunin and Bratanovic (2000:178) discuss the following issues surrounding interest-rate risk:

- **Repricing risk.** The most common type of interest-rate risk arises from timing differences in the repricing of bank assets, liabilities, and off-balance-sheet positions. While such mismatches are a fundamental part of banking, variations in interest rates expose a bank’s income and the underlying value of its instruments to unanticipated fluctuations.

- **Basis risk.** This arises from the imperfect correlation between the adjustment of rates earned and paid on different instruments that otherwise have similar repricing characteristics. When interest rates change, these differences result in shifts in cash flow and earnings among assets, liabilities and off-balance-sheet instruments.

- **Yield curve risk.** Repricing mismatches also expose a bank to risk deriving from changes in the slope and shape of the yield curve. Yield curve risk materialises when unanticipated shifts have an adverse effect on a bank’s income or underlying economic value.
• **Optionality.** An increasingly important source of interest-rate risk stems from the options embedded in many banks’ assets and liabilities. Options may be “stand alone” derivative instruments, such as exchange-traded options, or they may be embedded within otherwise standard instruments. Such options may include various types of bonds or notes with call or put provisions, nonmaturity deposit instruments that give depositors the right to withdraw their money, or loans that borrowers may prepay without penalty.

1.1.4. **Country Risk**

Larr (1999:24) defines country risk as measured credit and market risk exposures, both cross-border and local currency-denominated. Effective and efficient country risk management requires structure and principles, which are provided through the interconnectivity and integration of assessments, policies, processes as well as internal and external information. The likelihood of effective country risk management is enhanced when a large number of affected individuals trust the system and adherence to the principles facilitates trust.

According to the Annual Report of Standard Bank (1998:54), a bank is exposed to country risk through transactions with counterparties in foreign countries. Risk arises when conditions or events in a particular country reduce the ability of counterparties in that country to meet their obligations. Such conditions include the imposition of exchange controls, a debt moratorium, insufficient foreign exchange, political instability and civil war.

Country risk is a particular form of concentration risk. Exposure to individual countries, not necessarily relating to credit only, must be within set limits. Limits are generally set on a risk-weighted basis using VaR (Value-at-Risk) methods.
and various other factors for higher risk countries in order to take a prudent view (Standard Bank Annual Report 1998:54).

Most banks have developed specific methods and apply certain rules to manage country risk.

1.1.5. Liquidity Risk

Liquidity can be described as a bank’s ability to meet deposit withdrawals and provide for the legitimate credit needs of its customers. According to Chorafas (1990:44), a bank should be carrying sufficient capital to meet its asset-growth objectives; cover unexpected loan losses; underwrite interest rate risk; account for fraud when it happens; and supports longer-term operating needs. The less liquid a bank, the greater the risk of failure. On the other hand, the more liquid a bank, the less capital is used for more remunerative purposes.

The Comptroller’s Handbook (1994:29) states that liquidity risk is the risk that a bank will be unable to meet its funding requirements, and that the ultimate responsibility for setting liquidity policies and reviewing liquidity decisions lies at the bank’s highest level of management. According to Standard Bank’s Annual Report (1998:52), liquidity risk is the risk that the bank has insufficient funds or marketable assets available to fulfil its obligations to counterparties.

Two elements of liquidity risk are identified according to a Standard Bank Board Memorandum (1995:8). The first arises from a bank’s balance sheet structure and refers to its ability to meet obligations when they fall due. Such obligations mainly comprise call, notice or term deposits and commitments to lend including unutilised overdraft facilities. The mix of these obligations and their incidence in any period of time will vary between banks, but the maintenance of the capacity to meet them is an essential principle of banking. The second element of liquidity
risk arises from bank trading activities and refers to the risk that a market loses depth in a particular instrument. This would make it difficult to transact in any volume without causing an adverse price movement. This element of liquidity risk is usually dealt with under price risk.

It is therefore evident that liquidity risk is determined by a bank’s ability to meet its obligations and controlled by its highest management level through applicable policies.

1.1.6. Legal Risk

According to Wilhelm (2000:326), legal (compliance) risk is the risk to earnings or capital arising from violations or non-conformance with laws, rules, regulations, prescribed policies or ethical standards. The risk also arises when laws or rules governing certain bank products or activities of the bank’s clients may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. It could lead to a diminished reputation; reduced franchise value; limited business opportunities; lessened expansion potential; and inability to enforce contracts.

Currently some banks are managing legal risk as part of a compliance management process or view it as a sub-risk of operational risk.

1.1.7. Reputation Risk

According to the Financial Services Authority (FSA) (1999:23), reputation risk is the potential that negative publicity about a bank’s business practices and/or internal controls, whether true or not, will cause a decline in the customer base, a reduction in revenue, or decrease in liquidity.
The larger the bank, the greater the financial cost of any reputation damage, as it will affect all product-lines, not just the one where the problem occurred. The time taken to discover errors or fraud can significantly affect the extent of the actual loss and the reputation damage. Reputation risk does not merely arise from large scale, once-off events. A series of small blows to a bank’s reputation may in aggregate be sufficient to destroy the bank.

According to Wilson (2000:380), reputation risk is the risk of an unexpected loss in share price or revenue due to the impact on the reputation of a firm. Such a loss in reputation could, for example, occur due to miss selling of derivatives. A good “control” or mitigating action for reputation risk is strong ethical values and integrity of the firm’s employees and a good public relations machine when things go wrong.

It seems that most banks manage reputation risk as a sub-risk of the other major risks like credit risk and operational risk. Reputation risk is also viewed as poor service and the inability to deliver products that may damage the bank’s relationship with clients and business partners. Dealing with undesirable counterparties and the negative sentiment of regulators contribute to this risk, which are currently being managed by some banks as reputation risk.

1.1.8. Operational Risk

Operational risk is defined in the Comptroller’s Handbook (1994:36) as the risk of loss occurring as a result of inadequate systems and control; human error; or management failure. Banks are exposed to operational risk in all activities. Schwartz and Smith (1997:322) give a similar description by stating that operational risk is the risk of loss arising from human error, management failure and fraud; or from shortcomings in systems or controls. They also state that
operational risk management is sometimes seen as a discreet aspect of overall risk management.

According to Standard Bank’s Annual Report (1998:57), the breakdown of controls and procedures for the efficient functioning of human, physical and operating resources is regarded as the prime source of operational risk. It is therefore defined as a potential loss arising from malfunctions in automated systems; failures in internal financial and administrative controls; and non-compliance with the bank’s policies and procedures. It also refers to losses as a result of error, fraud and other criminal activities.

According to a research performed by Erasmus (2000:10), Standard Bank defines operational risk as: “the risk of loss arising from breakdowns in internal controls established to ensure the proper functioning of people, systems and facilities.” He also states that ABSA defines it as “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.”

From the above-mentioned definitions it is clear that there is no consistency in the definitions of operational risk. This needs to be addressed during the research.

Operational risk could furthermore be sub-divided into various risk categories, of which Standard Bank’s Annual Report (1998:57) provides the following examples:

- *Transaction risk* - the risk involved in the execution, recording, interpretation, documentation or settlement of a transaction.
• *Operations control risk* - the risk of failure of established controls and procedures, processing errors and unauthorised or fraudulent transactions.

• *Systems risk* – which results from system malfunction or unavailability.

• *Legal or regulatory risk* - the risk that transactions or agreements with clients and other counterparties may not be legally enforceable.

• *Reputation risk* – which results from poor service and the actual or perceived inability to deliver products that may damage the bank’s relationships with clients and business partners.

• *Human resource risk* - includes the inability to recruit, train and retain the correct mix of skilled staff. This results in the inability to ensure an effective and efficient workforce to achieve the objectives and targets of the bank.

Examples, such as those mentioned above, could also cause some confusion and inconsistency towards establishing an agreed definition of operational risk for the banking industry.

Many banks are currently managing operational risk through their internal audit departments. The internal audit departments identify and monitor operational risk within the bank through regular reviews of its controls. Significant deficiencies are subsequently reported to, and reviewed by, the Group Board Audit Committee.

1.2. **Problem Statement**

It is evident from the preceding discussion of the various types of risk, that operational risk, unlike the major risks such as credit, market (price) and liquidity, is not specific and includes a wide spectrum of other risk factors. This
may lead to a “wide” approach by management and certain crucial aspects may be neglected. This in turn could lead to significant losses for a bank.

According to the FSA (1999:6), the main concern, from a regulator’s point of view, is to capture all types of risk and to ensure that there is sufficient capital in a bank to ensure protection up to a certain confidence level. It may be insignificant that operational risk is an umbrella term or is defined in process terms and lies alongside other types of risks. What seems important is that everything is covered in some way. However, if in the future a capital charge is to be allocated to operational risk, there should be a method in place to quantify operational risk. According to the FSA (1999:13), an essential first step towards quantifying operational risk is to determine some definitional common ground and from a cursory survey of the many definitions used in the market, it is clear that there is no consensus on a definition for operational risk. If capital is to be allocated for operational risk, this lack of homogeneity could present a problem.

In seeking to define operational risk many institutions, according to the FSA (1999:14), have concluded that it encompasses all those risks that are not categorised as market or credit risk (a negative approach). This may be a tidy solution to the problem of finding a meaningful definition, but it seems ultimately unsatisfactory on both a practical and an intellectual level. Given the shortcomings of the negative approach to a definition of operational risk, several institutions have attempted to define operational risk in positive terms, but still lack a common agreed definition which will classify it as a primary risk type alongside other risk types such as credit and market risk.

The FSA (1999:16) states that some areas of operational risk may be difficult to quantify, but the task would be even harder without consensus on the definition. Similarly if capital is to be allocated for operational risk, there needs to be a level
playing field among banks. A common accepted definition could be seen as the first step towards this goal and will form part of this study.

According to a survey launched by the Basel Committee (1998a:1), several common themes emerged relating to operational risk, namely:

- The awareness of operational risk among banks is increasing. Virtually all banks assign primary responsibility for managing operational risk to business line heads.
- While all banks surveyed have some framework for measuring operational risk, many indicated that they were only in the early stages of developing an operational risk measurement and monitoring framework. Furthermore, awareness of operational risk as a separate risk type is a relatively recent phenomenon in most banks. Few banks, at the time of the survey, measured and reported this risk on a regular basis. Many, however, tracked operational performance; and analysed and monitored loss experience.
- Many banks have identified significant conceptual issues and data needs, required for developing general measures of operational risk.

Banks, generally, operate in environments where risk often changes, hence the need for an efficient risk management process, categorised by risk type, to be able to address the specific risk factors. A clear description of all the risk factors will ensure the allocation of accountability and responsibility to deal with each of these. Such descriptions for operational risk still lacks as it seems that all the risk factors that can not be addressed under the primary risk types, for example credit, market, and liquidity risk types, are included under operational risk. This may lead to a situation where operational risk becomes a “dumping ground” for risk factors and may result in critical focus areas being neglected.
From the above it seems as if operational risk management, as one of management’s latest problem areas is still treated as a “wild card”. This presents a problem regarding the acceptance of a common definition of operational risk and the risk factors it comprises. Research is, therefore, necessary to determine the current status, conceptual issues and underlying factors of operational risk management, in order to provide a comprehensive description of this risk category and to differentiate it from other risks in a banking environment.

Work done by the Basel Committee (1998a:4) also indicates that there is uncertainty about which factors are important to operational risk. This may be caused by the absence of a direct relationship between risk factors usually identified and the size and frequency of losses. This is in contrast to market risk where changes in prices have an easily computed impact on the value of the bank’s trading portfolio and perhaps its credit risk. To date, there is little research that correlates operational risk factors to experiences with operational losses. Research in this field is necessary to determine the risk factors of operational risk, especially as operational losses tend to become a major issue with banks in South Africa.

Ludwig (1999:33) mentions that the importance of operational risk skyrockets in the context of heightened co-variance among risks, which results from increasing volumes; increased volatility; greater innovation; and computerisation. Thus it becomes increasingly important to distinguish between the risk factors by risk type in order to address it quickly and effectively.

Ludwig (1999:33) furthermore states that the co-variance among risk areas is foreseen to increase substantially, thus increasing the expected volatility of risks. For example, the impact of market events may be larger and quicker than ever before and what may start out as a market or credit risk may even translate into other areas like operational risk.
Another aspect, which needs to be researched, is the perception that operational risk is more difficult to hedge than other risk types, for example, credit risk which can be hedged via insurance and derivative instruments. In the past, diversification was seen as the ideal way of coping with both the frequency and impact of problems related to operational risk management. This is no longer popular in business, however, as effective risk management requires improved analyses, more research, comprehensive information and adequate controls (Clements 1999:39). In this regard it becomes imperative that internal identification and control measures be clearly stipulated and implemented to ensure that operational risk factors are timeously addressed. Neglecting to address operational risk factors can have a major effect on the business of a bank. It is stated that major operational risk losses are perceived to have low probabilities, but the impact could be very large and perhaps exceed those of credit or market risk (Basel 1998a:4).

Operational risk management is also affected by factors external to a bank. The political and economic situation of a country, for example, can have direct implications on a bank’s operations. Political decisions, for example, could impose higher taxes, which in turn could result in greater tax liabilities for a bank and lead to a reduction in net profits. The economic environment could also influence a bank’s business, for example, the inflation rate could affect interest rates, which will have a direct impact on a bank’s profitability. Research is thus needed to explore and analyse the external and internal factors and their impact on the management of operational risk with the aim to address and neutralise the possible negative affect they may have on a bank’s operations and business.
1.3. **Purpose of the Research**

The purpose of this research is to develop a structured approach to the management of operational risk in a banking environment. In order to attain this purpose the following objectives are formulated:

- To determine the various components of operational risk management in a banking environment through a comprehensive literature study. This will include the determination of a definition, the primary risk factors to be included as part of operational risk and the elements of an operational risk management process.
- To identify and critically assess the current and proposed national and international approach towards operational risk management in banking environments.
- To develop a framework for a structured approach to the management of operational risk, in order to ensure a positive contribution towards overall risk management in a banking environment.

The research will also establish a basis for future studies on operational risk management in a banking environment, as it is becoming increasingly critical for banks to include operational risk management as an integral part of the overall risk management process.

1.4. **Approach**

The research comprises three phases:

- Phase 1 – an extensive literature review.
- Phase 2 – planning and conducting the empirical research.
• Phase 3 – interpretation and integration of the literature and empirical research results to develop a structured approach to operational risk management.

*Phase 1* – An extensive literature study, based on a qualitative exploratory research framework, which includes the identification and analysis of key concepts. Clear definitions were set for applicable concepts and all relevant risk factors were identified. Furthermore, documented approaches to the management of operational risk were analysed.

*Phase 2* – Planning and conducting the empirical research. The research relating to the management of operational risk in a banking environment is explorative, based on a literature study and the experience, views and perceptions of senior executives concerned and involved in operational risk management. The empirical information was obtained from the main South African banking institutions and leading international banks. The international institutions are included to broaden the scope of the research. Information was gathered from senior managers in the above-mentioned institutions, through a structured questionnaire. The South African banks, which were approached during the research, are:

- ABSA Bank Ltd.
- BoE Bank Ltd.
- FirstRand Bank Ltd.
- HBZ Bank Ltd.
- Investec Bank Ltd.
- Mercantile Bank Ltd.
- Nedcor Bank Ltd.
- Old Mutual Bank Ltd.
- Saambou Bank Ltd.
• South African Bank of Athens Ltd.
• Standard Bank of South Africa Ltd.
• Peoples Bank Ltd.
• Unibank Ltd.

The following foreign banks were approached, firstly, because they are among the top financial institutions in the world according to a previous research study by Van der Merwe (1996:22), and, secondly, to obtain a world-wide geographical spread:

• Barclays Bank - London UK.
• Canadian Imperial Bank of Commerce.
• Citi Group.
• Commonwealth Bank of Australia - Australia.
• De Nederlandsche Bank – Amsterdam.
• Deutsche Bank.
• Lloyds Bank - London UK.
• Royal Bank of Scotland.
• Standard Bank London.
• Standard Chartered Bank – London.
• Union Bank of Switzerland – Zurich Switzerland.
• Westpac Banking Corporation – Australia.

The perspectives, personal experience and opinions of senior managers and executives of the above-mentioned banking institutions, form an important part of this research.

Phase 3 – Interpretation and integration of the literature and empirical research results in developing a structured approach to operational risk management. The
aim of this phase is to interpret the data in order to come to realistic conclusions and recommendations.

1.5. **Presentation Structure of the Study**

This study is structured into six chapters:

- *Chapter 1* consists of an introduction and background to the study.
- *Chapter 2* entails an overview of risk management in banking environments.
- *Chapter 3* provides a comprehensive literature study of existing theories and concepts regarding operational risk management in a banking environment.
- *Chapter 4* deals with the research methodology as well as the design of questions for the empirical research.
- *Chapter 5* focuses on the interpretation of the empirical research results by means of quantitative and qualitative analysis. The results are integrated with the theories and concepts identified during the literature review to develop a structured approach to operational risk management in a banking environment.
- *Chapter 6* deals with the development of a framework for a structured approach to operational risk management in a banking environment.
- *Chapter 7* provides a summary of the findings, conclusions and recommendations for further research.
CHAPTER 2

AN OVERVIEW OF RISK MANAGEMENT IN A BANKING ENVIRONMENT

2.1. Introduction

Any financial institution is subject to risks during the execution of daily activities. The risk of errors in operations or incorrect payments, for example, may negatively impact the market’s perception towards a bank, resulting in a loss of business and income, which may influence its long-term solvency. Risk management, therefore, is crucial to ensuring continued income generation and long-term solvency. Banking risks are significantly different from those of conventional business undertakings. This is largely due to the main trading activities of banks that relate to money and financial instruments as opposed to physical goods or commodities.

The special nature of banking risks has absorbed many resources in attempts to recognise, define and manage it. Despite this, and notwithstanding the relative maturity of the banking industry, there is no universally accepted approach to the taxonomy of risk (Standard Bank Report on Risk Management dated 7 October 1997). Goldman et al. (1998:29) add that even the term “risk management” does not have a universally agreed definition. The lack of a universal approach to risk classification has led to dissimilar and unrelated risks often being combined for the convenience of management and control. It has also resulted in the combination of risks under a composite name, more descriptive of the product or service, than of the underlying risk. This confirms the writer’s belief concerning operational risk in as far as it appears to be a “dumping ground” for those risk factors which cannot be associated with another major risk type.
This chapter will therefore firstly, focus on the terms: risk and risk management as well as the risk management process which can be applied to any risk type. Secondly, the classification of risks will be explored and operational risk will be demarcated to determine the main underlying risk factors that should be addressed when formulating an acceptable definition of operational risk, for the purposes of this study.

2.2. Risk, Risk Management and the Risk Management Process

Essinger and Rosen (1991:4) define risk as "... a measure of the anticipated difference between expectations and reality". This difference exists because the future is unknown, thus making it all the more important to manage risk.

Valsamakis et al. (1996:27) define risk "...as the presence of uncertainty, where there may be uncertainty as to the occurrence of an event producing a loss, and uncertainty as regards the outcome of the event..." Gitman (2000:237) defines risk in its most basic sense as the chance of financial loss. He also states that the term "risk" is used interchangeably with uncertainty to refer to the variability of returns associated with a given asset.

From the above definitions it is clear that risk evolves around uncertainty which might result in a loss to an organisation. Banks face a variety of risks that must be considered when servicing the needs of their customers. These needs include, for example, activities such as the provision of credit, acceptance of deposits, and the exchange of currencies on short notice, which enable customers to make the myriad payments necessitated by modern economic life (Falkena & Kok 1988:2).
The flexibility that permits the provision of these services could cause uncertainty. In this sense banks must manage the risk, caused by the uncertainties surrounding it, to stay in business. Hence the importance of understanding the concept of risk management in the context of addressing uncertainty to prevent or reduce financial losses or adverse effects.

2.2.1. Risk Management

Taylor (1983:220) made the following statement, in emphasising the importance of understanding the term “risk management”: “We clearly cannot eliminate risk, but we can manage it.” Although Goldman et al. (1998:29) state that the term “risk management” does not have a universally agreed definition, they describe it as a reference to the complete set of policies and procedures which organisations have in place to manage, monitor and control their exposure to risk. In this sense Green (1992:45) states that risk management is a combination of procedures, systems and persons, used to control the potential losses of a financial institution. It also entails an activity to deal with changing environments that affect a bank’s business. For example, a change in external factors, such as social, political or economic attitudes, may mean the emergence of new risk types, or more likely, changes in the weighting of importance that should be given to identified risk types.

Essinger and Rosen (1991:4) define risk management as an effective method for minimising the adverse effects of risk and maximising the benefits of incurring the risk. Adding to this viewpoint, Valsamakis et al. (1996:14) state that risk management is “…aimed at protecting the organisation, its people, assets, and profits, against consequences (adverse)...more particularly aimed at reducing the severity and variability of losses.” Another definition of risk management is that of Dickson (1989:18) who defines it as the identification, analysis and economic
control of those risks that threaten the assets or earning capacity of an organisation. Greene and Serbein (1983:3) define risk management as the process for conserving the earning power and assets of a firm by minimising the financial effect of accidental losses.

It is evident that risk management entails the control of risks facing an organisation and minimising the potential adverse effects of risk consequences. The focus of risk management, however, is dependent on and will change according to the nature of an organisation’s business. For example, the latest developments in electronic banking may have a significant influence on a bank’s business and the accompanying risks that should be considered as part of the risk management responsibilities. The rapid pace of technological innovation is likely to change the nature and scope of the risks which a bank face, forcing the bank to introduce processes that will enable management to respond to the current risks and to adjust to new risks. As such, Goldman et al. (1998:39) emphasise the importance of effective risk research and mention that it constitutes a significant part of risk management.

According to the Basel Committee (1998a:10), a risk management process, that includes the basic elements of assessing risks, controlling risk exposure and monitoring risks, will enable banks to respond to these challenges. It is therefore imperative to establish an integrated approach to risk management that forms the basis for the management of all the risk types.

2.2.2. Integrated Approach to Risk Management

As organisations encounter new types of risk while pursuing new business objectives, they need an integrated risk management framework for a holistic approach to risk management. Banks, for example, have increasingly become
exposed to compliance and regulatory risk as they have expanded their business. Credit risk, for example, has become more of an issue, as banks became more involved in trading over-the-counter derivatives. In addition, as banks became more heavily involved in trading activities, market risk has also become an important concern. It is clear, therefore, that an effective risk management function, which is based on a firm-wide and integrated framework, is necessary to ensure that all the risks are covered.

Schwartz and Smith (1997:410) identify a number of major trends and developments that confirm the need for an integrated risk management approach. These trends are the following:

- Globalisation and integration of financial markets have broken down the boundaries between countries and established a closer bond between international markets and economies. Thus, financial institutions with international investments and operations need to manage global risks on an integrated basis.
- Financial and derivative products involve various risk types, for example, credit, interest-rate and market risk, which highlights the need for an integrated approach to risk management.
- Technological developments and the dependency on computer systems also attribute to a wider risk exposure and the need for an integrated approach to risk management.

The above trends and developments have increased the complexity of risk management because risks can easily be transferred from one to another, for example market risk to credit risk, and they can also roam across counterparties, industries, markets, and countries (Schwartz & Smith 1997:411). It is thus clear that financial institutions need an integrated risk management approach.
However, to establish an integrated risk management approach, it is necessary to ensure the effectiveness of the components of an integrated risk management framework. Schwartz and Smith (1997:411) classify these components as follows:

- Organisational effectiveness;
- Risk performance management; and
- Systems technology.

2.2.2.1. Organisational Effectiveness

Schwartz and Smith (1997:411) state that the overall risk management framework is underpinned by three fundamental aspects of the organisation, namely:

- Business strategy which defines how the organisation will compete in target business segments;
- Organisational structure and people that provide management direction and control for business and risk management activities; and
- Incentive compensation system which provides rewards for key personnel.

Business Strategy. If an organisation’s strategy take risk into account, the organisation could increase its effectiveness of risk management by, for example, integrating risk management controls into their business processes and operations (Freeman 1999:16). Venkat (2000:589) adds that institutions can enhance the overall effectiveness of risk management by closely linking it to business strategy formulation. This can be accomplished by proactively acknowledging
and incorporating risk management considerations into business decisions regarding, for example, new ventures, products, trading strategies, and customer initiatives. The involvement, for example, of risk managers in developing business strategies and formulating relationships or product plans, ensures that business initiatives are consistent with risk management policies. Organisations that have a successful integrated business strategy and risk management process are proactive in defining markets that should be targeted and the risks they should accept or mitigate. From a strategic perspective, these organisations are better positioned to achieve a balance between originating business and managing risk (Schwartz & Smith 1997:411-412).

Organisational Structure. An organisational structure must be in place to facilitate communication about risk and to enforce the stature and clout the risk management team must have within the institution (Freeman 1999:15). A typical traditional organisation structure and risk management responsibility for a financial institution is shown in figure 2.1. This structure is based on functional areas and is often ineffective in managing risk as much risk is multi-dimensional and interrelates. Therefore various types of risk should not be segregated and managed by separate functions or departments. Schwartz and Smith (1997:415) indicate that most financial institutions have already initiated efforts to centralise risk functions that deal with all aspects of financial risk including credit, market, liquidity, technology and operational risk. To manage all risks on an integrated basis, this centralised risk management function has the following key responsibilities (Schwartz & Smith 1997:416):

- Establish risk management policies and procedures and reporting requirements.
- Coordinate or direct daily risk management activities.
- Measure global risks on a consistent and integrated basis and monitor development that may impact the organisation's exposures.
- Review and approve risk management methodologies and models.
- Work with the audit and compliance functions to ensure that business activities comply with laws, regulations and internal policies and procedures.
- Communicate risk management results to executive management and the board of directors.

**Figure 2.1: Risk Organisational Structure**

![Diagram of risk organisational structure]

Source: Schwartz & Smith (1997: 413)

Goldman *et al.* (1998:38) state that the way in which an organisation is structured to undertake risk management is of paramount importance. A central theme regarding the different approaches towards an organisational structure for risk management, is the recognition of a top-down approach of the process that is
illustrated in figure 2.2. Unless risk management is fully endorsed and actively supported by the Board and by the senior management of an organisation as an integral part of the way the organisation is managed, it cannot be effective. Thus the board needs to set out clearly the organisation's attitude towards risk and the assignment of responsibility for assessing and controlling risk. In addition, the board also needs to endorse the organisation's system of risk policies, risk limits and to review those arrangements on a systematic basis.

**Figure 2.2: Risk Management Structure**

Source: Goldman *et al.* (1998:29)

Consequently, after the endorsement of the risk policies, they need to be managed on a daily basis by appropriate levels of authority and a framework of risk committees.
Goldman et al. (1998:38) state that with an effective top-down management process, it is also essential that the risk management function must be established independently from the business areas and operated as a controlling or monitoring function. The role of the risk management function is to provide assurance to senior management and the board that the organisation is assessing its risk effectively and is complying with its own risk management standards.

*Incentive Compensation System.* Freeman (1999:17) states that the creation of a fair payment scheme for employees poses a major challenge and is a critical element of risk management. An organisation may have all the risk management tools, processes and systems in place, but without motivated personnel these would be useless. Schwartz and Smith (1997:416) mention that if incentive compensation is a key driver of human behavior then, by extension, it is also a key driver of risk management. The effectiveness of a financial institution in managing its risks is thus ultimately dependent on the collective decisions made and actions taken by its people. Hence, the importance of an effective incentive scheme to ensure a motivated workforce and that the right people are placed in the right positions.

### 2.2.2.2. Risk Performance Management

The core objective of any performance measurement system is to establish a benchmark that could be used to evaluate the economic return of business activities. Schwartz and Smith (1997:418) state that the key to measuring the risk performance of a business activity is to clearly establish a link between risk and return. Gitman (2000:239) describes return as the gain or loss experienced on an investment over a given period of time. He also states that there are three basic risk preference behaviors, which could be used to determine the link between risk and return, namely:
• *Risk-indifferent.* The attitude towards risk that requires no changes in return for an increase in risk.

• *Risk-averse.* The attitude towards risk that requires an increase in return for an increase in risk.

• *Risk-seeking.* The attitude towards risk whereby a decreased return would be accepted for an increase in risk.

Most managers tend to be risk-averse. Thus, before management accepts an increase in risk, they would require an improvement of performance that would increase return. However, in the modern banking industry it sometimes requires from management to take a risk-seeking approach towards risk to ensure a competitive edge over their rivals and a positive growth in business.

2.2.2.3. **Systems Technology**

An integrated risk management system should tie all the risk-generating factors together across the entire range of the financial institution’s activities. An integrated systems environment is therefore a key component of an integrated risk management framework because the output, such as reports and graphics, is imperative to support the measuring and managing of risk.

According to Williams (2000a:614), risk management needs technology that will allow information to be drawn from all levels within the organisation. She (2000a:634) also states that an institution’s ability to manage risk will determine its competitive advantage. This ability is, however, highly dependent on technology. Therefore, an institution’s ability to plan, create, implement and maintain risk information technology (IT) is regarded as a core competency.
2.2.3. Risk Management Process

Venkat (2000:592) is of the opinion that as financial institutions come under increasing pressure to improve shareholder value, they need to consider a business and risk management model that goes beyond merely measuring, monitoring and reporting risk. A model, which links the business mission and strategies to execution and to the elements of the risk management infrastructure, is required. An integrated approach to managing risk ensures full identification and awareness of significant risks, consistent risk measures and proper management controls, thus addressing the above-mentioned concerns. However, this integrated approach needs to be managed to ensure the effectiveness of risk management as well as the continued profitability and viability of a bank. This could be achieved by following a formal risk management process.

Venkat (2000:592) describes a risk management process as a structured cycle of control activities that provides management with assurance that all risks within the institution are being effectively managed. Although every institution will have its own unique approach to this process, depending on the potential effect of risk on its business, it is a process of identifying exposures to risk, choosing the best method of handling each exposure and implementing it accordingly (Kreitner et al. 1990:606-608). This, according to Kreitner et al. (1990:608), usually leaves the risk manager with four basic alternatives from which to choose when deciding how to manage risk, namely:

- **Risk avoidance.** An activity that may lead to risk exposure is identified and subsequently avoided. For example, in the 1980s many companies decided not to extend their operations to South Africa in order to avoid the risk of the political instability.
• **Risk assumption.** A specific risk is identified and accepted as part of daily activities. This usually is the case when the odds are strongly against an event happening or when the potential loss is low.

• **Risk transfer.** Risk exposure is identified and is subsequently transferred to a third party who is prepared to take the risk, for example, insurance companies. When an insurance company agrees to pay the losses of an insured, the risk faced by the insured is transferred.

• **Risk reduction.** The lessening of the uncertainty of a loss in a risky situation. For example, many companies go to great lengths to promote worker safety to avoid not only the financial costs of injury, but also the down time and disruption of work that would accompany it. Risk reduction can be achieved in different ways, for example, hazard reduction and loss reduction. Hazard reduction involves reducing the odds that a loss will occur and loss reduction involves reducing the severity of the loss.

Although the above points refer to alternatives on how to manage risk exposure, they do not indicate specific steps within a risk management process. It is usually up to the management of an organisation to determine and implement a risk management process which will be appropriate to their specific business. However, there are various viewpoints about the elements that should be included in such a risk management process.

In this regard Valsamakis *et al.* (2000:56-86) developed a model for a risk management process (see figure 2.3) which identifies four activities, namely:
- *Risk identification*. Every risk management programme must necessarily be put in motion by the process of risk identification.

- *Risk evaluation*. This activity entails the following:
  - The evaluation of both loss frequency and loss severity. This entails the measuring of the expected average loss and the maximum possible loss.
  - An analysis of the financial strength of the organisation which entails the assessment of the organisation’s risk retention capacity. This will indicate the impact of a given risk relative to the organisation's financial strength.

**Figure 2.3: Model for a Risk Management Process**

Source: Valsamakis *et al.* (2000: 80)

- *Risk control*. Risk control concerns the implementation of loss control programmes, which aim to achieve the following:
  - The reduction of the magnitude of the exposure;
- The reduction of the frequency of loss-producing events;
- The dealing with loss-producing events; and
- The recovery from loss-producing events.

- *Risk finance.* This step entails the financial provision for losses that may occur. It therefore selects the most efficient method of financially providing for the consequences of risk by means of the following alternatives:
  - The retention of risk by accepting it as a management concern (self-funding plan);
  - The combination of risk reducing strategies (e.g. hedging) by, for example, investing in futures contracts. This is a strategy that eliminates the risk associated with a future market commitment (Ritchken 1996:52);
  - The transfer of the cost of risk to a third party by means of, for example, insurance.

Mayland (1993:155) summarises risk management as a circle (see figure 2.4) of interrelated and continuing steps, namely exposure identification; risk assessment; risk control; and risk financing.

A brief explanation of these steps is as follows:

- *Exposure identification.* Mayland (1993:155) states that exposure identification is a continuous discovery process where alternative scenarios are explored as the operating environment changes over time.
Figure 2.4: Administering the Risk Management Process – A Systematic and Continuous Effort

Source: Mayland (1993:155)

- **Risk assessment.** This is described as attempts to measure the potential frequency and severity of the exposures that have been identified. This process is supported with regular reports to alert management to any changes in the risk assessment.

- **Risk control.** Risk control is seen as the application of techniques to reduce the probability of loss. These range from informal control to periodic review to interactive control.

- **Risk finance.** Risk finance is the last step of the process and refers to the provision of sufficient funds to meet loss situations as they occur. Funding can be accomplished by, for example, a variety of internal and external financial resources including insurance and risk-based pricing.
The Basel Committee on Banking Supervision (1998a:10-15) states that a risk management process should include the three basic elements, namely assessing risk, controlling risk exposure, and monitoring risk. A further description of the above is as follows:

- **Assessing risks.** This activity involves an analytical process of identifying risk and, where possible, to quantifying it.

- **Managing and controlling risks.** After assessing risks, management should take steps to manage and control it. This phase of a risk management process includes activities such as implementing security policies and measures; coordinating internal communications; evaluating and upgrading products and services; implementing measures to ensure that outsourcing risks are controlled and managed; and developing contingency plans.

- **Monitoring risks.** Ongoing monitoring is seen as an important aspect of any risk management process. This can, for example, be achieved by system testing and auditing.

Goldman et al. (1998:38-43) identify the following elements of a comprehensive risk management process:

- **Risk identification.** Risk identification refers to the need for a firm to define and understand the nature of the risk that it faces. This is an essential part of any risk management process.

- **Risk measurement.** Any risk management system must enable a firm to assess and manage the risk that it faces. In order to do this, a risk measurement methodology should be in place which allows comparisons to be made across the different risk types.
Risk policies and procedures. A risk management system has to be based on a set of written risk policies and procedures that are endorsed by the Board and implemented by the senior management of the firm.

Risk analysis and monitoring. Risk monitoring is seen as the operational process whereby the firm ensures that it is operating within its defined risk policies and procedures.

Risk reporting. This activity is closely linked to risk measurement and is seen as the process by which a firm reports on risk internally through its management information system and externally to its regulators and shareholders.

Risk verification and audit. The final component of a risk management process is to ensure that the risk management system and techniques, which the firm is using, are effective.

Venkat (2000:592) identifies the following steps of a risk management process:

- Risk awareness. Risk awareness is seen as a top-down commitment to risk management that acknowledges the exposure and risk impact of each business initiative on the overall risk profile of the firm.

- Risk assessment. Risk assessment enables the organisation to determine whether a specific transaction, portfolio or business is appropriate from a risk-return perspective. By assessing the sources of revenues and risks associated with a transaction or by business activity, management is able to assess both desired as well as unhealthy concentrations of risks within portfolios or businesses.
• **Operations.** It is imperative that appropriate procedures are in place to ensure that all aspects of business execution are undertaken in a controlled manner. In this sense, ensuring the integrity and accessibility of data is critical for meaningful risk management.

• **Measurement and control.** Measurement and control are seen as fundamental attributes of a risk management process. Measurement entails quantifying risk to determine the types and extent of risk. Risk measurement also serves as a basis for control mechanisms.

• **Evaluation.** This entails an examination of different risk-taking activities to ensure that there is adequate differentiation between those businesses or products that create value and those that destroy value. This aspect of the risk management process allows the firm to actively allocate and balance different risk types.

A comparison of the viewpoints of the different authors regarding the elements of a risk management process indicates that they differ from each other with regard to semantics and the classification of elements. For example: Some authors use the term assessment whilst others use the term evaluation and measurement in the same sense. With regard to the classification of elements some authors classify risk reporting, monitoring and risk policies and procedures as major elements of the risk management process, while other authors include all of it under an element which they call risk control. The aforementioned differences are negligible from a holistic point of view, and therefore the following classification will be used for purposes of this study:

• Risk identification that includes risk awareness.

• Risk evaluation that includes risk assessment and risk measuring.
- Risk control that includes issues such as risk reporting, monitoring and risk policies and procedures.
- Risk financing.

These elements are congruent with the model presented by Valsamakis. To substantiate this decision, it is necessary to take a more detailed look at the different elements.

2.3. **Elements of a Risk Management Process**

The elements of a risk management process, namely risk identification, risk evaluation, risk control, and risk financing were identified in the preceding section and will now be discussed in detail.

2.3.1. **Risk Identification**

Risk identification could be seen as the starting point of the risk management process. It is important that management realises that as a business grows, expands or improves, the exposure to risk will also change. Hence the importance of risk identification in the risk management process which obviously filters down to the other elements of the process.

The Financial and Management Accounting Committee (FMAC) (1999:13) states that risk is most often used in three distinct senses, namely risk as an opportunity, risk as a hazard or threat and risk as uncertainty. The above distinction could assist in the identification process, as well as in the management of the other elements of the process.
• **Risk as an opportunity.** Risk, as an opportunity is, according to the FMAC (1999:13), implicit in the concept that a relationship exists between risk and return. The greater the risk, the greater the potential return and the greater the potential for a loss. In this regard, the risk should be managed by using techniques to maximise the upside within the constraints of the organisation’s operating environment and minimising the downside of the risk.

• **Risk as a hazard or threat.** Risk as a hazard or threat usually refers to potential negative events (downside) such as financial loss, fraud, theft, damage to reputation, injury or death, systems failure or a lawsuit. In this regard, the management of the risk should include the positioning of management techniques to reduce the probability of the negative event without incurring excessive costs or paralising the organisation. Valsamakis *et al.* (1996:39) define hazard as relating to the environment surrounding the cause of loss.

• **Risk as an uncertainty.** According to the FMAC (1999:14), risk as an uncertainty refers to the distribution of all possible outcomes being negative or positive. In this context, risk management seeks to reduce the variance between anticipated outcomes and actual results.

According to the above-mentioned distinction it could be concluded that the two extremes are risk as a hazard and risk as an opportunity. Table 2.1 depicts the nature of the three risk perceptions in a summarised format.
Table 2.1: The Nature of the Three Risk Perceptions

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Uncertainty/Variance</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Traditional focus</td>
<td>• Control focused on the distribution of outcomes</td>
<td>• Investment focused</td>
</tr>
<tr>
<td>• Defensive in nature</td>
<td>• Hedging in nature</td>
<td>• Offensive in nature</td>
</tr>
<tr>
<td>• Purpose is to allocate resources to reduce the probability or impact</td>
<td>• Purpose is to reduce the variance between anticipated outcomes and actual results</td>
<td>• Purpose is to take action to achieve positive gains</td>
</tr>
<tr>
<td>of a negative event</td>
<td></td>
<td>• Requirements of a growth strategy due to implicit relationship between</td>
</tr>
<tr>
<td></td>
<td></td>
<td>risk and return</td>
</tr>
</tbody>
</table>

Source: FMAC (1999:15)

According to the J.P. Morgan/Arthur Andersen Guide to Corporate Risk Management (1997:13), only when the risk exposure is identified, can management work to transform the business’s risk position to bring it in line with its mandate to shareholders.

There are a vast number of exposures facing an organisation which should be taken into account depending on the business of the organisation. Examples of these exposures are reflected in figure 2.5. If management is aware of the exposures that the organisation face it could be more easily coupled to a specific risk type during risk identification.
Figure 2.5: Risk Exposures

Competitive Pressure
Powerful world players and new, aggressive entrepreneurs increase the need for acquisitions and alliances and threaten hostile takeover

Investors
Growth in both managed and individual investment plus greater global flexibility demands more information and disclosures

Globalisation
Bringing uncharted new markets, complex logistics, global supply chains and specialised local requirements

Financial Volatility
International capital flows, currency and interest rate volatility and complex derivative and hedging instruments

Source: The FMAC (1999:15)

It is, however, important to note and emphasise the fact that risk identification should be approached in a systematic way. The FMAC (1999: 17) states that this could be achieved by:

- Developing a sound understanding of the strategic and operational objectives of the organisation including critical success factors as well as the opportunities and threats related to the achievement of these objectives which represent risk.
- Analysing the functions undertaken within the organisation to identify the significant risks that flow from these objectives.
Katz (1995:199) states that a systematic approach is needed to ensure that all risk types are identified. This includes all forms of underlying risk factors per risk type, which can be documented and included in the risk management process.

Valsamakis et al. (1996:34) state that risk identification can be more systematically achieved when viewed from a macro- and micro-identification perspective.

- Macro-identification concerns the highlighting of major risk sources of which the consequences may have a very significant negative financial impact on the organisation.
- Micro-identification aims to identify risks within the major risk types that may be pivotal to physical risk management or risk control objectives.

Valsamakis et al. (2000:92) mention the following important features of risk identification:

- It is unlikely that one particular method or technique of identification will be sufficient to identify all the risk exposures and address all the associated problems. It would be more appropriate to consider a combination of methods to ensure that identification is as complete as possible.
- Various methods have developed since their application in solving problems within particular industries, making them more useful in those industries, than others. For example, a flow chart is an appropriate method of identifying risk in an industrial process which involves goods or materials moving through stages.
However, where flow processes are not the main issue, another method of identification would be more appropriate.

- The process of risk identification is assisted and enhanced by consultation with as many people outside the risk management department as possible, such as various line managers and others in the workforce who know the organisation and who possibly have their own ideas on the risks associated with the business.

- Risk identification is an ongoing process and should not be regarded as an isolated or once-off exercise. It is essential that risks, which have been identified, be monitored and new risks highlighted.

- Finally, risk identification entails a certain degree of creativity. While past routines used in risk identification provide some system and rigour to the activity, there should be no limit imposed on lateral approaches to identification.

2.3.2. Risk Evaluation

Once risks have been identified, they should be evaluated. Valsamakis et al. (1996:104) define risk evaluation as the appraisal, the assessment or the finding of the numerical expression of risk. Risk evaluation thus entails the quantification of the risk and determining its possible impact on an organisation (Valsamakis et al. 2000:26). According to Head (1986:50), the process of risk evaluation is the analysis of loss exposure, where attention is focused on how frequent and how severe accidents are likely to be and how they may interfere with the organisation's success. Valsamakis et al. (2000:26) also state that risk evaluation and assessment concern the following:
• The evaluation of both loss frequency and loss severity – an analysis that will provide, *inter alia*, the two significant measures of expected average loss and maximum possible loss.

• An analysis of the financial strength of the organisation which entails the assessment of the firm’s risk potential capacity. The objective is to ascertain what the impact of a given risk might be relative to the financial strength of the firm.

According to KPMG (1998:8), a generally accepted measure of risk is a combination of its likelihood (how likely it is to occur) and its impact (the consequence of the risk).

The *impact* is considered as the potential financial, reputational or other damage in any single year, using a combination of both quantitative and qualitative factors (KPMG 1998:8). The FMAC (1999:17) states that the assessment of the potential impact of a particular risk may be complicated by the fact that a range of possible outcomes may exist or that the risk may occur a number of times during a given period of time.

The *likelihood* that a risk might occur should be assessed by taking into account the current conditions and processes to mitigate the chance of the event occurring. Valsamakis *et al.* (1996:26) state that managing risk implies not only the financial provision for the consequences of an event, but the effort to:

• reduce or minimise the likelihood of the loss-producing event occurring; and

• reduce or minimise the adverse effects once the event has occurred.
In order to determine the impact and likelihood of a risk, appropriate techniques should be applied to measure it. Goldman et al. (1998:39) state that a firm has to develop a measurement methodology that allows a comparison of risks. This will enable risk considerations to be factored into performance measurement and capital allocation decisions. Katz (1995:164) states that when making an assessment, the following should be considered:

- The significance of the risk under consideration and whether the probability for loss is high, medium or low;
- The timing of the risk;
- The likelihood that the risk, if unmanaged or not managed properly, will eventually turn into a material financial loss;
- The potential financial impact;
- The potential embarrassment that a loss may incur;
- The manner in which the risk should be controlled; and
- The cost of control against the potential loss.

Schwartz and Smith (1997:260) argue that many risk variables such as political, personnel, regulatory and liquidity are often difficult to capture through quantitative techniques and yet can cause significant risk exposures for an organisation. They (1997:260) also argue that it seems that the simplest approach to estimate risk is to ask the business manager to decide whether the impact of a loss arising from each identified risk type would be high, medium or low. Another, more quantitative approach is to ask the business manager to estimate both the possible financial loss arising from the risk and the likelihood of that loss occurring.

Accurate measures of potential exposures are, notwithstanding the above, critical to making conscious risk and return trade-offs. Although sophisticated
methodologies for measuring risk are becoming available, it is important to apply the correct methodology to the identified risk factors per risk type. The following are examples of such methodologies:

- **Value at Risk (VaR)** - shows increasing promise as a risk measurement tool, especially with regard to financial instruments. Goldman et al. (1998:81) state that although VaR has a narrow meaning as a unit of risk, the general convention will be followed by using it to refer to any model that combines an ability to mark-to-market, with an ability to assign probabilities to the future states of underlying risk factors. Schwartz and Smith (1997:265) also point out that the VaR concept is quite general and can be applied on a firm-wide basis to financial and non-financial firms to assist in the management of risk.

- **Stress testing** - determines, for example, how portfolios may behave under extreme conditions and involves revaluing the entire portfolio under these extreme conditions (Jones & Sheikh 1999:52).

- **Historical simulation** - determines events that may induce extreme gains or losses by using all historical interest rate changes and equity returns to revalue the current portfolio under historical outcomes (Jones & Sheikh 1999:52).

- **Model risk measures** - measure potential losses when mathematical decision-making procedures are not precise enough to handle adverse market conditions or human error (Duarte 1997:60).

As soon as a risk type and the exposure to the organisation have been identified, the process of risk management should continue by means of risk control.
2.3.3. Risk Control

Having performed a risk assessment, a bank’s management should take steps to manage and control the risks it faces. Valsamakis et al. (1996:120) define risk control as methods of countering risk. In a broader sense it includes, firstly, all activities conducted for the purpose of eliminating or reducing the factors that may cause loss to the organisation. Secondly, it minimises the loss that occurs when preventative methods have not been fully effective. Risk control can thus be seen as an activity to mitigate risk.

It is evident that effective risk control requires a well-supported risk management programme. The programme should be governed by a clearly defined risk management strategy which, in turn, should be consistent with business strategies and objectives. Katz (1995:161) states that these controls (programmes) need to be established for that risk it intends to manage.

The Basel Committee (1998c:11) states that having made an assessment of risks, bank management should take steps to manage and control these risks. This phase of the risk management process could include activities such as implementing policies and procedures, internal controls, risk reporting and decision-making, as well as, determining an organisational structure to form the basis of the process.

Venkat (2000:587) states that an effective risk management framework balances the infrastructure aspects of risk management, such as, roles, responsibilities, accountabilities, policies, methodologies, controls and information tools, with the more qualitative aspects of risk management, such as, philosophy, culture, training, awareness, and appropriate behavioral reinforcement. He (2000:594)
states that the risk management infrastructure forms the foundation for the risk management framework. It provides the organisational, analytic, operational, and system(s) support for effectively executing the risk management process and consists of the following:

- A central and independent risk management unit with clearly defined roles and participation in the strategic decision-making process.
- Formulated policies and procedures that clearly define and communicate the risk management process.
- Consistent methodologies for risk measurement that capture the potential for losses, foregone opportunities and risk diversification effects across different risk categories.
- Limit structures that set maximum tolerances in relation to capital and the firm's risk-taking philosophy.
- Comprehensive management reports that communicate risk on a periodic basis.
- Information technology to satisfy risk information needs throughout the organisation.

Organisational structure. Understanding the organisational structure of a firm is at the core of understanding how it needs to approach the challenge of risk control. The foundation for an effective risk control environment is an organisational structure that provides adequate supervision of risk management activities, appropriate segregation of duties and proper reporting of positions and exposures (Morgan & Andersen 1997:66).

According to Schwartz and Smith (1997:415), several financial institutions have central risk functions that deal with all aspects of financial risks, including credit,
market, liquidity, technology and operational risks. The key responsibilities of central risk management functions normally include:

- Establishing risk management policies and procedures, including management reporting requirements;
- Coordinating or directing day-to-day risk management activities through risk limits, capital allocation, and transaction approval processes;
- Measuring global risks on a consistent and integrated basis and monitoring developments that may influence the organisation's risk exposures;
- Reviewing and approving risk management methodologies and models;
- Working with audit and compliance functions to ensure that business activities comply with laws, regulations, policies and procedures; and
- Communicating risk management results to executive management and board of directors as well as other interested parties.

It is evident that the modern outlook regarding risk management is to establish a centralised management structure within an organisation, as a controlling body, to ensure effective overall risk management. Chapter 3 deals with this issue in more detail.

*Policy and Procedures.* Formal policies and procedures provide consistency and discipline within an organisation and can also be effective in keeping the focus on its objectives. According to Morgan and Andersen (1997:71), effective risk
management policies should be concise, yet provide adequate detail on the following:

- Exposure definition;
- Exposure measurement methodologies;
- Authorised risk management strategies and related limits; and
- Performance measures by which the risk programme will be evaluated.

Morgan and Andersen (1997:75) also state that procedure documents should support the policies and provide additional detail which establishes the following:

- Responsibilities within various functions;
- Authorised transactors;
- Reporting requirements, including frequency;
- Confirmation, processing, and settlement procedures;
- Valuation;
- Credit risk measurement activities; and
- Accounting and financial reporting requirements.

To ensure the positive contribution of policies and procedures to an organisation, it is important they are updated and in line with the organisation's strategy, business and internal operations.

**Internal controls.** As soon as the organisation’s policies and procedures have been approved, internal controls should be established to ensure their implementation and effectiveness. The Basel Committee (1998a:8) states that internal control is a process that affects everyone from the board of directors to
all levels of personnel. It is a continuous operating process at all levels within a bank. Its main objectives, identified by the Basel Committee, are:

- efficiency and effectiveness of activities;
- reliability, completeness and timeliness of financial and management information; and
- compliance with applicable laws and regulations.

According to Katz (1995:26), internal controls should include a total system of control to ensure an orderly and efficient execution of business activities; adherence to management policies; the safeguarding of the assets of the business; and the completeness of financial books and records. He (1995:26) also states that internal control standards involve the following:

- Dictating the conditions under which business activities take place;
- Determining the extent of specific controls that affect each transaction or activity; and
- Implementing controls that ultimately enforce, supervise and maintain discipline over the entire management process.

Internal controls can be divided into primary and secondary controls. Primary controls prevent a mistake occurring and secondary controls act as a safety net by minimising adverse results (Schwartz & Smith 1997:43). The Basel Committee (1998a:10) states that a sound internal control process is critical to a bank’s ability to meet its goals and to maintain financial viability. Subsequently, they identified the following interrelated elements of internal control:

• *Management direction and the control culture*. The board of directors, for example, should provide governance, guidance and direction to senior management. They are also responsible for approving and reviewing the overall business strategies and significant policies of the organisation as well as the organisational structure. Top management is also responsible for promoting integrity and high standards of ethics; and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal control.

• *Risk recognition and assessment*. An effective internal control system requires that the risks that could adversely affect the achievement of a bank’s goals are recognised and continually assessed.

• *Control activities and segregation of duties*. Control activities should be an integral part of the daily activities of a bank. This necessitates an appropriate control structure with defined control activities performed on every business level. This, in turn, also necessitates a segregation of duties in order to ensure that personnel, for example, are not assigned conflicting responsibilities that could have a negative effect on business.

• *Information and communication*. An effective internal control system requires that there is comprehensive internal financial, operational and compliance information, as well as, external market information about events and conditions that are relevant to decision-making. An effective communication system should exist to ensure that the information is available to those who need it.
• Monitoring activities and correcting deficiencies. The overall effectiveness of a bank’s internal controls should be monitored continuously. Monitoring of key risks should be part of the daily activities of a bank as well as periodic evaluations by the business lines and internal audit.

It is obvious that effective internal controls will add to the effectiveness of a bank’s risk management process. It is important, however, to have a supportive organisational structure and the active involvement of personnel on all management levels.

Risk reporting and decision-making. Goldman et al. (1998:42) state that risk reporting is the process whereby the firm reports on risk internally, through its management information system, and externally, to its regulators and shareholders. This is an important aspect of risk control that should be enhanced to ensure that the applicable data is available to management for decision-making. Recently banks started reporting to the Registrar of Banks, in terms of Regulation 37(5) of the Banks Act, 1990, on the material malfunction and continuous concerns of their business. This can be seen as an essential element of the risk management process that entails the identification and evaluation of key risk types. While the ultimate report to the Registrar of Banks is an essential issue in this regard, continuous management attention and communication is required.

2.3.4. Risk Financing

According to Ritchie and Marshall (1993:245), risk management may be seen as part of the organisation’s general financial planning and control activity. Thus when managing risk, the cost of risk, as the final step of a risk management
process, is an important issue to consider. Valsamakis et al. (1996:243) state that through systematic identification, evaluation and control, the severity and frequency of losses can be reduced. The risk management process, however, must also include the element of financing. They also argue that risk financing becomes visible when consideration is given to the pursuit of minimising the total cost of risk to an organisation.

A risk management process should be cost effective and expenditure should be to the benefit of the organisation. Hence, the cost of risk should reflect cost-efficiency and ensure optimal financing. Valsamakis et al. (1996:244) define the cost-of-risk as the sum of:

- net insurance premiums;
- unreimbursed losses;
- risk control and loss prevention expenses; and
- administration costs.

The basic concept of risk financing is to ensure that the cost of risk and of the risk management process do not exceed the potential benefits they have for the organisation. A risk management process can therefore require a pre-financing or post-financing policy. The risk type plays an important role in dictating the risk financing policy. An example of a pre-financing policy is financing by means of insurance and self-funding, while post-financing could consist of cash resources, debt and equity finance (Valsamakis et al. 1996:249).

The writer is of the opinion that the management of every risk type must be subject to a financial evaluation process to determine its contribution towards the overall effectiveness and profitability of an organisation by comparing its cost to benefits.
During the discussion of the risk management process it is evident that the identified model (see figure 2.3) could be used generically for all risk types. However, the methodologies for measuring, evaluating, controlling and financing risk types may differ radically according to the risk type. To be able to distinguish between the risk types and to determine the approach to and views of operational risk, it is necessary to discuss the classification of risks. This is the focus of the next section.

2.4. Risk Classification

Different organisations are exposed to different risks. For example, financial institutions, like banks and manufacturing companies are subject to different risk types. Although the broad grouping of risk types might be similar, they could differ from organisation to organisation, depending on the organisation’s primary business. Mills and Stiles (1994:215) state that few business opportunities have the same degree of risk attached to them and “The real challenge is to get a handle upon such risks”. As such, a classification of the risk types that an organisation faces could enhance the risk management process.

Venkat (2000:585) states that most managers would agree that it is neither possible nor desirable to completely eliminate risk from the business proposition. What is required is an understanding of all the risks that arise from a particular business and then the effective management of these risks.

2.4.1. Broad Groupings of Risks

Valsamakis et al. (2000:35) state that different people may classify risks in various arbitrary ways. For example, Doherty (1985) as well as Greene and
Serbein (1983) approach risk classification against the backdrop of an organisation seeking to earn a profit making it susceptible to the collective effect of various risks. They classify risks as follows:

**Doherty**
- Marketing risk
- Finance risk
- Resource management risk
- Environmental risk

**Greene and Serbein**
- Property and personnel
- Marketing
- Finance
- Personnel and production
- Environment

The aforementioned classifications of risk do not differentiate between the basic characteristics of the risk types. Valsamakis *et al.* (1996:28), however, focus on these characteristics by grouping all risks into two broad categories, namely, pure risks and speculative risks. Pure risks are those risks that concern the possibility of loss or no loss, for example, the possibility of fire loss to a firm’s plant and equipment, to liability claims due to defective products, and to possible theft of assets and fraud. Those risks that offer a chance of gain or loss are termed speculative risks.

The classification of Valsamakis is the same as the classification of Athearn *et al.* (1988:3). This distinction between pure and speculative risk is illustrated in figure 2.6.
Figure 2.6: Risk Outcomes

Pure Risk

Speculative Risk

Loss  No loss  Loss  No change  Gain

Source: Athearn et al. (1988:3)

Valsamakis et al. (1996:28 & 304) state that the methods of treating these two categories of risk differ. The financial consequences associated with pure risks can often be mitigated by risk management techniques, such as insurance, while speculative risks may be treated by techniques such as hedging.

Kreitner et al. (1990:606) have a similar approach to the classification of risks as they also classify all risks as either pure or speculative. They, however, integrate the risks that an individual faces and those that an organisation faces into one diagram. Figure 2.7 outlines this classification (Kreitner et al. 1990:606).
Figure 2.7: A Classification of Risk

Source: Kreitner et al. (1990:606)
The aforementioned gives an overview of broad classifications of risk types as seen by various authors, irrespective of the type of business of the organisation. The next section focuses on the classification of risk types from a financial services industry point of view.

2.4.2. Classification of Risks from the Financial Services Industry Point of View

Goldman et al. (1998:34) divide risks into the following broad groups:

- **Business risks** – Market and credit risks can be thought of as business risks, that is, the risks a financial institution chooses to assume with the objective of making money;
- **Consequential risks** – By contrast the other risks, which a firm faces, are not assumed with the view of remuneration, but are consequential risks, That is, risks that inevitably arise as a result of being in the financial services business.

This approach by Goldman et al. is graphically depicted in figure 2.8.

The Royal Bank Finance Group has a three-tiered model, which is used to identify and analyse risk facing the organisation as a whole (see figure 2.9). The levels of the model are described by the Financial and Management Accounting Committee (1999:16) as follows:

- **Level 1 risks**: Systemic risks are the political, economic, social and financial risks over which an organisation has very little
control. These create the environment within which the organisation must operate.

- **Level 2 risks**: These are factors that the organisation cannot control but can influence. The Royal Bank Financial Group identifies several level 2 risks, including competitive, reputation and regulatory risks.

- **Level 3 risks**: These risks vary within each industry but can be generally viewed as risks that an organisation can have a great deal of influence over, for example, credit, market, liquidity, technology, operating and people risks.

**Figure 2.8: Business Risk versus Consequential Risk**

Source: Goldman *et al.* (1998:34)
Figure 2.9: Risk Management Framework at the Royal Bank Financial Group

Source: FMAC (1999:16)

Van Greuning and Bratanovic (2000:3-4) state that banks are subject to a wide array of risks in the course of their operations, but that they can be classified into four main categories, namely, financial, operational, business and event risks. These risk categories are depicted in figure 2.10 and can briefly be described as follows:

- **Financial risks** comprise two types of risk. Firstly, pure risk, which includes liquidity, credit and solvency risks that may result in a loss if not properly managed. Secondly, speculative risks that are based on financial arbitrage and may result in a profit if the
arbitrage is correct, or loss if it is incorrect. The main categories are interest-rate risk, currency risk and market risk.

- **Operational risks** are related to a bank’s overall business strategy; organisation; function of internal systems; compliance with bank policies and procedures; and measures against mismanagement and fraud:

- **Business risks** are associated with a bank’s business environment and include macro-economic policy concerns; legal and regulatory factors; the financial sector infrastructure and payment system; and the overall systemic risk for operations.

- **Event risks** include all types of exogenous risks that could jeopardise a bank’s operations or undermine its financial condition and capital adequacy.

The Group of Thirty classifies risks into four main categories, namely (Morgan & Andersen 1997:48):

- **Market risk** – Uncertainty, related to the change in value, or liquidity of a portfolio of financial instruments, resulting from changes in the financial markets.

- **Credit risk** – Degree of uncertainty about counterparties’ ability to fulfill their legal obligations.

- **Operational risk** – Uncertainty related to losses resulting from inadequate systems or controls, human error or management failure.

- **Legal risk** – Uncertainty regarding the possibility that a contract will not be enforceable.
Figure 2.10: The Banking Risk Spectrum

Source: Van Greuning & Bratanovic (2000:4)

Goldman et al. (1998:31) mention that while there is no single agreed listing of all the relevant risk types, the seven categories identified by The Basel...
Committee in their 1994 papers on risk management provide a useful reference. These are shown in table 2.2.

**Table 2.2: Risk Types**

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market risk</td>
<td>The risk to an institution’s financial condition arising from adverse movements in the level or volatility of market prices.</td>
</tr>
<tr>
<td>Credit risk</td>
<td>The risk that a counterparty will fail to perform on an obligation owed to the firm.</td>
</tr>
<tr>
<td>Liquidity risk</td>
<td>An institution faces two types of liquidity risk: one related to specific products or markets; the other related to the general funding of the institution’s activities.</td>
</tr>
<tr>
<td>Operational risk</td>
<td>The risk that deficiencies in information systems or internal controls will result in unexpected loss. The risk is associated with human error, system failures and inadequate procedures and controls.</td>
</tr>
<tr>
<td>Legal risk</td>
<td>The risk that contracts is not legally enforceable or documented correctly.</td>
</tr>
<tr>
<td>Reputation risk</td>
<td>The risk that any action taken by a firm or its employees creates a negative perception in the external market place.</td>
</tr>
<tr>
<td>Settlement risk</td>
<td>The risk that a firm will not receive funds or instruments from its counterparties at the expected time.</td>
</tr>
</tbody>
</table>

Source: Adapted from Goldman *et al.* (1998:32)

Venkat (2000:587) states that risks could be broadly classified into four risk types, namely:
• **Market risk** – The risk of loss due to adverse changes in financial markets.

• **Credit risk** – The risk of loss arising from the failure of a counterparty to perform on a financial obligation.

• **Insurance risk** – The risk of loss due to claims experience or expenses exceeding expected levels reflected in premiums.

• **Operational risk** – The risk of loss resulting from human acts, technology failure and breakdown in internal controls, disaster or the impact of external factors.

As mentioned previously, the risk classification is dependent on the type of business of the organisation. For example, The Basel Committee (1998c:17-25) provides examples of possible risks a bank may face from an electronic banking point of view. These include the following:

• Operational risk.

• Reputation risk.

• Legal risk.

• Credit risk.

• Liquidity risk.

• Interest-rate risk.

• Market risk.

• Country risk.

Freeman (1999:45) classifies the various risk types as business risk, operational risk, insurance risk, credit risk and market risk, while Stampleman (1998:34) states that the risks a bank is likely to face, especially from an electronic point of view, are:
• Operational risk.
• Reputation risk.
• Legal risk.
• Credit risk.
• Liquidity risk.

Schwartz and Smith (1997:355) state that one should be able to compare and correlate every possible quantifiable risk including market risk, credit risk, liquidity risk, operational risk, regulatory risk and “human error” risk. During an interview with the CEO of the Commerce Exchange Bank (Mike Clemens), Foster (1998:13) identified the following risk types:

• Credit risk.
• Market risk.
• Liquidity risk.
• Operational risk.
• Compliance risk.
• Strategic risk.
• Reputation risk.

Falkena and Kok (1988:4) categorise bank-related risks as follows:

• **Credit risk** – The risk of the borrower being unable to repay his loans.
• **Interest-rate risk** – Interest-rate risk exposure is a characteristic of any financial institution and stems from assets and liabilities maturing at different times (Falkena & Kok 1988:37).
- **Liquidity risk** – Banks have to manage their liquidity risk to be able to meet unexpected demands for cash, money transfers or term loans without hesitation or delay.

- **Currency risk** – Those banks involved in international finance faces currency risk. This entails the risk of the relative values of currencies changing to the detriment of banks.

- **Investment risk** – Changes in interest rates, stock or property prices will impact on the market value of a bank’s marketable securities and fixed assets.

- **Capital risk** – Banks have to assess and manage their capital risk exposure. This refers to the risk of a bank’s own capital resources being adversely affected by external developments. Banks have to maintain adequate capital resources in order to protect their depositors against the impact of, for example, operating losses or capital losses on investments.

Mckenzie (1992:4-9), on the other hand, concentrates on derivatives when she classifies risks into the following main categories:

- **Market-price risk** – The risk that the value of a financial instrument will decline as a result of changes in exchange or interest rates.

- **Credit risk** – The risk that a counterparty to a financial transaction will fail to perform according to the terms and conditions of the contract, causing the other party to suffer a financial loss.

- **Market liquidity risk** – The risk that a financial instrument cannot be sold quickly at prices which equate to its market value.

- **Settlement risk** – The risk that at a particular settlement or contract maturity point, the financial institution pays out funds before it is
certain that it will receive the appropriate payment from the counterparty.

- **Transaction and technology risk** – The risk that a financial loss is incurred as a result of a transaction not being executed properly. Some types of settlement errors are a subject of transaction risk and the nature of the risks relating to each type of transaction will depend on:

  - Quality of controls, systems and personnel;
  - Transaction volumes; and
  - Complexity of the particular instrument.

From the above discussion on the approaches of different authors, it is clear that there are different viewpoints on the classification of risk types. It is, however, evident that the classification of risk types is dependent on the business of the organisation. For example, the approaches of Mckenzie as well as Falkena and Kok differ because they classify the risk types according to derivatives and banking risks, respectively. In certain cases, different authors inherently agree on the risk types, but their approaches to them differ. For example, the approaches to business risk of Van Greuninig and Bratanovic and Goldman *et al.* respectively. Goldman *et al.* (1998:34) see business risk as market and credit risks that an organisation takes with the objective of making money. Van Greuninig and Bratanovic (2000:3), on the other hand, associate business risk with the business environment of banks that includes macro-economic policy concerns; legal and regulatory factors; the financial sector infrastructure and payment system; and the overall systemic risk for operations.

Notwithstanding the above-mentioned differences regarding broad risk classifications, it is essential that an organisation be aware of all the significant
risks it faces. Taking into account the broad risk classification, described by Valsamakis, namely speculative and pure risk, it could be possible to group the various risks under these broad categories, even though there are different perceptions as to their content. An example of how risks could be classified, based on the definitions of the risk types and that of pure and speculative risks, is as follows:

<table>
<thead>
<tr>
<th>Speculative Risk</th>
<th>Pure Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market risk</td>
<td>Operational risk</td>
</tr>
<tr>
<td>Credit risk</td>
<td>Technology risk</td>
</tr>
<tr>
<td>Interest-rate risk</td>
<td>Reputation risk</td>
</tr>
<tr>
<td>Liquidity risk</td>
<td>Compliance risk</td>
</tr>
<tr>
<td>Country risk</td>
<td>Legal risk</td>
</tr>
<tr>
<td>Settlement risk</td>
<td>Insurance risk</td>
</tr>
</tbody>
</table>

An important issue, regarding the classification of risk types, is that a clear understanding of each risk type the organisation faces is necessary to ensure the proactive management thereof.

During the above discussion it has become evident that most authors regard operational risk as one of the main risk types, notwithstanding differences of opinion regarding its content or its underlying risk factors.

Although there might be various arguments, approaches and viewpoints regarding the classification of risk types, this study will only concentrate on operational risk in a banking environment. For this purpose, it is necessary to discuss operational risk in more detail to establish a basis for the literature study.
2.5. **Viewpoints on Operational Risk**

The previous section clearly indicates that most authors and organisations classify operational risk as one of the main risk types, although there are different viewpoints on the detail thereof. Notwithstanding these differences, it appears that banks are becoming more aware of operational risk, which is causing major changes to their internal risk structures. According to Venkat (2000:595) firms are attempting to bring the responsibility of market, credit and operational risk under the supervision of one organisation unit with the responsibility to identify, measure, monitor and manage these risks.

A major event, which resulted in an increased focus on operational risk, was the Barings Bank saga during 1995. Many authors and reporters argued that ineffective operational risk management caused the fall of Barings Bank. Freeman (1999:58) also states that the collapse of Barings Bank led many competitors to question their own vulnerability to an operational failure. Bloom and Galloway (1999:6) state that “Operational risk - posed by procedural errors, computer and network crashes, service or product quality lapses, fraud, failure to comply with regulations or company policies, or political landscapes - has always been present, but not always well recognised.”

The expansion of e-commerce initiatives by financial institutions is a further aspect that is bringing operational risk to the forefront, according to a report issued by Meridien Research (Williams 2000b:17). In this report, Deborah Williams, the research director and author of the report, says that operational risk has been attracting a lot of attention, as regulators call for capital to be set aside to cover this risk type. According to Williams, there are capital charges for market risk and credit risk to ensure that institutions are adequately capitalised to cover any potential losses. She also adds that the Bank of International
Settlements has been calling for specific capital assessments, but firms are better off defining risk relative to their own operations and allocating the necessary capital themselves, rather than waiting for a regulator to set the amount. Though the final guidelines are not yet finalised, it is likely that banks will be required to apply an explicit capital charge to cover losses arising from operational risk. However, objections to this idea are, according to McNee (2000:16), based on the fact that there is no standard methodology or even an industry-wide definition of operational risk. Hence, another reason for banks to take a close and intense look at defining operational risk in such a way that it could be managed and controlled. Cooper (1999:1) also maintains that financial institutions are undergoing a period of enormous change, which has mostly increased their potential for operational risk, indicating another reason for focusing on it. Furthermore, a recent spate of mergers and acquisitions among financial institutions, as well as internal restructuring, are also forcing these institutions to consider operational risk to be managed as one of the major risk types.

Furthermore, and according to Bloom and Galloway (1999:6), globalisation, consolidation and new technology have lavished the banking industry with profit-making opportunities and at the same time left it open to equal amounts of operational risk. Bloom and Galloway (1999:6) state that according to the Basel Committee, operational risk has become too important to ignore and banks must take a disciplined and proactive approach to managing it. Even though it is obvious that operational risk is becoming a major risk issue within the international banking and financial industries, the dissimilarities of the various definitions and approaches should be addressed. This could possibly be accomplished by establishing a universal agreed definition of operational risk. However, Freeman (1999:61) states that firms differ in their breadth of definition for operational risk, for instance, "whereas four-fifths of Australian financial institutions include personnel risks in their definition of operational risk, only
half of British firms agree.” It was mentioned previously that many authors and organisations have different approaches to and viewpoints on operational risk. The various definitions indicate certain similarities as well as differences, which should be taken into account when trying to formulate a unanimous approach towards operational risk.

Although there is currently a lack of a universal agreed definition for operational risk, many organisations do have their own interpretation thereof and manages it accordingly. According to Freeman (1999:58), individual firms need to develop their own definitions for risks, based on their experience and preferred terminology. He (1999:58) states that one way of describing operational risk, is to identify its underlying factors or a sub-set of the area it covers, for example:

- Transaction processing/control error.
- System failure error.
- Business interruption.
- Personnel risk.
- Legal liability.
- Breach of firm policy.

From various other definitions and viewpoints, similar underlying factors can be identified as is evident in the following discussion.

Morgan and Andersen (1997:48) state that operational risk is the uncertainty related to losses resulting from inadequate systems or controls, human error, or management failure. Chew (1996:299) points out that it is the unexpected losses arising from deficiencies in management information, support and control systems.
Schwartz and Smith (1997:322) consider operational risk as the risk of loss arising from human error, management failure and fraud or from shortcomings in systems or controls. They also state that an objective of operational risk management should be to recognise these factors and to address it in such a manner that its adverse effects are eliminated or minimised.

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

- Direct financial losses;
- Indirect losses; and
- Potential earnings forgone as a result of a lack of operational capability to transact business.

KPMG (1998:6-7) states that operational risk is the potential exposure to unexpected financial or other damage arising from how an organisation pursues its business objectives. KPMG joins the viewpoints of other authors, by stating that operational risk could be seen as all the other risks that do not form part of credit or market risk. Another example of this viewpoint, is that of Wilmot, from Chase Manhattan Bank, who states that “We need to consider all other risks when measuring and managing operational risk” (Cooper 1999:7). Freeman (1999:58) states that although many firms choose to define operational risk as “everything else”, there has been significant progress in getting to grips with
defining its scope and possible impact. He (1999:60) also states that “the wider the definition of operational risk adopted by a firm, the more vulnerable it is to a loss of business”.

Goldman et al. (1998:37) constitute that operational risk covers a broad range of risks that are internal to the firm, and has in the past received rather less attention than other aspects of risk. However, attention is increasingly being focused on this issue because of the scale of the losses that firms have suffered, as a result of breakdowns in internal controls. In addition to the Barings Bank example, Goldman et al. (1998:37) also mention the following examples that indicate the diversity of operational risk and the scale of the losses that could arise as a result:

- **Example 1** – Toshihide Iguchi, a US government bond trader at Daiwa bank in New York, created a loss of over US$1 billion for his bank over a period of 10 years because he was able to cover up the losses on his bond trading, by switching securities out of clients’ custody accounts.

- **Example 2** – A fund manager at Morgan Grenfell Asset management in London, created a loss, of a similar size for Deutsche Bank by failing to follow the investment guidelines for the mutual fund he was managing and investing instead in highly speculative unlisted stocks. When the scale of the problem was finally revealed, Deutsche Bank had to step in and compensate customers for any loss they might have incurred as a result of this fund manager’s unconventional actions.

Mayland (1993:2) defines operational risk as the risk of loss due to failures when executing transactions. The failure can be caused by the bank, the customer or another party to the transaction, including payment networks, communication
providers and others. Operational risks include disasters, employee actions, power failure and the like.

Alexander (2000:1) states that operational risks include many different types of risk, from the simple “operations” risks of processing transactions, unauthorised activities, and system risks, to other types of risk that are not included in market or credit risk, for example, human risk, legal risk, information risk and reputation risk.

To find a definition for operational risk and to simply conclude that it encompasses all those risks that are not categorised as market or credit risk, seems totally unsatisfactory, because by only defining what it is not, it cannot be managed as a specific risk type. A more “positive” definition of operational risk should assist in determining exactly what it is and how it should be managed. The Basel Committee defined operational risk as “…the risk that deficiencies in information systems or internal controls will result in unexpected loss. The risk is associated with human error, systems failure and inadequate procedures and controls.” (FSA 1999:14).

Crouhy and Mark (2000:344) state that operational risk is the risk associated with operating the business and can be subdivided into operational failure risk and operational strategic risk (see figure 2.11.):

- **Operational failure risk** arises from the potential for failure in the course of operating the business. A firm uses people, processes and technology to achieve business plans, and any of these factors may experience a failure of some kind. Operational failure risk is thus the risk internal to the organisation caused by these factors.
- **Operational strategic risk** arises from environmental factors, such as a new competitor that changes the business paradigm, a major political and regulatory regime change, earthquakes and other factors that are generally outside the control of the organisation (external).

**Figure 2.11: Two Broad Categories of Operational Risk**

![Diagram showing the two broad categories of operational risk: operational strategic risk and operational failure risk.](image)

Operational strategic risk:
The risk of choosing an inappropriate strategy in response to environmental factors, such as:
- political
- taxation
- regulation
- government
- societal
- competition

Operational failure risk:
The risk encountered in the pursuit of a particular strategy due to:
- people
- process
- technology

Source: Crouhy & Mark (2000:345)

Although the external and internal factors can be seen as the two broad categories, Crouhy and Mark (2000:345) mention that one should observe that a failure to address a strategic issue could translate into an operational failure risk. For example, a change in the tax laws could be seen as an operational failure risk, although it is originally an external or operational strategic risk. In other words, the two types of risk are interrelated and tend to overlap. Wilson (2000:386) states that the Operation Risk Forum defined operational risk as "... the exposure to potential financial losses. Such losses may be caused by internal or external events, trends and changes, which were not captured and prevented by the
corporate governance and internal control framework, systems, policies, organisation, ethical standards or other key controls and standards of the firm. Such losses exclude those already captured by other risk categories such as market, credit or strategic/business risk.”

Venkat (2000:587) approaches operational risk from a firm-wide risk management framework and define it as the risk of loss resulting from human acts (intentional and unintentional), technology failure, and breakdown in internal controls, disaster, or the impact of external factors.

Cooper (1999:6-7) summarises the opinions of experts from certain leading financial institutions, regarding operational risk, as follows:

- “…the risk that external events, or deficiencies in internal controls and information systems, will result in an economic loss – whether anticipated to some extent or unexpected.”
- “Operational risk can be defined as the potential for loss from the breakdown of people, process or technology, applied in pursuit of the organisation’s business objectives.”
- “The definition should capture business disruption, failure of controls, errors, omissions and external events. We have classed operational risk as: relationships, people, technology, physical assets and other external exposures, also direct and indirect losses and reputation risk costs”.
- “Operational risk touches compliance, technology, transactional and infrastructure issues…”

It is obvious that there are a vast number of views and approaches to a definition for operational risk. However, there is a clear indication that most viewpoints
include the same underlying factors, which is an indication that it should be included in a universal definition for operational risk. An early analysis of the definitions shows the following most common underlying risk factors, which are discussed in more detail in chapter 3:

- Processes (Technology).
- People (Human error)
- External exposures.
- Systems and controls.

According to the reasons mentioned, it is clear that operational risk is emerging as a major concern to management of banks and financial institutions. The lessons learned from past experience as well as the planned future, for example, regulators who want to force banks to set aside capital to cover losses as a result of operational risk, are clear indicators that operational risk needs to be addressed and managed sooner than later. However, it seems that there are currently more questions than answers around operational risk for banks as well as for regulators. Cooper (1999:1) states, for example, that the measurement and management of operational risk is sure to remain “a hot topic for some time to come.”

2.6. Summary

This chapter focused on an overview of risk management as well as various approaches and viewpoints.

Firstly, risk, as the overarching concept, is viewed as the possibility of incurring misfortune or loss, which, if not effectively managed, might result in adverse effects for the organisation. Subsequently, managing the risks, is indicated as the
control thereof and the minimising of the potential adverse effects of the risk consequences. An integrated approach to risk management became evident, based on trends such as the globalisation and integration of financial markets, derivative products, which involve various risk types, and technology developments. To establish an integrated risk management approach, it is necessary to ensure the effectiveness of the components of an integrated risk management framework, which are classified as organisational effectiveness, risk performance management and systems technology.

Thirdly, the risk management process consists of various elements, as seen by different authors. Notwithstanding differences in opinions by these authors, a holistic view on the classification of elements for a risk management process was identified, namely:

- Risk identification.
- Risk evaluation.
- Risk control.
- Risk finance.

After a brief overview of the elements of a risk management process, risk classification was discussed. The general approach is to group risks into main categories of risk types. It is evident that there does not exist a general agreed classification amongst different authors, but it is clear that for an organisation to effectively manage its risks, risk types must be clearly understood and formulated according to the business of the organisation. Although some authors differ as to the content of operational risk, most of them regard it as a main risk type, which led to focusing on an overview of operational risk. Various definitions and approaches of operational risk were identified, in order to
determine the most common underlying operational risk factors that should be addressed when formulating an acceptable definition for operational risk.
CHAPTER 3

OPERATIONAL RISK MANAGEMENT: A LITERATURE REVIEW

3.1. Introduction

Globalisation and new technology have provided the banking industry with profit-making opportunities but have also made it more vulnerable to operational risk (Bloom & Galloway 1999:6). It seems that the industry's risk-control capability has not kept pace with these developments as proved by, for example, the Barings Bank trading saga in 1995. This occurrence, together with many others, motivated banks to take a more proactive approach to operational risk management.

In the previous chapters, it was mentioned that operational risk is not a clearly defined concept, although most banks recognise it as an important aspect of risk management. This chapter encompasses a comprehensive literature study of existing theories and concepts pertaining to operational risk in a banking environment. The first challenge is to identify the underlying risk factors on which a definition for operational risk could be based. This definition could, in turn, be used for the classification of operational risk in the identification process. The second challenge is to evaluate the risk factors to determine their potential impact on banking institutions. The appropriate techniques available to measure these factors, and therefore to control them, will also be discussed. Thirdly, risk control will be addressed in terms of the activities needed to eliminate or reduce the potential adverse effects of the underlying risk factors as well as the organisational structures that should be in place to support risk management activities. Lastly, the cost of managing operational risk will be discussed.
3.2. Identification of Operational Risk

According to Williams (2000b:17), determining operational risk depends on a particular firm. She (2000b:17) also states that “The key thing is that firms really need an internal definition of operational risk. People talk about key factors or key risk factors with the idea being to pick a finite list of things that you believe you have exposure to, and then prioritise those and focus on the ones that seem to be the most important.”

Williams (2000b:17) emphasises that risk identification, as the first step of a risk management process, provides an important foundation for the firm to rely on in the future. Furthermore, if there is not a clear understanding of what operational risk means to the individual business units and the corporation as a whole, the ability to build any technology systems for the measurement and management of the risks will not be possible.

The definitions which different authors assign to operational risk were discussed in the previous chapter. Before a definition for operational risk can be adopted, however, it is important to understand its origination. While this might sound straightforward, it often causes confusion as managers focus on the effect, rather than the cause of the risk. In this regard, Rachlin (1998:115) states that banks often try to reduce the symptoms rather than try to rectify the underlying problems. Hence, the necessity to take a brief look at causes and effects of operational risk.

Crouhy and Mark (2000:357) state that an organisation should analyse the causes and the effects of an operational loss. For example, failure to have an independent group vet all mathematical models is a cause; and a loss event
arising from using erroneous models is the effect. Table 3.1 provides further examples.

A further example of a cause, is human fallibility. The effect of this risk is, for example, financial loss, however, this may be the final outcome of a chain of effects. A bank should attempt to identify all the links in that chain to ensure that they are addressed during the managing of the risk. It should be kept in mind that causation of risk is invariably complex. It could take a particular combination of causes to produce an effect, for example, the starting point of risk may not cause a loss without the interaction of poor systems and controls or processes. There may be many causes contributing to one loss. According to Crouhy and Mark (2000:357), most banks start by recovering the losses and then try to fit the causes to them. This reactive approach may not be adequate to solve the problem (cause) and could be successfully addressed by a proactive risk management approach.

Table 3.1: Causes and Effects

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Cause</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>People (human resources)</td>
<td>Loss of key staff due to defection of key staff to competitor.</td>
<td>Variance in revenues/profits (for example, cost of recruiting replacements, costs of training, disruption to existing staff).</td>
</tr>
<tr>
<td>Process</td>
<td>Declining productivity as value grows.</td>
<td>Variance in process costs from predicted levels (excluding process malfunction).</td>
</tr>
<tr>
<td>Technology</td>
<td>Year 2000 upgrade expenditure. Application development.</td>
<td>Variance in technology running costs from predicted levels.</td>
</tr>
</tbody>
</table>

Source: Adapted from Crouhy & Mark (2000:358)
Laycock (1998:132) lists six categories of causes that could give rise to operational risk (see table 3.2).

**Table 3.2: Causes and Events**

<table>
<thead>
<tr>
<th>Category</th>
<th>Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>People/employees</td>
<td>Errors, Misdeeds, Employment law, Employer's liability, Absence/loss of key staff, Organisational structure, Corporate governance, Wrongful trading</td>
</tr>
<tr>
<td>Customer relationships</td>
<td>Client suitability, Client capacity/ultra vires, Client powers/authority to transact, Money laundering</td>
</tr>
<tr>
<td>Technology</td>
<td>System failure, System integrity, System age, System suitability, System support, System conformance to corporate standards, Model risk, Data quality</td>
</tr>
<tr>
<td>Assets</td>
<td>Business interruption, Asset loss/destruction, Third party theft, Fraud</td>
</tr>
<tr>
<td>Regulators/supplier</td>
<td>Legal risk, Compliance with standards, Changes in regulatory standards, Supplier “failure”</td>
</tr>
<tr>
<td>Other</td>
<td>Project risk, Reputation risk</td>
</tr>
</tbody>
</table>


This list is, however, not exhaustive and presents only one way of categorising the causes and events relating to operational risk. Among the categories listed are
some that are extremely difficult or impossible to quantify, such as, the organisational issues. Laycock (1998:132) states, furthermore, that operational event risk represents the potential for fluctuations in the income statement or the cash-flow statement due to risks or exposures associated with the following:

- Inadequate defined controls;
- Systems or control failure; and
- Unmanageable events.

According to Laycock (1998:133) causes and effects could be classified as follows:

- High-frequency/low-impact events, for example, there are likely to be several possible causes (for example, human error and system failure) which may lead to the late settlement of a security transaction.
- Low-frequency/high-impact events such as wrongful trading, potentially involving several factors, for example, poor or ineffective controls in addition to the propensity for an individual to commit one or more wrongful acts.

He (1998:133) furthermore states that high-frequency/low-impact events can often be distinguished from low-frequency/high-impact events by the time lag between the operational event itself and the moment when its effect is felt by the organisation. High-frequency/low-impact events tend to make themselves felt in a relatively short period of time, while low-frequency/high-impact events might only generate an effect long after the event. There could, however, be exceptions, for example, a fire or a flood is a risk with a low frequency of which the impact is usually felt quickly.
Crouhy and Mark (2000:345) state that operational risk can be broken down into three main risk factors namely the failures of people, processes and technology deployed within the business (see table 3.3). They also classify these main risk factors according to internal and external dependencies. Internal dependencies should be reviewed according to a set of common factors consisting of three key components, namely, capacity, capability and availability. For example, the following questions could be asked if operational risk arises from people risk:

- Does the business have enough people (capacity) to accomplish its business plans?
- Do the people have the right skills (capabilities)?
- Are the people going to be there when needed (availability)?

<table>
<thead>
<tr>
<th>People risk</th>
<th>Incompetence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fraud</td>
</tr>
<tr>
<td>Process risk</td>
<td>Mark-to-model error</td>
</tr>
<tr>
<td>Model risk</td>
<td>Model/methodology error</td>
</tr>
<tr>
<td>Transaction risk</td>
<td>Execution error</td>
</tr>
<tr>
<td></td>
<td>Product complexity</td>
</tr>
<tr>
<td></td>
<td>Booking error</td>
</tr>
<tr>
<td></td>
<td>Settlement error</td>
</tr>
<tr>
<td></td>
<td>Documentation/contract risk</td>
</tr>
<tr>
<td></td>
<td>Exceeding limits</td>
</tr>
<tr>
<td></td>
<td>Security risks</td>
</tr>
<tr>
<td></td>
<td>Volume risks</td>
</tr>
<tr>
<td>Operational control risk</td>
<td></td>
</tr>
<tr>
<td>Technology risk</td>
<td>System failure</td>
</tr>
<tr>
<td></td>
<td>Programming error</td>
</tr>
<tr>
<td></td>
<td>Information risk</td>
</tr>
<tr>
<td></td>
<td>Telecommunication risk</td>
</tr>
</tbody>
</table>

Source: Crouhy & Mark (2000:350)

The external dependencies are analysed in terms of the specific type of external interaction with the business of a bank. For example, clients that are external to a bank but could influence the business.
According to Crouhy and Mark (2000:355), these internal and external risk dependencies cannot be viewed in isolation from one another. One needs to examine the degree of interconnected risk exposure across the main factors of operational risk, in order to understand the full impact of the risk. For example, if a bank introduces a new computer system it will have an effect on people and processes which, in turn, could have an effect on the operational risk exposure of the bank. People must be trained to use the system and processes must be adapted to incorporate the system.

Furthermore, the sources that drive these factors of operational risk should also be examined. These drivers are, according to Crouhy and Mark (2000:356), change, complexity and complacency. Change refers to such items as introducing new technology or new products, for example, a merger or acquisition, or moving from internal supply to outsourcing. Complexity refers to such items as complexity in products, process or technology, while complacency refers to ineffective management of the business, particularly in key operational risk areas such as fraud and unauthorised trading.

The model depicted in figure 3.1 illustrates how these underlying drivers of risk (change, complexity and complacency) could be connected to the main operational risk factors (people, processes and technology). It indicates that a change or failure of any of the three drivers could have an effect on the operational risk factors of a bank. The drivers themselves are also interdependent (internal/external) and could influence each other.
Figure 3.1.    Interconnectivity of Operational Risk Exposure Dependencies

Operational Risk due to:

People
Processes
Technology

Drivers

Change
Complexity
Complacency

Source: Crouhy & Mark (2000:355)
Rachlin (1998:115) states that the Bank of Scotland considers operational risk to arise from five factors, namely:

- The process operated by the bank;
- The people in the bank who help operate and manage the processes;
- The system used to support the processes;
- The impact on the people, processes and systems that the business strategy, may have; and
- The risks resulting from the external environment in which the bank operates.

Once again it is evident that the main risk factors for operational risk could inherently be perceived as people, processes, systems (technology) and external factors.

Rachlin (1998:177) depicts the underlying risk factors of operational risk in a model (see figure 3.2.), and describes it as follows:

*Process.* Banks operate a large number of processes in order to deliver their services. These include processes for making payments, accepting deposits and clearing cheques and so on. Risks can arise at all stages of these processes.
Figure 3.2: Key Areas of Operational Risk


People. Although many operational risk incidents are said to be the result of major internal control failures, it is often the case that they are the failures of people. With many bank branches evolving into mainly sales operations and the need for general banking skills being greatly reduced, issues can arise with regard to the integrity and competence of staff and management.

Systems. Almost all banking services depend on IT systems. Problems can arise from the corruption of data stored on the system, whether accidental or deliberate, for example, programming errors or fraud.

Business Strategy. Business strategy in the form of mergers, take-overs and re-engineering projects can have an important effect on processes, systems and
people. It is important that operational risk issues are considered when deciding on a business strategy.

*External environment.* The external environment in which a bank operates could give rise to operational risks. The bank itself tends to have little or no control over the source of such risk. The risks could arise from *inter alia* compliance, legal and litigation issues, unanticipated tax changes and the physical threats the bank faces, such as, robberies and cash heists. It would also include the effect of natural disasters such as earthquakes, flooding and tornadoes.

According to the FSA (1999:15-16) operational risk exposures could be grouped as follows:

*Processes and systems*

- The risk of errors arising from information systems;
- The risk of systems failure leading to either error or loss of business;
- The risk arising from systems infiltration, for example computer hacking; and
- The risk arising from inadequate processes leading to time delays and efficiency, resulting in financial losses and loss of business.

*People*

- The risk arising from the possibility of incompetent, inexperienced, unsuitable, negligent and/or maverick staff;
- The risk of human error with specific regard to processing;
- The risk that a working culture may lead to low morale, high staff turnover, low concentration, low productivity and industrial action;
- The risk of fraudulent and other criminal activity; and
• The risks associated with unauthorised and/or ill-informed decision-making at all levels, particularly with regard to business strategy, project management, change management, liquidity and outsourcing.

External factors

• Acts of God;
• External criminal activities;
• Domestic political upheaval;
• The regulatory, legal, tax, and business environment and any changes in that environment;
• Risks associated with third parties, for example suppliers and contractors; and
• Deterioration of a bank’s reputation as perceived by the market.

From the preceding discussion it is evident that there is general agreement that operational risk consists of the following underlying risk factors:

• Processes.
• People.
• Systems/Technology.
• External factors.

The risk factors could evidently be divided into two broad categories, namely, internal and external factors. The internal factors could be grouped into processes, people and systems (technology), while the external factors are outside the direct control of a bank.
3.2.1. Definition of Operational Risk

From the above discussion it is evident that an accepted definition for operational risk should include both the internal and external underlying risk factors. A suggested working definition for operational risk by the FSA (1999:15) is: “The risk that the continuation of business may lead to loss as a result of human fallibility, technological shortcomings and/or various external factors. A bank should mitigate these risks through the use of systems and controls. However, if the latter is inadequate, they may constitute new risks and/or exacerbate existing risks.”

The factors, included in the definition, could easily be identified as:

- People (human fallibility);
- Systems (technological shortcomings and breakdowns);
- Processes (systems control); and
- External factors.

It could, however, be said that other risks that a bank is exposed to could also include the above-mentioned factors. As such it is important to qualify the interrelationship of these operational risk factors with the other primary risks, such as, credit risk, market risk, liquidity risk and country risk. It is, therefore, imperative to distinguish clearly between operational risk and the other risks to ensure a more positive management approach towards operational risk.

In chapter 2 the views of various authors with regard to the classification of risks were briefly discussed. These authors included people, processes or systems only in their description of operational risk and did not mention it in their description of other main risk types (for example, credit, market, liquidity, etc.). The
descriptions which Van Greuning and Bratanovic (2000:10) assign to the
different risks also proves this point (refer to table 3.4). These factors could,
however, have an indirect influence on the other risk types, necessitating a firm-
wide risk management approach.

Table 3.4: A Summary of Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance Sheet Structure</td>
<td>Risks resulting from the structure and composition of a bank’s assets and liabilities and off-balance sheet positions.</td>
</tr>
<tr>
<td>Income Structure and Profitability</td>
<td>Risk of a bank that does not have sufficient income to cover its expenses and maintain capital adequacy.</td>
</tr>
<tr>
<td>Solvency Risk and Capital Adequacy</td>
<td>Risk of a bank having insufficient capital to continue operations. Risk of non-compliance with minimum regulatory capital standards.</td>
</tr>
<tr>
<td>Credit Risk</td>
<td>Risk that a party to a credit agreement will not be able or willing to service interest or repay the principal.</td>
</tr>
<tr>
<td>Liquidity Risk</td>
<td>Risk of a bank having insufficient funds on hand to meet its current obligations.</td>
</tr>
<tr>
<td>Interest Rate Risk</td>
<td>Risk of changes in interest rates that will have an adverse effect on a bank’s income or expenses.</td>
</tr>
<tr>
<td>Market Risk</td>
<td>Risk of capital resulting from adverse market price movements related to investments in commodity, equity, fixed interest or currency markets.</td>
</tr>
<tr>
<td>Currency Risk</td>
<td>Risk of adverse exchange rates movements due to the mismatch between foreign receivable and payables.</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Risk related to a bank’s overall business strategy; organisation; functioning of internal systems, including computer-related and other technologies; compliance with bank policies and procedures; and measures against mismanagement and fraud.</td>
</tr>
</tbody>
</table>

Source: Adapted from Van Greuning & Bratanovic (2000:10)

According to the FSA (1999:16), it is imperative that a definition of operational risk should be as comprehensive as possible. It is prudent to consider all the risks
that an institution faces and to mitigate those risks. Failure to include a risk explicitly in a definition may result in failure to consider that risk. Therefore, the inclusion of the underlying risk factors of operational risk in its definition is imperative. Reflecting the main underlying risk factors in the definition of operational risk could also assist the process of evaluating and quantifying operational risk for control purposes.

During a conference on 21 May 1998, the Operational Risk Forum decided to identify a narrow and a wide definition of operational risk. Wilson (2000:386) describes these definitions as follows:

- **Narrow definition**: Operational risk is seen as risk residing in departments called “operations” and is described as those errors and omissions of controls, systems and processes which may lead to potential losses.

- **Wide definition**: Operational risk is seen as all risks not covered by market or credit risk. The problem with this approach is that it may leave an unidentified residue, which could impact the income statement materially and undermine the wide definition approach.

Wilson (2000:386) states that in order to accommodate the wide and narrow definitions, the Operational Risk Forum defined operational risk as follows (also mentioned in chapter 2):

“Operational risk is the exposure to potential financial losses. Such losses may be caused by internal or external events, trends and changes, which were not captured and prevented by the corporate governance and internal control framework, systems, policies, organisation, ethical standards or other key controls and standards of the firm. Such losses exclude those
already captured by other risk categories such as market, credit, or strategic/business risk.”

Although this definition includes the main underlying operational risk factors (People, systems, process and external factors), it also includes other elements or “sub-risk” factors such as policies, control frameworks and ethical standards. This approach could possibly lend itself to the omission of other factors, for example, procedures, organisational structures and risk principles. This definition, although comprehensive, should rather be stated differently by referring to only the main underlying risk factors. This will ensure that no “sub-risk” factors are omitted and that it still covers the requirements of a narrow and wide approach.

Taking into account all the previously discussed viewpoints of operational risk, a suitable definition for operational risk management in a banking environment could be the following:

**Operational risk is the exposure of a bank to potential losses, resulting from shortcomings and/or failures in the execution of its operations. These losses may be caused by internal failures or shortcomings of people, processes, and systems, as well as the inability of people, processes and systems to cope with the adverse effects of external factors.**

This definition firstly comprises the main underlying operational risk factors, namely, people, processes and systems. Although the factors are seen as an integral part of operational risk, they could also have an influence on the total organisation in terms of its operations. As such, it is important to take cognisance of the interrelationships between operational risk and the other main risk types.
(for example, credit, market, and liquidity risk). The following example illustrates the interrelationship between operational and credit risk:

The failure of a bank’s credit system could result in a loss of credit business. Although it is a loss in terms of credit business, the loss is a result of the system failure. As such, the loss should be classified as an operational loss. The actual risk (operational risk) should be addressed by operational risk control measures, for example, to ensure that back-up systems are in place to prevent any losses due to system failures.

Secondly, the definition includes the risk pertaining to the external factors which are beyond the direct control of a bank. The definition looks specifically at the adverse effect external factors could have on the bank if the people, processes and systems cannot cope with them. For example:

If lightning should neutralise the internal systems of a bank, preventing the bank from doing business, it could result in a loss. The adverse effect on the systems could be seen as an operational risk exposure, hence the necessity to address it according to an operational risks management process. For instance, having a back-up system to ensure the normal continuation of business could be seen as an operational risk control mechanism.

Thirdly, the definition excludes the risk exposures to a bank caused by other risks such as market, credit, liquidity, and country. The intention of the definition is to indicate in a positive way what operational risk entails rather than to indicate that it consist of all the factors not covered by the aforementioned risks. This positive approach towards operational risk should allow management to be more specific in addressing all the relevant operational risk factors.
Each of the underlying risk factors contained in the above definition will be discussed in detail in the ensuing section.

3.2.2. **Underlying Operational Risk Factors**

Katz (1995:200) states that no business should be entered into without a full and early assessment being made of the underlying risk factors that relate to it. Furthermore, all risk factors need to be identified such that credit, operating, accounting, reporting and risk management tools can be put in place. Davies et al. (1998:76) state that a central requirement of a risk allocation process is to be able to assess the extent to which the exposure to a risk factor increases or decreases the expected volatility of earnings. This emphasises the necessity to identify risk factors with sufficient precision to be able to monitor and control them effectively.

In the previous section operational risk was defined based on the primary underlying operational risk factors that were identified as:

- People;
- Systems (Technology);
- Processes; and
- External factors.

This section deals in detail with each of these underlying risk factors to determine their effect on operational risk.

During the detailed analysis of the primary underlying operational risk factors, additional sub-risks of operational risk will be identified, for example, people as
a risk factor could result from human error, which could cause fraud and subsequently be viewed as fraud risk. However, it must be emphasised that the dynamic nature of a business could influence its exposure to risks and additional underlying risk factors could evolve, changing the overall potential effect of operational risk.

3.2.2.1. People

Katz (1995:166) states that there is always a human factor to consider in undertaking any business activity. Knowledge, experience, capability and reliability of the persons involved in all of the business processes are critical risk factors. A variety of authors include this factor as part of the definition for operational risk as shown by the following extracts:

- “The risk of human error or fraud...”
- “The risk of direct or indirect loss resulting from inadequate people...”
- “…risk of loss due to failure in people...”
- “…the risk is associated with human error...”

Hoffman (1998:29) defines people risk as the risk of loss caused intentionally or unintentionally by an employee (for example, an employee error or employee misdeed) or involving employees, such as, in the area of employment disputes or intellectual capital. According to Donahoe (1999:3), people risk comprises incompetence and fraud.

Kingsley et al. (1998:4) state that people are arguably a company’s most important resource. However, historically they have been overlooked when evaluating operational risk, as it is so difficult to measure and model the risks of:
• Human error.
• Lack of integrity and honesty.
• Lack of segregation of duties.
• Lack of customer focus and professionalism, lack of teamwork and respect for the individual.
• Reliance on key individuals.
• Insufficient skills, training, management or supervision.
• Lack of a culture of control.

Kingsley et al. (1998:4) argue that people risks continue to be the major contributing factor in many dramatic failures and as such, despite the difficulties of measuring it, they must be targeted in any programme that aims to improve risk management.

It is evident that people, as an underlying risk factor of operational risk, could include a variety of sub-risks to be addressed during a risk management process. Rachlin (1998:127), for example, mentions the following sub-risks:

• Integrity:
  • Fraud.
  • Collusion.
  • Malice, the unauthorised use of information.
  • Rogue trading.
• Competency.
• Management.
• Personnel.
• Health and safety.
The FSA (1999:15) identifies the following primary sources of people risks:

- Inexperienced, incompetent, unsuitable, negligent and/or maverick staff.
- Human error.
- Working culture creating low morale, high staff turnover, poor concentration, low productivity and industrial action.
- Fraud and theft.
- Unauthorised and/or ill-informed decision-making at all levels, particularly with regard to business strategy, project management, change management, liquidity and outsourcing.

Similarly, Katz (1995:39) identifies the following employee risk factors:

- Fraud.
- Willful neglect.
- Neglect of duties.
- Lack of knowledge.
- Lack of motivation.

Wilson (2000:380) states that human resource (people) risk is not just the responsibility of the human resources department, although they do contribute to controlling of the risk. The business units themselves have specific responsibilities regarding the control of operational risk. For example, given the rogue trader problems, which some banks have suffered, it is also important that the operational risk manager checks that the human resources department has sufficient controls with regard to personnel security, namely (Wilson 2000:380):
• Hiring procedures:
  • References and working credentials.
  • Existing and ongoing security training and awareness programmes.
  • Job descriptions defining security roles and responsibilities.

• Termination procedures:
  • The extent of the termination debriefing.
  • Ensuring revocation of physical access (cards, keys, system access authority ID etc).

According to the Standard Bank Annual Report (1998:57), human resources risk includes the inability to recruit, train and retain the correct mix of skilled staff. This may occur as a result of inappropriate training or remuneration policies. Failure to meet objectives relating to equity targets will increase this risk.

From the above, it is evident that there are a variety of sub-factors to be considered under “people”, as a primary underlying risk factor of operational risk. The following list comprises the people risks that different authors have identified:

• Employee fraud/unauthorised activities/misdeed.
• Staff changes and selection.
• Staff training/capabilities.
• Discipline.
• Corporate ethics.
• Recruitment and retention.
- Structures/accountability/responsibility.

This is, however, not an exhaustive list and would depend on the business concerned and the environment in which it operates. What seems imperative, however, is that an organisation should proactively identify the sources of its people risk in order to manage it as an integral part of the risk management process.

3.2.2.2. Systems (Technology)

According to Basel (1998c:6), a bank faces risk when the systems it chooses are not well designed or implemented. For example, a bank is exposed to the risk of an interruption or slow-down of its existing systems if the electronic banking or electronic money system it chooses is not compatible with user requirements. A further problem banks face is the rapid pace of change that characterises information technology. This presents banks with the risk of systems obsolescence. For example, computer software that facilitates the use of electronic banking and electronic money products by customers will require regular updating. This type of software poses a risk for banks as criminal or malicious individuals could interrupt and modify it, leading to potential losses. In addition, rapid technological change can mean that staff may fail to fully understand the nature of new technology employed by the bank. This could result in operational problems with new or updated systems (Basel 1998c:6).

New technologies often have implications of complexity and uncertainty. The newer the technology, the greater the risk that it may not perform as expected. According to Remenyi and Heapfield (1996:351), it is well known in the information technology profession that new systems often require modifications in order for them to work as anticipated. Yet another aspect, which needs to be
considered, although forming part of people risk, is the new skills required for the technologies. The learning of new technologies and ways of doing things are often met with resistance among employees. Not only does this resistance need to be monitored and controlled, but also effective training programs need to be implemented.

Operational risk could also be identified in terms of a risk resulting from system failures, which reflects the possibility that systems are inherently flawed and could arise from various factors. Various authors include systems as an underlying risk factor in the definition of operational risk as depicted in the following extracts:

- "...risk are those of malfunctioning of the information systems..."
- "...the potential for adverse fluctuation due to the effects attributable to system..."
- "The risk run by a firm ... its internal practices, policies and systems..."
- "Operational risk arises from the potential for inadequate systems..."

In addition, the Basel Committee (1998c:20) also lists the following examples of possible risks relating to systems:

- Counterfeiting of electronic money, for example, criminals alter or duplicate electronic money products to obtain goods or funds without proper payment.
- Service provider risk, for example, a service provider may not deliver services expected by the bank and deficiencies in systems or data integrity or reliability may result.
• Obsolescence of systems could, for example, cause delays or disruptions in processing transactions.

Wilson (2000:381) states that system risk, in the wide definition, includes all system risks including external pressure, such as, the risk of not keeping up with the progress of changing technology. Technology risk is at the heart of a business, such as, investment banking and should be addressed during the implementation of any system changes or developments.

According to Wilson (2000:396), technology risk could arise from maintenance contracts for existing information technology (IT) infrastructure and application software through to the complete outsourcing of projects or the whole IT service. A firm could be exposed across all business areas to general technology risk. He (2000:396) also states that the operational risk manager should assess general technology risks by reviewing a firm’s compliance with the typical technology controls. Such controls would be designed to protect the IT facility against: human error; data theft; voice equipment failure; and other failures (media, control computer equipment, purchased software, undetected and ancillary equipment); to minimise exposure to fire, heat, water, smoke, corrosive fumes etc. He (2000:397) lists the following types of risk protection against the aforementioned risks:

• Physical protection.
• Functional protection.
• Data protection.

These will be discussed in more detail during the control element of the operational risk management process.
Based on the literature study regarding systems as an operational risk factor, the sub-risks could be summarised as follows:

- Systems failures.
- Security breaches.
- Non-development of systems and implementation failure.
- Insufficient systems capacity.
- Poor data integrity.

This list could be expanded or formulated more accurately according to the systems needs of the organisation.

3.2.2.3. Processes

According to various definitions of operational risk, it is once again evident that processes form an integral part of operational risk and could thus be seen as a main underlying risk factor. This is substantiated by the following examples:

- “The risk of loss caused by failure in operational processes...”
- “Operational risk is the exposure to financial or other damage arising through unforeseen events or failure in operational processes...”
- “Risks are associated with any other day-to-day business processing...”
- “Operational risk involves processing...”
- “Operational risk arises from failure to control...processing...”
- “Operational risk is the potential for loss caused by events such as the breakdown of processes...”
Wilson (2000:380) states that process risk is the risk of business process being insufficient and causing unexpected losses. A proactive operational risk function should be able to address the risks involved during any changes or developments of processes during, for example, mergers, acquisitions and disposals, environmental changes, the implementation of new systems and re-engineering of processes. Financial institutions rely on prompt, accurate and efficient data capturing and processing, which could also add to the management activity to address any processing risks in a proactive manner (Kingsley et al. 1998:5).

According to Crouhy et al. (1998:50), process risk would also include execution errors. The operational risk management process should also address these errors in order to prevent them from occurring. If they do occur, the process should reduce their adverse effects on the organisation.

The process environment, as seen by Davies et al. (1998:66), forms part of the operations environment and, as can be seen in figure 3.3, the components of the environment act upon and influence each other. Thus an external event, such as, the introduction of the Euro, could have an impact on a bank's process environment as it could influence the internal processes which relate to the activities involved in dealing with the Euro.

The process environment ultimately controls the quality of data integrity. This, according to Davies et al. (1998:66) includes both static data (for example, data concerning customers and instruments) and transaction data (for example, data concerning trades and positions).
Figure 3.3: The Operations Risk Environment

Source: Davies et al. (1998:66)

The risk could arise at any part of the process from order capture to the recording of the transaction to the general ledger. Davies et al. (1998:66) state that operational risk is, therefore, not limited to operation functions and may also exist in the following circumstances:

- **Set up**
  - The set up of new instruments and counterparties.
  - New business process to control the migration of new products into the process environment.

- **Pre-settlement activity**
  The settlement and agreement of trade data and details of settlements with third parties:
  - trade capture;
  - confirmation/affirmation;
• balancing to exchanges; and
• maintenance events, for example, rates re-fixes and expiries.

*Post-settlement activity*

The movement of and control over, cash and physical assets:

• processing of the movement of assets, for example, cash and stock;
• inventory management, for example, custody and corporate actions processing; and
• reconciliation of internal records to custodians and agents.

In order to address the processing risks, as part of operational risk, it must be determined exactly where the risks are within each environment. According to Davies *et al.* (1998:67), this activity can be initiated by looking at the process flow of a single trade, determining where the risk occurs and how it can be measured.

It is also evident that processes form an integral part of operational risk and could thus be seen as one of its main underlying risk factors.

These sub-risk factors of processes could be summarised as follows, based on the preceding literature study:

• Processing of new products.
• Recording and reporting.
• Business processes.
• Settlements and controls.
3.2.2.4. External Factors

External factors beyond the direct control and influence of the organisation could have an adverse effect on the internal underlying operational factors (people, processes and systems). It is imperative, therefore, that these external factors should be considered during an operational risk management process. The following extracts from various definitions confirm this view:

- "Operational risk also includes losses from external events..."
- "Operational strategic risk originates outside the firm since it stems mainly from external factors that are not under a bank’s direct control..."
- "...view business operational risk as encompassing all dimensions of the firm’s decentralised resources...as well as certain external areas, such as regulatory and fraud risk..."
- "...risk of business disruption, control failures, errors, misdeeds or external events..."

According to research conducted by PwC (1999:36), external events pertaining to operational risk include those beyond the institution’s control, for example:

- Systemic risk (an external issue affecting multiple institutions simultaneously with broad consequences);
- Exposure to other industry participants (for example, custodians, exchanges and SWIFT\textsuperscript{1});

\textsuperscript{1} SWIFT: Society of World-wide Inter-bank Financial Telecommunications
• Physical or natural disasters; or
• A change in regulation/law/accounting/tax.

It is important to understand that reference to external events is not intended to include defaults or market factors that would be captured under definitions of market and/or credit risk.

According to the FSA (1999:20), Banker’s Trust views fraud risk as an external risk factor. However, it could also evolve internally. Mayland (1993:3) states that fraud risk is the risk resulting from the illegal actions of the bank’s employees, customers, additional parties to a transaction or outside intruders. Systemic risk is also seen as a sub-risk factor. Mayland (1993:3) states that systemic risk arises when a bank participates in a payments or securities clearance network. If a network participant, for example, fails to settle and causes other participants to have liquidity problems, it is possible it could also suffer liquidity problems. Systemic risks, however, are a legitimate concern of credit administration and credit policy executives. There is a great deal of regulatory concern for systemic risk and most of the payments, securities and derivatives networks devote a great deal of effort to understanding and controlling systemic risk.

Regulations are another external factor that could cause operational risk for a bank. Mayland (1993:4) states that the regulators are concerned that some banks are not devoting enough management attention to the “off-balance-sheet” risks associated with corporate services. Regulators are therefore responding with specific requirements that force banks to manage operating credit risks as one of their priorities. For example, the Office of the Comptroller of the Currency, issued a Banking Circular in 1989, to alert national banks to the risks associated with large value payment systems. It also required that each national bank periodically assesses the risks associated with each system in which it
participates, documents procedures to perform the assessments; and monitors those risks on an ongoing basis. In addition, it further defined the risks that should be assessed and managed. These include credit risks as well as settlement, liquidity/systemic risks, operational risks, legal risks and sovereign risks (Mayland 1993:4).

Rachlin (1998:127) lists the following sub-factors of external environmental risk:

- Outsourcing/external supplier risk.
- Physical security.
- Money laundering.
- Compliance.
- Financial reporting.
- Tax.
- Legal (litigation).
- Natural disaster.
- Terrorist threat.
- Strike risk.

Because banks have no direct control over that part of operational risk which is generated by the external factors, it is difficult to manage it proactively. Although it is difficult to quantify these factors, it is important for a bank to anticipate and address the relevant issues in order to reduce the factors' adverse effects.

As with the other main underlying risk factors of operational risk, external factors can be divided into sub-risks to demarcate the areas that should be addressed during the management process, namely:

- Criminal activities.
• Catastrophes/natural disasters.
• Regulations/compliance.
• Information security.
• Economic and political activities.

Once again it must be emphasised that this list could be expanded, depending on the exposures of the organisation.

3.2.3. Methods of Risk Identification

The Financial and Management Accounting Committee (FMAC) (1999:17) states that management and other relevant personnel could identify the key risks in a number of ways, for example:

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

The FSA (1999:64) states that the tools for identifying risks could include checklists, questionnaires, standard templates and facilitated workshops. The estimation of the impact and probability of the risk event is, however, usually left
to the judgement and experience of the business unit manager. Sometimes loss data of external or internal events could provide management with examples of the impact of similar events. In a diverse organisation, questionnaires tend to be less useful as the questions they contain may not be very business specific. However, where an institution is involved in similar business at a number of sites, for example, the branch network in a retail bank, a more detailed questionnaire may be suitable because of the homogeneous nature of these business units.

According to a survey by PwC (1999:53), multiple tools are being used to manage operational risk. They use “tools” as a general term for specific methodologies or procedures that help to facilitate the identification, assessment, control and management of operational risk. They (1999:53) also state that operational risk management tools have proved valuable to companies in raising awareness, tracking and monitoring risk and assessing financial impact. The tools they surveyed are self-risk assessment, risk maps/process flows, risk indicators, escalation triggers and loss event databases.

It seems there is a close relationship between methods and “tools” for the identification and on assessment of operational risk. This relationship will be discussed in more detail in the next section on the evaluation of operational risk.

3.2.4. Conclusion

It is evident that although the sub-risks pertaining to the underlying main risk factors were summarised, an exhaustive list of all the sub-risks could not be compiled as it will differ from one organisation to another, depending on the organisation’s risk exposures. The potential standardisation of the sub-risks for each underlying risk factor therefore seems a near impossible task.
The following section will concentrate on the next step of the operational risk management process, that is, the evaluation of operational risk.

3.3. Evaluation of Operational Risk

Valsamakis et al. (1996:104) state that risk evaluation fulfils a dual role: one of facilitating the method of treatment, the other of measuring the effect or degree of success following implementation. During the evaluation of risk one can, according to Crouhy and Mark (2000:351), assess operational risk in terms of the likelihood of operational failure and the severity of potential loss (given that a failure occurs). They (2000:371) also state that the process of operational risk assessment needs to include a review of the likelihood (frequency) of a particular operational risk occurring as well as the magnitude (severity) of the effect that the operational risk will have on the business. The assessment should include the options available to manage and take appropriate action to reduce the risk. The assessment of operational risk, however, is much more complicated than, for example, market or credit risk. These types of risk are mostly based on factual data such as prices, volatility and other external data contained in large databases.

According to O'Brien (1999:16), the banking industry is on notice that it has to step up its thinking about how to measure and not simply manage operational risk. The need to quantify operational risk was also emphasised by the major publicised losses at financial institutions during the past few years, which were wholly or partly due to operational risk. For example, the losses sustained during 1998 by investors in hedge fund long-term capital management and by Sumitomo, Daiwa, Natwest and Barings.
According to the Basel Committee (1998a:3), most banks are considering the measurement of operational risk, but only a few have formal measurement systems in place. The existing methodologies are relatively simple and experimental, although a few banks seem to have made considerable progress in developing more advanced techniques. Measuring operational risk requires both an estimate of the probability of an operational loss event and the potential size of the loss. Most approaches rely to a certain degree on risk indicating factors to provide an indication of the likelihood of an operational loss event occurring. These factors are generally assessments that are translated into grades (such as an audit assessment), for example, grades from qualitative assessments such as internal audit ratings as well as data on quality of operations such as error rate or measures of business riskiness such as revenue volatility. Banks that incorporate these factors into their measurement approach can use them to identify those business activities with a high degree of operational risk (Basel 1998a:4).

In interviews with thirty major banks on operational risk, during September 1998 the Basel Committee found that many banks have identified significant conceptual issues and data needs which would need to be addressed in order to develop general measures of operational risk. Operational risk factors are largely internal to a bank and a clear mathematical and statistical link between risk factors and the likelihood and size of operational losses does not exist. Experience with large losses is limited and many banks lack historical data on their own operational losses and their causes.

Bloom and Galloway (1999:3) state that operational risk is an “inside job” related to the interaction of people, processes, systems and culture. They (1999:3) also state that operational risk is more difficult to measure than market
or credit risk due to a lack of data. For example, the management of market risk is underpinned by the factual world of prices, volatility and other external data, packaged with significant history in large databases. An actuarial approach to operational risk, however, struggles with this lack of objective data. According to Bloom and Galloway (1999:3), there is little historical data on operational risk occurrences and despite pleas to develop shared databases, the likelihood of gathering enough data to support an actuarial method seems remote. Given the evolving nature of operations, an historical view of operational risk may not be the right approach. Thus banks should rather develop suitable internal measures for operational risk to substitute historical risk data. This means identifying categories and classes of risk and gathering all readily available evidence which, together, can support a reliable measure of operational risk in each area of activity and for each category. The evidence can include known risk experience, inherent risk scoring mechanisms and subjectively based measurements of risk impact and likelihood.

Crouhy and Mark (2000:351) state that clear guiding principles for the operational risk measurement process should be set to ensure that it provides an appropriate measure of operational risk across all business units throughout a bank. These guiding principles are illustrated in figure 3.4.
They (1998:52) explain the guiding principles as follows:

- **Objectivity**: operational risk should be measured using standard objective criteria.
- **Consistency**: similar operational risk profiles in different business units should result in similar reported operational risk.
- **Relevance**: risk should be reported in a way that makes it easier to address the operational risk.
- **Transparency**: all essential operational risk should be reported and assessed in a way that makes the risk management transparent to senior managers.
- **Bank-wide**: operational risk measures should be designed in such a way that the results can be aggregated across the entire organisation.
- **Completeness**: all material operational risks should be identified and captured.
Crouhy and Mark (2000:387) list the following key tasks to be addressed by a measurement method:

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

Crouhy et al. (1998:52) also describe a four-step measurement process for operational risk, namely:

- **Input (Step 1).** The first step is to gather the information needed to perform a complete assessment of all significant operational risks. A useful source of information is, for example, reports, such as audit and regulatory reports (see table 3.5). It is, however, important to verify the information contained in these reports. Any gaps in information could be filled through discussions with the relevant managers. Particular attention should also be paid to any changes in the business or operating environment that occurred after the information was first produced.

- **Risk Assessment Framework (Step 2).** The information gathered in step 1 needs to be analysed and processed through a risk assessment framework an example of which is depicted in figure 3.5. The framework allows for the assessment of the four
underlying risk factors of operational risk (people, processes, technology and external factors).

Table 3.5: Sources of Information in the Measurement Process of Operational Risk

<table>
<thead>
<tr>
<th>Likelihood of occurrence</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit report</td>
<td>Management interviews</td>
</tr>
<tr>
<td>Regulatory reports</td>
<td>Loss history</td>
</tr>
<tr>
<td>Management reports</td>
<td></td>
</tr>
<tr>
<td>Expert reports</td>
<td></td>
</tr>
<tr>
<td>Business recovery plans</td>
<td></td>
</tr>
<tr>
<td>Budget plans</td>
<td></td>
</tr>
<tr>
<td>Operations plans</td>
<td></td>
</tr>
</tbody>
</table>

Source: Adapted from Crouhy et al. (1998:54)

Figure 3.5: Measurement Process of Operational Risk – Risk Assessment Framework

Source: Adapted from Crouhy et al. (1998:54)
The internal and external dependencies (discussed previously in this chapter) may be assessed in terms of capacity, capability, and availability.

The likelihood that an operational failure may occur within the next year should be assessed for each of the four underlying risk factors. This assessment could be expressed as a rating along a five-point likelihood continuum as depicted in table 3.6.

**Table 3.6: Five-point Likelihood Continuum**

<table>
<thead>
<tr>
<th>Likelihood that an operational failure will occur within the next year</th>
</tr>
</thead>
<tbody>
<tr>
<td>VL</td>
</tr>
<tr>
<td>L</td>
</tr>
<tr>
<td>M</td>
</tr>
<tr>
<td>H</td>
</tr>
<tr>
<td>VH</td>
</tr>
</tbody>
</table>

Source: Crouhy et al. (1998:56)

The next action is the severity assessment, which describes the potential loss to the bank when an operational failure occurs. Typically, this could be expressed as a numerical value. The severity should be assessed for each identified risk exposure. Operational risk measures are not exact as there is usually no easy way to combine the individual likelihood of loss and severity assessments into an overall measure of operational risk within a business unit. For an accurate measurement, the likelihood of a loss would need to be expressed in numerical terms, for example, low risk: 0% - 10%, medium risk: 10% - 60%, and high risk: 60% - 100%. This cannot be accomplished without statistically
significant historical data on operational losses. The financial industry currently measures operational risk using a combination of both qualitative and quantitative data. According to Crouhy and Mark (2000:357), an organisation should strive to take a quantitative approach based on statistical data. Where the data is unavailable or unreliable, a qualitative approach may be used to generate a risk rating. Neither approach, however, on its own tells the whole story. The quantitative approach is often too rigid, while the qualitative approach is often too vague. The hybrid approach requires a numerical expression of the amount at risk, based on both quantitative and qualitative data.

Once gathered, the relevant data may be shown in a summary report as illustrated in table 3.7.

Table 3.7: Example of a Risk Assessment Report

Likelihood of event (in 12 months)

<table>
<thead>
<tr>
<th>Operational risk scenarios</th>
<th>Internal dependencies</th>
<th>External dependencies</th>
<th>Overall assessment</th>
<th>Severity (Value)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>People Process Technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outsourcing</td>
<td>L VL VL</td>
<td>M M</td>
<td>M</td>
<td>50-100</td>
</tr>
<tr>
<td>Privacy</td>
<td>L M VL</td>
<td>L L</td>
<td>L</td>
<td>50-100</td>
</tr>
<tr>
<td>Compliance</td>
<td>L VL VL</td>
<td>VL VL</td>
<td>L</td>
<td>35-70</td>
</tr>
<tr>
<td>Fraud</td>
<td>L L VL</td>
<td>VL VL</td>
<td>L</td>
<td>5-10</td>
</tr>
<tr>
<td>Downsizing</td>
<td>L VL VL</td>
<td>L L</td>
<td>L</td>
<td>5-10</td>
</tr>
<tr>
<td>Political environment</td>
<td>VL M VL</td>
<td>VL VL</td>
<td>L</td>
<td>5-10</td>
</tr>
<tr>
<td>Overall assessment</td>
<td>L M VL</td>
<td>L L</td>
<td>L</td>
<td>150-300</td>
</tr>
</tbody>
</table>

Source: Crouhy *et al.* (1998:57)
• **Review and Validation (Step 3).** After a summary report is generated, senior business management should review it. Thereafter the operational risk committee should review it to ensure that the framework was applied consistently across the business.

• **Output (Step 4).** The last step is to formally report the final assessment of operational risk to business management. The output of the assessment process, as presented in figure 3.6, has two main uses. Firstly, to provide better operational risk information to management to use in risk management decisions and, secondly, to reflect the extent of the exposure of the business unit to operational risk. Generally, operational risk assessment guides management action in deciding, for example, whether to purchase insurance to mitigate some of the risks.

**Figure 3.6: Fourth Step in the Measurement Process of Operational Risk**

![Operational Risk Reporting and Analysis](image)

- Better capital allocation
- Improved Risk Reporting and Analysis
- Management Action
  - Investment
  - Divestment
  - New development
  - Tighter controls
  - Insurance/risk financing

Source: Crouhy *et al.* (1998:57)

Furthermore, the overall assessment of the likelihood of operational risk and severity of loss for a business unit could be plotted to provide relevant information on operational risk exposures across the bank as
depicted in figure 3.7. The figure indicates clearly that if a business unit falls in the upper quadrant, then the business unit has a high likelihood of operational risk and a high severity of loss (if failure occurs). These units should be the focus of management's attention.

Figure 3.7: Summary of Risk Reporting

![Risk Reporting Diagram]

Source: Adapted from Crouhy et al. (1998:58)

It is evident from the above-mentioned that the measurement should entail the quantification risk factors in a consistent manner throughout the organisation, to determine the extent of operational risk. A variety of risk measurement approaches may be used, depending on the business need and the appropriate level of sophistication. Risk measurement then serves as a basis for control mechanisms such as the setting of limits or constraints to prevent or minimise operational risk.
3.3.1. Approaches to Measuring Operational Risk

Kinglsey et al. (1998:7) state that there are a number of methodologies for measuring operational risk. These range from simplistic to much more detailed calculations. One of the critical steps during the evaluation of operational risk is to determine and agree on the methodology of measuring it. In this regard, operational risk is one of the risks that does not lend itself to easy quantification. According to Stoll (1996:4), this could pose a problem, especially if a bank requires visible benefits of a risk adjusted performance measure and wants to determine the allocation of capital relating to operational risk.

According to Alexander (2000:2), choosing the best methodology for any given category of operational risk is less of an issue than the application of the methodology or model to produce meaningful measures of operational risk. The major problem with any model for operational risk is the adequacy of data as depicted by Alexander (2000:2) in the following examples:

- Internal loss event data for low-frequency/high-impact risks such as fraud may be too incomplete to estimate an extreme value distribution for measuring the tail loss. Augmenting the database with external data may also not be appropriate.
- Operating costs have a tenuous relationship with operational loss. As such, the proportional charges that regulators are considering for operational risk, based on a fixed percentage of operating costs, may be very inaccurate.
- Internal risk ratings are based on assessments of the size and frequency of operational losses from the different activities in a business unit. This data is likely to be inaccurate because it is subjective.
Regression models of operational risk that are based on the Capital Asset Pricing Model (CAPM) framework, produce betas that are based on many subjective choices of data. For example, what constitutes a "reputational event" in regression models of shareholder value for reputational risk?

The inadequacy of the data means that subjective choice is much more of an issue in operational risk than it is in market or credit risk measurement, for example. Some models for measuring operational risks use observable, and therefore "objective" data. In such models, however, it is still necessary to take many decisions that result in subjective choices. Other models for operational risk are based almost entirely on subjective estimates of the probabilities and impacts of events that are thought to contribute to operational loss.

The FMAC (1999:17) states that once risks have been identified, an assessment of the possible impact and corresponding likelihood of occurrence may be made. They (1999:17) describe the concepts as follows:

- **Impact.** The assessment of the potential impact of a particular risk may be complicated as a range of possible outcomes may exist or the risk may occur a number of times in a given time period. Such complications should be anticipated and a consistent approach adopted which may, for example, seek to estimate a worst case scenario over a given period. The assessment of the impact of the risk on the organisation should take into account the financial impact, the impact on the organisation's viability and objectives as well as the political and community sensitivity. The analysis may be either qualitative or quantitative, but should be consistent to permit comparisons. An example of a qualitative approach is
using a scale to determine impact. Table 3.8 indicates how such a scale could be used.

<table>
<thead>
<tr>
<th>Scale</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Financial impact on the organisation is likely to exceed a value; or have a significant impact on the organisation’s viability or strategic objectives; or significant impact on political and/or community sensitivity.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Financial impact on the organisation is likely to be between two values; or have a moderate impact on the organisation’s viability or strategic objectives; or a moderate impact on political and/or community sensitivity</td>
</tr>
<tr>
<td>Low</td>
<td>Financial impact on the organisation is likely to be between two values; or have a minimal impact on the organisation’s viability or strategic objectives; or a minimal impact on political and/or community sensitivity</td>
</tr>
</tbody>
</table>

Source: Adapted from the FMAC (1999:18)

- **Likelihood.** The likelihood of a risk occurring may be based on a gross, net and/or a target basis. The gross basis assesses the inherent likelihood of the event occurring in the absence of any processes that the organisation may have in place to reduce that likelihood. The net basis assesses the likelihood. It takes into account current conditions and processes to mitigate the chance of the event occurring. The target likelihood of a risk occurring reflects the risk appetite of the organisation. Where the net
likelihood and the target likelihood for a particular risk differ, the risk profile would need to be altered accordingly. According to PwC (1999:19), it is common practice to assess likelihood in terms of:

- High – probable;
- Moderate – possible; or
- Low – remote.

The scale depicted in table 3.9 may be used to indicate the likelihood of occurrences.

**Table 3.9: Scale to Determine the Likelihood of Occurrences**

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Description</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Probable. Likely to occur in a one-year period; or more than 25% chance of occurrence.</td>
<td>Potential of it occurring several times within the next 10 years; has occurred within the past two years; typical of operations of this type due to external influences.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Possible. Likely to occur in a 10-year period; or less than 25% chance of occurrence but greater than 2%.</td>
<td>May occur more than once within the next 10 years; may be difficult to control due to some external influences; history of occurrence in the organisation.</td>
</tr>
<tr>
<td>Low</td>
<td>Remote. Not likely to occur in a 10-year period or less than 2% chance of occurrence.</td>
<td>Has not occurred in this country; would be surprising if it occurred.</td>
</tr>
</tbody>
</table>

Source: Adapted from PwC (1999:19)
Although some methodologies for the measuring of operational risk seem quite complicated, a bank should determine the best method to use to ensure the best result. In this context the different approaches and models to measure operational risk will be discussed under the following:

- Qualitative approaches to measure operational risk; and
- Quantitative approaches to measure operational risk.

3.3.1.1. Qualitative Approaches to Measuring Operational Risk

Most approaches to operational risk and internal control are qualitative in that the identification of operational risk is measured in words rather than numbers. Wilson (2000:388) states that a common approach is to perform a review of the way a business manages operational risk and then to perform a risk assessment based upon the “objective” judgement of an experienced reviewer.

Self-risk assessments and risk maps/process flows are popular qualitative methods.

Self-Risk Assessments. According to the FSA (1999:10) this method is becoming the classic “bottom-up” way of thinking about operational risk. However, relatively few banks currently use this approach to determine economic capital. In this approach, each business unit, in collaboration with the central operational risk control unit, assesses the operational risk it is exposed to. This is done on the basis of inside knowledge (including that of internal audit and possible simple modeling), but also of wider thinking to extreme events and experiences. PwC (1999:56) regards self-risk assessment as an internally driven analysis of risks, controls and their implementation. Its objective is an open, common understanding of the strengths and weaknesses of the operational risk
environment. Self-risk assessment could also be seen as a key tool to identify issues, raise awareness, create common understanding and achieve recognition that the business units create, manage, and mitigate operational risks.

There are, however, several drawbacks to this approach. The FSA (1999:10) lists the following examples:

- It may backfire and turn a helpful methodology for business units into something far more regimented.
- Some banks will complete the exercise more fairly than others.
- Business units may not be good at estimating risks.
- Business units may perceive risks differently.
- The experience of staff could have an effect on the estimation of risk.

On the other hand, the FSA (1999:10) states that self-risk assessment is a common approach and many banks have a degree of experience in its implementation. It may be possible to build on this experience as it is a useful method to help control operational risk.

The FSA (1999:63) states that the process of operational self-risk assessment has three important components, namely:

- an analysis by business unit managers of the risks their unit is facing;
- an estimation by these managers of the loss that could arise as a result of these risk events occurring; and
- the use of the aforementioned to compute a capital charge.
According to PwC (1999:58), self-risk assessments have tended to be a "bottom-up" activity where the primary emphasis is on the business unit which takes the risk and knows the operation best. The main contributors to any self-risk assessment approach, therefore, are the business unit's operational risk staff and its front- and back-office staff. A new trend, however, is to use a top-down approach for self-risk assessment. This approach allows for more frequent reviews and generally is more accepted as a value-added exercise at the business unit level. According to the FSA (1999:65), the process of self-risk assessment requires management to make estimates of the likely impact of operational risk events and the probability of the event arising. Management in many businesses has to do this with little historic data to base their estimates on. As with any form of estimating, it is not an exact science. The resulting figures, which may give rise to capital allocation using this method of self-risk assessment, will depend on a number of factors. According to the FSA (1999:65-66), these factors include the following:

- The perception of the business unit management of what a large loss is. Different business unit managers, even within the same business unit, will have different perceptions of what they see as a large or the largest possible loss. This is likely to lead to inconsistency between business units in an organisation and, more importantly, between organisations.

- Whether consciously or not, a business unit's targets and budgets may influence its estimates. There may be some self-interest in making the estimations of impact and probability either higher or lower. This would be to either gain greater financing for the area or to present the area as less risky than may otherwise be the case.

- The time horizon used by the business is likely to influence the frequency and size of the loss it estimates. For example, where a
business’s management considers potential losses over a short term, say, one year, they are more likely to estimate that smaller losses will arise. However, if they consider a longer time horizon, for instance 10 years, they are more likely to estimate or accept a larger loss that may arise in this period. Therefore, businesses with shorter time horizons are likely to estimate more frequent but smaller losses than those with longer time horizons that will estimate larger but less frequent events.

- The loss experience of the business managers will be important in determining the types and sizes of losses they identify. For instance, very few people have suffered IT security breaches. This type of loss, therefore, is likely to be assessed as smaller than the, more commonly suffered, external fraud attempt.

- Certain losses are more emotive than others and are likely to be given a higher prominence by business managers. For example, fraud and computer viruses are emotive subjects and are likely to get much higher focus than, for instance, clerical errors or poor computer software maintenance.

- Whether or not business unit management’s estimates inherently include expected and unexpected losses.

Laycock (1998:137) states that risk assessments based on the use of expert panels or intuitive “gut feeling” often distinguish between frequency and severity of events. One frequently used tool is the risk assessment grid that is illustrated in figure 3.8. Managers can use this grid to adjust their response to risks that are low-frequency/high-impact and those that are high-frequency/low-impact in nature.
Figure 3.8: Risk Assessment Grid

Source: Adapted from Laycock (1998:137)

PwC (1999:56) identifies four general approaches that may be used during self-risk assessments, namely:

- **Questionnaires.** The typical approach is to start with a comprehensive list of controls and ask for compliance with them. Best-practice lists, that are unique for each type of business or process, may then be accumulated and turned into a checklist questionnaire.

- **Issue-orientated forms.** This approach is briefer than questionnaires. It often starts with a risk map, then request textual open-ended responses on how risks are being controlled; to what extent controls are in place; how risks are monitored and
measured to assure controls are operating; and what improvements can be made to the organisation.

- **Facilitated workshops.** These workshops are usually attended by a cross-section of a business unit's operational and support staff and are facilitated by an operational risk management function facilitator. In most workshops, the delegates identify the risk issues, the biggest risks facing the organisation and the steps needed to take corrective action.

- **Independent assessments.** An independent party, whether risk management or internal audit, perform a comprehensive review of operations, risks and controls and prepares an assessment report that is reviewed with the business unit.

Self-risk assessment may be a single activity or a variety of activities that trigger discussions and elicit reflections on the operational risk facing the business. They also provide an assessment of the operational risk management techniques employed. The deliverable for all these self-risk assessment approaches is a report that presents the findings, the issues identified and a timetable or work-plan for corrective action and continuous improvement at both a summary and detailed level. The challenge in all these self-risk assessment approaches is to create an open forum with independent participation that ensures objectivity. Without this forum many organisations tend to simply report that risks are under control instead of giving the process its proper attention (PwC 1999:59).

According to the FSA (1999:67), the concept of self-risk assessment has arisen out of the need for business unit management to obtain more a formal and better understanding of their risks and controls and their interrelation. This then allows management to assign responsibility and develop action plans to further mitigate risks where necessary. This approach can also benefit organisations by improving
its risk control culture by focusing business units on the management of operational risk in a formalised manner. However, to extend this process by adding a resulting capital charge, based on business unit management’s assessment, is likely to be seen by some of them as a penalty for their honesty and openness.

The FSA (1999:67) states that as with all self-risk assessment programmes, the following are required in varying proportions to make the output from the process reliable:

- A culture of trust, openness and honesty between the central function or authority using the information that is collected and the participants completing the self-assessment;
- A sufficient audit trail for the data collected and aggregated;
- An expectation that the level of any data manipulation by participants is less than the increased benefits it could generate;
- Recognition by participants of the severity of sanctions if they are misleading in any way;
- A consistency of approach between business units and organisations.

For the results of a self-risk assessment exercise to be reliable when calculating a capital charge there must be no duplication in the assessment of risks. While checklists and questionnaires may help ensure completeness, the only tool that can assist with the identification of duplication is a thorough independent review of the assessment. Thus, any decision to use this technique should include consideration of the concern around duplication. The extension of the self-risk assessment process to calculate a capital charge may also result in management
becoming aware of a process that is currently widely accepted as helping to improve operational risk management in businesses.

*Risk Maps/Process Flows.* Risk maps/process flows may be used to identify and analyse operational risk. Risks may be identified by type, business unit or organisation functions. The results may be used to assess weaknesses, raise awareness and prioritise actions (PwC 1999:60).

PwC (1999:60) states that risk maps are often the first technique applied to any operational risk analysis. They take a business or process, analyse it to identify all the inherent risks and define the desired or appropriate controls. Process flows are closely related to risk maps in that they provide diagrammatic representation of processes and define the key risk and control points at each step.

The information for the risk maps/process flows is collected mainly through interviews, focus groups, and/or facilitated meetings or workshops with the business units. The key tasks are outlined and the responsibilities and accountabilities are confirmed or defined. This information is primarily in the form of narratives of risks and controls. The resulting reports can, for example, raise awareness, provide a top-down view of key risks and identify gaps in responsibilities (PwC 1999:61).

Although risk maps/process flows are valuable, PwC (1999:61) states that one should understand their limitations, namely:

- Risk maps/process flows are detailed bottom-up tools of which the results are appropriate for line personnel, but too detailed for use by senior management;
- The analysis is qualitative and reflects staff’s perceptions; and
- Risk maps/process flows define the risks, potential weak points and standards for control, but do not identify how well those controls are being followed.

According to the FMAC (1999:20), however, risk maps or risk matrices are widely viewed as a simple yet powerful way of displaying the relationship between likelihood and impact of identified key risks, thus providing both measurement and reporting of the risk profile. A typical example of a risk map is depicted by the FMAC in figure 3.9.

**Figure 3.9: Example of a Risk Map**

<table>
<thead>
<tr>
<th>HAZARD</th>
<th>LIKELIHOOD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Impact</strong></td>
<td><strong>High</strong></td>
</tr>
<tr>
<td>Property development approvals</td>
<td>Schedule delays caused by subcontractors or systems integration difficulties</td>
</tr>
<tr>
<td>Production quality problems</td>
<td>Construction cost overrun</td>
</tr>
<tr>
<td>Serious accident</td>
<td>Loss of certification at any site</td>
</tr>
<tr>
<td>Corporate governance or succession planning</td>
<td>Information systems and communication facilities at any site</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Low (Remote)</strong></td>
<td><strong>Medium (Possible)</strong></td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td></td>
</tr>
</tbody>
</table>

Source: Adapted from the FMAC (1999:21)
It is evident that the aforementioned may be used to qualify operational risk issues that may serve as a basis for management and control purposes. It is also evident, however, that a quantitative approach in measuring operational risk is necessary to determine a basis for capital allocation.

3.3.1.2. Quantitative Approaches to Measuring Operational Risk

PwC (2000:2) states that operational risk may be the most significant risk an organisation faces. Consequently, organisations need a quantification framework to understand and effectively manage operational risk. Up until now the data and methodology to support such a quantification process have not been available. According to Crouhy and Mark (2000:362), banks have started to develop databases of historical operational risk events in an effort to quantify various unexpected risks. The intention is to use the databases to develop statistically defined “worst-case” estimates. These estimates may then be applicable to a selected subset of a bank’s business in the same way that many banks already use historical loss data to derive credit risk measures.

In order to allocate capital to operational risk it seems imperative to quantify it. Banker’s Trust is one of the first banks to describe how to calculate operational risk capital. Wilson (2000:391) lists the following steps used by Banker’s Trust:

- Identify centralised information (from centralised departments such as human resources) which predicts control risk across the entire organisation (for example, staff turnover);
- Categorise which risks the information falls under (for example, human resources risk); and
- Compare new information to the existing internal and external loss information on the databases.
The most common way of analysing operational risk from a quantitative perspective is to determine losses arising from the daily operations of a bank. A paper published by the Manchester Business School on quantifying the mishandling of losses, shows that it is quantifiable and there is a significant amount of data available in the bank. The mishandling of a loss was defined as a loss arising from a control failure or uncontrolled process which will result in, for example, one of the following:

- Compensation being paid to a counterparty for any loss incurred by them.
- Charges being levied by corresponding banks to cover amendments or cancellations.
- Overdraft costs.
- Funding losses – where an account is overdrawn due to incorrect funding and the overdraft rate is higher than the funding rate.
- Penalty fees charged by corresponding banks or central banks for late payments, amendments or cancellations, for example.
- Opportunity loss – where no actual loss is made but funds are not under the bank’s power to invest, hence an opportunity to invest funds at a higher rate was missed.

Kingsley et al. (1998:9) identify two fundamental approaches to detailed calculations of operational risk namely top-down predictive modeling and bottom-up risk profiling.

- *Top-down predictive mathematical modeling* aims to measure the absolute and relative operational risks of businesses. It typically uses actuarial techniques such as:
• Modeling of low-value/high incident rate losses;
• Chaos theory modeling of high-value/low-incidence rate losses;
• Organisation's own loss experience; and
• Risks of new activities based upon reported loss experience in the market.

However, according to Kingsley et al. (1998:9), a limited number of firms already have functions specifically dedicated to high-value/low-incidence rate losses. These functions have established methodologies for evaluating exposures and the likelihood of such rare events occurring. The top-down approach provides for a swift implementation of an operational risk measurement process and can quickly result in revised allocations and improved management information. Kingsley et al. (1998:9) state that the top-down approach also represents a good start and best first estimate of the exposures. Financial institutions, however, will want to supplement it with operational risk profiling to capture improved accuracy and to help motivate individual line managers to reduce risk.

• The bottom-up operational risk profiling employs a detailed analysis of individual business processes, the controls in place and the identification and quantification of individual risks. By using a decision tree, for example, the value at operational risk can be derived as a function of:

\[
\text{Value of potential losses} \times \text{Chance of risk events occurring} \times \text{Chance of controls not preventing loss} = \text{Value at Operational Risk}
\]
The values and probabilities may be derived directly from management reports or by using score mechanisms. Operational risk profiling takes a long time to implement and requires particular care regarding the way potential losses and probabilities are determined. According to Kingsley et al. (1998:10), however, it provides the following:

- Ongoing assessment and upgrading of controls;
- Improved management information;
- Greater awareness and insight into the causes of operational losses;
- Motivation to change methods and behavior to reduce operational risk and improve control and returns from existing capital allocations; and
- A method of calculations that is transparent and often secures better buy-in and acceptance of the result.

Hoffman's approach (1998:34) to quantify operational risk is to identify a number of possible conceptual foundations for operational risk modeling, namely:

- *Factor-derived models.* These apply loss and/or causal factors to build a bottom-up prediction of loss expectancies;
- *Economic pricing models.* These are base forecasts on economic models. One such operational risk model uses the capital asset pricing model (CAPM) to suggest a relative distribution of pricing for operational risk among the other price determinants for capital;
- *Scenario analysis/subjective loss estimate models.* These models are used to capture diverse opinions, concerns and experience or
expertise of key managers and represent them in a matrix and graphic form; and

- *Statistical/actuarial loss potential models*. These use actual loss data to construct representations of loss frequencies and severity in the form of statistical probability distributions. Simulation techniques are then used to combine the distributions in modeling possible loss scenarios for the future.

Another approach to quantify the assessment of operational risk is by Peterken who concentrates on catastrophic risk as one of the external factors of operational risk. He (1998:15) states that catastrophic risk affects all businesses. Advances in the natural sciences have provided techniques with which these risks may be assessed and integrated into a company’s risk management strategy. According to Peterken (1998:15), catastrophic models produce individual forecasts of losses known as estimated maximum loss (EML). By taking the EML across a large number of different scenarios, in terms of location of the hazard and its intensity, loss exceedance curves (see figure 3.10) may be derived. These curves give the probability of a loss equal to or greater than a specified amount and may be used to calculate limits for insurance and other risk-transfer methods. They may also identify areas for risk-reduction programmes and assist in prioritising management efforts.

The area under a loss exceedance curve gives the annual average loss (AAL). This is the expected loss over a long period to the business. It is equivalent to the pure technical cost of risk (that is, the cost of transferring risk but before an amount for the uncertainty in those estimates and the randomness of their outcomes is made). Peterken (1998:15) states that AAL is a powerful statistic which may be used to compare levels of risk in different businesses and to evaluate the value of risk-transfer.
Figure 3.10 also indicates the loss exceedance curve where probabilities of occurrence become very small. Here there are two points of interest. The first point being the maximum possible loss (MPL), which paradoxically is set by management attitude to risk – the lowest probability they wish to take into account. The second is the maximum physical event (MPE), which is the loss caused by the largest event intensity possible, regardless of its probability.

**Figure 3.10: Loss Exceedance Curves**

Source: Peterken (1998:15)

Notwithstanding the preceding approaches and methodologies are used to quantify operational risk, the following are the most extensively used:
• The causal modeling of operational risk;
• Risk indicators;
• Escalation Triggers; and
• A loss-event database.

Each of the above-mentioned methods will now be discussed in detail.

*The Causal Model Approach to Quantify Operational Risk.* According to Wilson (2000:390) this methodology comprises the following steps:

• Define operational risk;
• Document and collect data;
• Build a prototype of the system;
• Refine data collection; and
• Finalise prototype and roll out throughout the organisation.

The FSA (1999:7) states that causal modeling for operational risk sets out a framework to determine regulatory capital. A prerequisite of this model is that it is essential to observe causes as well as effects (losses), otherwise the database will consist of useless information. For example, a lack of internal controls such as the segregation of duties is a cause, while a loss event such as fraud is the effect. In order to identify the causes and effects, Wilson (2000:393) states that it is also essential to split operational risk into “sub-risk categories”. He illustrates this approach by the example depicted in table 3.10, which indicates the “sub-risk category”, the effect or potential loss and the cause of the loss.
Table 3.10: Potential Losses and Possible Causes of Risk

<table>
<thead>
<tr>
<th>Risk category</th>
<th>The effect/potential loss</th>
<th>The causes of the loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process risks</td>
<td>Variance in process costs from predicted levels.</td>
<td>Declining productivity as volume grows.</td>
</tr>
<tr>
<td>Control risks</td>
<td>Variance in costs as a result of control failures.</td>
<td>Process malfunction, control failure, fraud.</td>
</tr>
<tr>
<td>Project risks</td>
<td>Project costs overruns/ failures.</td>
<td>Poor planning, project management, poor budgeting.</td>
</tr>
<tr>
<td>Technology risks</td>
<td>Variance in technology running costs from predicted levels.</td>
<td>Year 2000 upgrade expenditure required. Application development.</td>
</tr>
<tr>
<td>Human resource risks</td>
<td>Variance in revenue/ profits (for example, cost of recruiting replacements and training).</td>
<td>Loss of key staff due to defection to competitor.</td>
</tr>
<tr>
<td>Client service risks</td>
<td>Variance in revenues or profits as a result of customers lost.</td>
<td>Inappropriate derivative sale followed by litigation to poor ethical reputation. Poor client service.</td>
</tr>
<tr>
<td>Supplier management risks</td>
<td>Variance in costs of inputs (for example, purchases of resources).</td>
<td>Increases in consulting fees over budget due to poorly negotiated contract.</td>
</tr>
<tr>
<td>Regulatory risks</td>
<td>Reputation damage and fines levied by regulators.</td>
<td>Failure to follow regulatory procedures.</td>
</tr>
</tbody>
</table>


Wilson (2000:393) states that it is much easier to collect data on the effect of losses than the cause of losses. As such many banks start by collecting the losses and then try to fit the causes to them. An example of sources of loss data is shown in table 3.11.
Table 3.11: Sources of Loss Data

<table>
<thead>
<tr>
<th>Type</th>
<th>Sources of probability and magnitude of loss data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process risks</td>
<td>Historical variances</td>
</tr>
<tr>
<td></td>
<td>Supplier/vendor estimates</td>
</tr>
<tr>
<td></td>
<td>Industry benchmarking</td>
</tr>
<tr>
<td>Control risks</td>
<td>Historical variances</td>
</tr>
<tr>
<td></td>
<td>Industry and non-industry benchmarking</td>
</tr>
<tr>
<td></td>
<td>Delphic techniques based on business assessments</td>
</tr>
<tr>
<td>Project risks</td>
<td>Historical variances</td>
</tr>
<tr>
<td></td>
<td>Industry and non-industry benchmarking</td>
</tr>
<tr>
<td>Technology risks</td>
<td>Historical variances</td>
</tr>
<tr>
<td></td>
<td>Supplier/vendor estimates</td>
</tr>
<tr>
<td></td>
<td>Industry benchmarking</td>
</tr>
<tr>
<td>Human resources risks</td>
<td>Delphic techniques based on business assessments</td>
</tr>
<tr>
<td>Client service risks</td>
<td>Delphic techniques based on business assessments</td>
</tr>
<tr>
<td>Supplier management risks</td>
<td>Historical variances</td>
</tr>
<tr>
<td></td>
<td>Supplier/vendor estimates</td>
</tr>
<tr>
<td></td>
<td>Industry benchmarking</td>
</tr>
</tbody>
</table>


According to Wilson (2000:394), some banks split losses between high-frequency/low-impact and low-frequency/high-impact events. The high-impact events are usually the catastrophic ones. Few banks have much internal data on the latter. Therefore there is a need to use external as well as internal data. The types of data collected is divided by Wilson (2000:394) into four main sources, namely:
- Historical variances/loss events (past settlement losses from the back office).
- Supplier/vendor estimates.
- Industry benchmarking.
- Delphic techniques based upon business assessment.

According to Wilson (2000:394), the Delphic technique is the preferred method for the causal model, particularly when there is a general lack of data from the other three methods. The Delphic technique involves assembling a panel of experts in the bank and forcing them to look forward in time and to generate scenarios of what can go wrong in terms of causes, effects, magnitude and likelihood. A link between the qualitative and quantitative methods of measuring risk is subsequently made by forcing the senior executives to assign values to the scenarios.

Once enough data is available, the causal model approach models the cause/effect data and analyses the relationship between them. If the relationship has been determined in a Delphic workshop, using exception reporting of red, amber or green, it can, for example, incorporate risk visualisation. A frequency distribution of the events should be modeled which may eventually result in the measuring of the unexpected loss and subsequent allocation of risk capital to operational risk (Wilson 2000:395).

In summary, the FSA (1999:40) states that causal modeling for operational risk improves the understanding of the losses and provides a means for performing stress testing and simulations similar to the existing credit and market techniques.

*Risk Indicators.* According to PwC (1999:61), risk indicators are quantitative measures intended to provide insight to exposure to the effectiveness of
operational risk management and controls, for example, the number of failed trades or number and severity of errors and omissions. They may also include measures and metrics that are used to monitor the level of operational risk. The most common measures are listed by PwC in table 3.12.

Table 3.12: Common Measures

<table>
<thead>
<tr>
<th>Area</th>
<th>Head Office Measures</th>
<th>Business Unit Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>Temporary help</td>
<td>Temporary help</td>
</tr>
<tr>
<td></td>
<td>Turnover</td>
<td>Turnover</td>
</tr>
<tr>
<td></td>
<td>Tenure</td>
<td>Training budget versus actual</td>
</tr>
<tr>
<td></td>
<td>Management development versus plan</td>
<td>Vacation and absence</td>
</tr>
<tr>
<td>Business</td>
<td>Audit scoring</td>
<td>Audit score</td>
</tr>
<tr>
<td></td>
<td>Audit expectations</td>
<td>Customer satisfaction rating</td>
</tr>
<tr>
<td></td>
<td>Audit points outstanding</td>
<td>Audit points outstanding</td>
</tr>
<tr>
<td></td>
<td>Customer complaints</td>
<td>Customer complaints</td>
</tr>
<tr>
<td>IT</td>
<td>System downtime</td>
<td>System downtime</td>
</tr>
<tr>
<td></td>
<td>Number of system problems</td>
<td>Number of system problems</td>
</tr>
<tr>
<td>Operations</td>
<td>Physical losses</td>
<td>Settlement failures</td>
</tr>
<tr>
<td></td>
<td>Accounting losses</td>
<td>Accounting losses</td>
</tr>
<tr>
<td></td>
<td>Number of errors</td>
<td>Number of errors</td>
</tr>
<tr>
<td></td>
<td>Unreconciled accounts</td>
<td>Unreconciled accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluation losses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aged confirmations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Income statement adjustments</td>
</tr>
</tbody>
</table>

Source: PwC (1999:62)

The modern outlook is for organisations to develop “leading” indicators. These measures provide management with early warning signals of operational risk issues. Indicators are presented to management in various forms of management information. According to PwC (1999:64), these are often in the form of various stand-alone reports, usually on a monthly basis. Although the objectives of operational risk indicators are to support strategic decision-making, perform
trend analysis and support the goals of the operational risk management initiative, its real benefit is to provide predictive information to facilitate decision-making and enable preventative actions.

*Escalation Triggers.* Escalation triggers may be used as a basis to communicate potential problems to management. The starting point for escalation trigger points is a set of risk indicators with set goals or limits (primarily quantitative). When they reach the goal or limit, these indicators are highlighted and given to the predetermined appropriate business unit.

There are various strategies for setting escalation trigger points. Sometimes they are set very low and become a warning signal to the first level of management. Other times they are set at higher levels and therefore may have increased importance when reached. Currently, it seems that escalation triggers are set according to the individual manager's perception or past experience of an operational risk event (PwC 1999:66).

PwC (1999:66) states that while there are various ways to collect data for this tool, escalation trigger points are usually based on information contained in existing reports and systems. Business unit senior management and risk officers seem to be the predominant users of escalation triggers in their daily decision-making responsibilities. PwC (1999:67) also states that the effectiveness of escalation trigger points depends on the selection of the goals to highlight potential operational risk problems before they become an issue.

*Loss-Event Database.* PwC (1999:67) states that a loss event database captures and accumulates individual loss events across businesses and risk types. This information is comprehensive with no duplication. They (1999:67) also state that the loss event database model is the only tool that provides both financial and
quantitative measures of operational risk. The data, which can be applied consistently across the organisation, have according to PwC (1999:67) three potential applications, namely:

- **Empirical Analysis.** By studying what has happened, institutions can assess current policies and controls and gain comfort on their effectiveness. Collecting information and classifying it by risk, control point, or other factors, helps identify and focus resources on the key issues;

- **Quantifying the Loss from Operational Risk.** Accumulating the loss from incidents sets the value proposition for operational risk management. Losses are tracked and trends are determined to show the progress over time; and

- **Modeling of Operational Risk.** The raw data may be used to develop a predictive and causal model of risk and as input into the capital models. Management can also use the data to determine the most effective level of mitigation and investment.

Loss-event databases use organisations’ loss experiences as inputs. Events are described and stored in various locations for analysis. PwC (1999:67) states that in most cases, the data are based on the organisation’s loss experiences, but the inclusion of the external loss events of other institutions can enhance the analysis. Loss-event databases, however, have the following challenges, as listed by PwC (1999:70):

- Developing clear and consistent criteria for quantification to ensure that there is a standardised approach across all involved business units regarding the collection of data for a loss event database;
• Agreeing on the indirect data and quantifying the consequences. When quantifying the losses, companies may incur various types of costs. While the primary cost is the direct financial impact, there is less agreement on how to quantify other more subtle secondary impacts. Some institutions try to quantify the cost of business interruption or lost earnings, while most institutions simply consider it too subjective and ignore it, hence the necessity to agree on the indirect data and the quantifying of the consequences; and

• Determining accountability for identifying and describing events throughout the organisation. The collection and preparation of the information for the loss database should be a responsibility of the finance or controllers unit. Internal audit and the front- and back-office or operations should be the providers of information to the loss-event database. The head of operational risk should be responsible for the design of the database and its quality control.

3.3.2. Conclusion

Although there are various approaches and methodologies to evaluate and measure operational risk, the limitations of each should be taken into account when applied. No risk manager, however, should rely on a single aggregate measure as a basis for understanding the full extent of a firm’s exposure to operational risk. Donahoe (1998:102) also states that even where it is possible to quantify operational risk, a single number can never give the whole picture. The challenge is to standardise the risk management measurements and supplement the numbers with written commentary. Snapshots of data are insufficient by themselves. Rather, average numbers, highs and lows in a given period and other types of trend analysis are necessary.
PwC (1999:71) states that while each operational risk measurement tool is valuable, no one tool is sufficient to support a comprehensive operational risk initiative. In this regard, they outline the applications and limitations of each tool as depicted in table 3.13.

Table 3.13: Applications and Limitations of Each Tool

<table>
<thead>
<tr>
<th>Tool</th>
<th>Applications</th>
<th>Limitations</th>
</tr>
</thead>
</table>
| Self-risk assessment| - Reinforce responsibility with business units  
                        - Gain agreement on the operational risks and required next steps  
                        - Bring together independent views                                   | - Depends on method employed (some are more robust than others and may provide greater insights and buy-in)  
                        - Some alternatives may be time consuming  
                        - Primarily qualitative                                                    |
| Risk maps/process flows| - Detail understanding of operations and the specific operational risk activities | - Tool for lower level staff use – too detailed for senior management  
                        - Limited value to senior management  
                        - Difficult to maintain current  
                        - Primarily quantitative                                                     |
| Risk indicators     | - Measure effectiveness in operational risk management  
                        - Objective, quantitative  
                        - As often as daily updates                                                | - Risk/indicator correlation is unproven  
                        - Some operational risks difficult to measure  
                        - Uncertainty if the right measures are being used or just the measures where data are available |
| Escalation triggers | - Predetermine decision or intervention point for management                | - Depends on the quality of the target setting and the risk indicators used |
| Loss-event database | - Provides financial-based measures  
                        - Tool for empirical analysis  
                        - Tool for risk modeling and support for cost/benefit analysis          | - Data difficult to collect on a Consistent basis                           |

Source: PwC (1999:71)
The FSA (1999:28) states that operational risk should be forward and outward looking and not just focus internally on the organisation. The more banks and their stake-holding partners, be they customers, suppliers or venture partners, interact more openly and accessibly, the more operational risk management will need to consider the entire business or value chain.

The FSA (1999:28) also states that in future the value chain for financial services is likely to transcend several types of organisations. It will, therefore, be imperative to identify who in the value chain is running what operational risks. This means two things:

- As a close relationship exists between risk management and reward allocation, operational risk management has a vital role in helping financial institutions to understand how and where to create value through the superior understanding of risk.
- Banks and regulators will need to collaborate to ensure a level playing field for banks and other non-regulated organisations for when any changes in operational risk are viewed or considered for capital allocation purposes.

The methods applied may also differ from bank to bank, depending on the bank’s business strategy and developments. It is evident that the methods used to assess operational risk should be applied consistently and should be suitable to effectively determine the risk exposures of the underlying operational risk factors. This will enhance the efforts of management to control the relevant risks and serve as a basis for models which may be used to determine the allocation of capital according to the level of operational risk. This issue will be dealt with further in the section on capital adequacy.
The next step in the management of operational risk is the control of the identified risks. This issue will be dealt with in the ensuing section.

3.4. Control of Operational Risk

Risk control entails any activity that is aimed at preventing losses, minimising the consequences of losses that may arise from all risks facing the organisation and dealing with an adverse event in advance or as it occurs.

The FSA (1999:14) states that it is essential for a bank to have two types of controls in place in order to mitigate operational risk, namely preventative controls and contingency or damage limitation controls (for example, insurance). It is also important to distinguish between the sub-risks for each main underlying risk factor of operational risk in order to match the relevant mitigating controls to it. The FSA mapped the risks and their mitigating controls in table 3.14.

Table 3.14: Operational Risks Mapped to Mitigating Factors

<table>
<thead>
<tr>
<th>Primary Source of Operational Risk</th>
<th>Mitigating Systems and Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inexperienced, incompetent, unsuitable, negligent and/or maverick staff</td>
<td>Recruitment procedures, job descriptions, training programmes, disciplinary and appraisal procedures. Compliance at an individual level through training and information. Compliance checks. Active management.</td>
</tr>
<tr>
<td>Human error</td>
<td>Checking procedures, segregation of duties and IT systems.</td>
</tr>
<tr>
<td>Working culture creating low morale, high staff turnover, poor concentration, low productivity and industrial action</td>
<td>Competitive pay regime, performance-related pay, career planning, responsive management, line of communication, working environment, disciplinary and appraisal procedures.</td>
</tr>
<tr>
<td>Fraud and theft</td>
<td>Segregation of duties, compliance culture, checking procedures and reporting lines. IT and physical security. Supportive culture. Good pay structure with reduced emphasis on performance related pay. Recruitment procedures and holiday policy. Regular internal audits. Insurance.</td>
</tr>
<tr>
<td>Unauthorised and/or ill-informed decision making at all levels, particularly with regard to business strategy</td>
<td>Lines of authority, reporting lines. Breach procedures. Research and market information from IT systems, the internet and up to date libraries. Consultation at all levels with both internal and external experts. Project management. Decisions ratified at</td>
</tr>
<tr>
<td>Issue</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Errors in information systems</td>
<td>Up-to-date, virus and error free technology. Detection systems and limited access for personnel. Regular back-ups and protected records. Manual copies of essential information. Consulting from internal and external experts to ensure that suitable software packages are used. Training at all levels.</td>
</tr>
<tr>
<td>System infiltration</td>
<td>Firewalls and regularly altered access codes. Error-free software. Consultation from internal and external experts. Daily account reconciliation and other detection methods.</td>
</tr>
<tr>
<td>External criminal activities</td>
<td>Damage-proof buildings, security systems, emergency procedures and training. Ethical or non-political business strategies. Insurance.</td>
</tr>
<tr>
<td>Domestic political upheaval</td>
<td>Contingency planning.</td>
</tr>
<tr>
<td>Regulatory, legal, tax and business environment</td>
<td>Contingency planning, business strategy, internal experts and competent external advisors. Flexibility, research, preparation and diversification.</td>
</tr>
<tr>
<td>Third parties</td>
<td>Monitoring, reporting lines and regular reviews of contracts. Legal protection. Business and contingency planning. Market research.</td>
</tr>
<tr>
<td>Reputational deterioration</td>
<td>Strong individual reputation to protect in event of sectoral deterioration. Contingency planning and business strategy. Market awareness.</td>
</tr>
</tbody>
</table>

Source: FSA (1999:22)

According to Valsamakis et al. (2000:107), all risk control activities are directed towards minimising losses. They categorise these activities as follows:

- Activities aimed towards controlling the possible adverse occurrence of an event and then endeavoring to eliminate it; and
- Activities directed towards minimising the loss after it occurred (for example, loss control activities).

Risk control programmes should be supported by fundamental principles of risk control, which is briefly described by Valsamakis et al. (2000:114) as follows:

- The identification and application of management principles to risk control;
• The recognition that risk exposures and their associated losses should be deliberately assessed;
• The meaningful endeavor of loss prevention, recognising the impact of losses on the pace of technological development; and
• The recognition that approaches to risk control must be integrated with other activities within the organisation, thereby acknowledging the existing interrelationships.

Valsamakis et al. (2000:114) also state that the objectives of a risk control programme may be described as follows:

• *The reduction of the magnitude of the losses.* This entails the careful assessment of the magnitude of exposure *per se* with the quantum of the exposure; and
• *The reduction of the frequency of loss-producing events.* The possibility of reducing the frequency of loss-producing events exists independently from reducing the magnitude of an exposure or loss. This entails a critical analysis of the causes of loss, followed by implementation of plans and procedures to eliminate these causes.

According to Kingsley et al. (1998:6), the objectives of an operational risk management function are the following:

• To avoid potential catastrophic losses;
• To generate a broader understanding of operational risk issues at all levels of the firm that touch on key areas of risk;
• To enable the organisation to anticipate risks more effectively;
• To provide objective measurements of performance;
To change behavior in order to reduce operational risk and to enhance the culture of control within the organisation;

To provide objective information so that services offered by the organisation takes account of operational risks; and

To provide support in ensuring that adequate due diligence is shown when carrying out mergers and acquisitions.

Donahoe (1998:106) states that control will never be “airtight” or anticipate every possible situation. There are some characteristics of good controls, however, which may be implemented. These are depicted in table 3.15.

Table 3.15: Characteristics of Effective Controls

<table>
<thead>
<tr>
<th>Kinds of controls a firm might implement:</th>
<th>Whichever type is used:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Preventative controls</td>
<td>- Good controls are logical, sequenced, intuitive, focused and verifiable</td>
</tr>
<tr>
<td>- Managerial controls</td>
<td>- Controls should complement the business and should be part of the operational process. They should be appropriate both to the industry and to the company’s internal processes and should incorporate its risk philosophy and reflect its culture and history.</td>
</tr>
<tr>
<td>- Advisory controls</td>
<td>- Controls need to be arranged in a hierarchical and a logical sequence.</td>
</tr>
<tr>
<td>- Escalation controls</td>
<td>- Controls are only effective if timely and accurate information is available and if they are reviewed and acted on.</td>
</tr>
</tbody>
</table>

Source: Donahoe (1998:106)
According to Rachlin (1998:119), a bank should consider the following alternatives with regard to the control of risks (see figure 3.11):

- Put controls in place to limit the possibility of the risk arising;
- Accept the costs of the risk becoming an event as part of the cost of the business;
- Transfer the risk using insurance or other mechanisms; or
- Avoid the business altogether if the cost is too high.

**Figure 3.11: Key Risk Mitigating Decisions**

![Diagram showing four quadrants: Transfer, Avoid, Accept, Control, with Impact and Probability axes]


The tactics adopted will usually depend on the likelihood and effect of the risk occurring.
According to Rachlin (1998:119), the practices available to management to mitigate risks, together with tools that may assist with this, may be divided into three categories as described in table 3.16. In practice, risk mitigation is likely to be a combination of all three categories described in table 3.16.

**Table 3.16: Risk Mitigation Practices and Tools**

<table>
<thead>
<tr>
<th>Practice</th>
<th>Details</th>
<th>Possible tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk reduction</strong></td>
<td>The first steps management should take are to reduce the risks inherent in products and processes. Therefore, bank products and processes should be developed or re-engineered to minimise inherent operational risk.</td>
<td>A product design process that incorporates a formal risk assessment phase. A formal new product approval process where independent technical experts on operational risk areas review new products and approve their implementation.</td>
</tr>
<tr>
<td><strong>Risk control</strong></td>
<td>Appropriate preventative controls (those designed to minimise an operational risk event occurring such as firewalls, passwords and authorisation processes) and detective controls (those designed to highlight that an event has occurred as soon as possible, such as reconciliation) will need to be built around the key risk areas.</td>
<td>Minimum control standards. Internal audit recommendations. Risk control checklists.</td>
</tr>
<tr>
<td><strong>Risk containment</strong></td>
<td>There will generally be at least some residual risk remaining, both in terms of risks without controls and the possibility of control failures. It is important that some form of risk containment is considered.</td>
<td>Insurance. Business continuity plans. Computer disaster recovery procedures. Hot or cold back-up sites.</td>
</tr>
</tbody>
</table>

Source: Rachlin (1998:120)

The nature of the combination will, according to Rachlin (1998:119), depend on the company's philosophy – whether it's a risk adverse, risk neutral or risk-taking type of organisation. It will also depend upon an analysis of both the costs
of putting the control in place and any benefits that may accrue in terms of a reduction in operational risk losses. Rachlin illustrates the operational risk management practices in the diagram depicted in figure 3.12.

**Figure 3.12: Operational Risk Management Practices**

![Diagram showing operational risk management practices](image)

Source: Rachlin (1998:120)

According to Schwartz and Smith (1997:360), the establishing of appropriate policies, methodologies and infrastructure, as illustrated in figure 3.13, are the "necessary" three pillars for building a first-class risk management function. The methodologies refer to applying the appropriate analytical models to measure operational risk, while policies spell out the risk control structures designed to
ensure existence, completeness and accuracy for all transactions via appropriate segregation of duties. Schwartz and Smith (1997:366) also state that there must be an infrastructure in place to make policies and methodologies work. The first and most important component of an infrastructure is people. People are needed to make decisions and provide significant input.

Figure 3.13: Three Pillars

![Diagram of Three Pillars]

Source: Schwartz & Smith (1997:360)

Mark (1997:146) states that the appropriate policies, methodologies and infrastructure are the necessary three legs (pillars) for building a first-class risk management function. The function, however, is only as strong as its weakest leg. Obtaining management commitment to building a first-class risk management function provides the “sufficient condition” for success. Clearly, a first-class risk management function should be capable of creating the necessary tools to manage and control risk.
As operational risk exists throughout the organisation and may occur before, during and after the completion of a business transaction, it should be a requirement that all risk-taking authorities include a full review of operational risk. An operational risk policy, for example, should be in place to serve as a guideline regarding the organisation’s attitude towards operational risk.

3.4.1. Operational Risk Policy

According to the FMAC (1999:27), an organisation’s risk management policy statement defines its approach to risk management and its attitude to, and appetite for, risk. The policy also defines overall responsibility for the policy, for risk review as well as for reporting requirements. This policy should be adopted by management and endorsed by the board of directors.

Venkat (2000:599) states that risk management policies and procedures must be developed using a top-down approach to ensure that they are consistent with one another and appropriately reflect the strategic objectives and the overall risk appetite of the institution. This means that corporate risk management policies and procedures must be endorsed by senior management who should actively work towards influencing them into the culture of the organisation. Risk management policies and procedures provide detailed guidance on an organisation’s risk management approach. They should clearly communicate how the risk management infrastructure will work on a daily basis and the roles, responsibilities and accountabilities of different personnel with respect to risk management. Schwartz and Smith (1997:363) state that The Bank of England’s report on the Barings Bank revealed some general operational risk lessons, namely:
• Management teams have the duty to fully understand the business they manage;
• Responsibility for each business activity has to be clearly established and communicated;
• Relevant internal controls must be established for all business activities;
• Top management and the audit committee must ensure that significant weaknesses are revealed quickly;
• Senior management needs to ensure that policies are established to ensure transparency in their dealing operations; and
• An internal risk control structure should be designed to ensure existence, completeness and accuracy for all transactions via appropriate segregation of duties.

Carr and Walsh (1999:48) state that a corporation must establish integrated risk management policies and practices consistent with its mission, culture and management philosophy. These policies should identify the organisation's exposures and how to manage them within the context of the organisation's strategic plan. According to Carr and Walsh (1999:49), these policies should spell out the following:

• The corporate philosophy on risk management;
• The objectives of the risk management policy;
• The delegation of responsibility; and
• The authorised methodology, including systems, for measuring risk, limiting risk taking, applying independent internal controls and generating comprehensive, timely and independent risk reports.
Goldman *et al.* (1998:41) emphasise the fact that in order to be effective, a risk management system has to be based on a set of written risk policies and procedures that are endorsed by the board of directors and implemented by the senior management of the bank. Donahoe (1998:106) also confirms the aforementioned by stating that written risk policies must be clear and well disseminated throughout the organisation. The bank, therefore, not only has to ensure that the policies are disseminated to the staff involved, but they also understand it.

To ensure that all policy directives are carried out on a daily basis, complete and thorough operation procedures should be documented and communicated to the appropriate staff. The procedures should, for example, include controls for transaction initiation and capture, confirmation, settlements, accounting, valuation and safekeeping, as well as cash flow management. The procedures should also specify the hierarchy and frequency of management reporting, as well as sign-off authorities. The principle of segregation of duties should underlie all of the procedures (Carr & Walsh 1999:49).

According to the Basel Committee (1998a:16), it is not sufficient for senior management to simply establish appropriate policies and procedures for the various activities and divisions of the bank. They must regularly ensure that all areas of the bank are in compliance with such policies and procedures and also determine that existing policies and procedures remain adequate and relevant.

According to the FMAC (1999:41), operational risk management policies are a formal communication to the entire organisation about the company’s approach to operational risk management. Policies typically include a definition of operational risk; the organisational approach and related roles and responsibilities; key principles for management; and a high-level discussion of
information and related technology. Freeman (1999:15) once again emphasises that the organisational structure cannot work unless it has proper policies, standards and controls built into the system. These must be clear, measurable and enforceable.

Carr and Walsh (1999:50) state that risk management policies should identify the internal management controls required to monitor the organisation’s risks. This will be addressed in the ensuing section.

3.4.2. Internal Controls

According to Schwartz and Smith (1997:43), internal controls are usually divided into primary and secondary controls. Primary controls prevent a mistake from occurring and secondary controls act as a safety net by identifying potential results. Controls, such as the separation of trading and operations responsibilities, are provided by the structure of an organisation itself, while others are contained in the operating procedures of the institution. They (1997:43) also describe the following examples of controls:

- *Separation of Function.* The delineation of responsibilities is designed to provide an institutionalised primary control mechanism. Checks and balances are provided by forced separation of function. Those individuals responsible for committing an institution to a transaction, for example, should not also perform clearance or accounting functions. According to the Basel Committee (1998a:28) the segregation of duties is not limited to situations involving simultaneous front and back office control by one individual, it can also result in serious problems when an individual has the responsibility for the following:
• approval of the disbursement of funds and the actual disbursement;
• customer and proprietary accounts;
• transactions in both the "banking" and "trading" books;
• informally providing information to customers about their positions while marketing to the same customers;
• assessing the adequacy of loan documentation and monitoring the borrower after loan origination; and
• any other area where significant conflicts of interest emerge and are not mitigated by other factors.

Katz (1995:28) states that the segregation of duties should typically separate activities such as the:
• custody and recording of assets;
• processing of a transaction and the accounting; and
• execution and authorisation of a transaction and processing of settlement funds.

Any inappropriate circumstances, if discovered, should be brought to the attention of senior management, who must take corrective action.

• **Dual Entry.** Another of the important primary operational controls is the double checking work. Some organisations go so far as to have duplicate staff for each function, such as an input clerk and a verifier. Other organisations use the hierarchy system of a supervisor who signs off all parts of the process activities.

• **Reconciliation.** Comparing the output of various systems or reports is a strong secondary control. Reconciliation highlights, for example, potential failures in primary controls or systems.

Crouhy *et al.* (1998:46) noted a variety of techniques which are used to control or mitigate operational risk. They (1998:46) state that most banks noted that internal
controls are seen as the major tool for managing operational risk. Banks also cited insurance as an important mitigator for some forms of operational risk. Several banks have established a provision for operational losses similar to traditional loan loss reserves. Banks are also exploring the use of reinsurance to cover operational losses. This issue will be discussed in the section on operational risk finance.

The Basel Committee (1998a:6) came to the same conclusion as Crouhy et al. (earlier in this section) that most banks viewed internal controls as the major tool for managing operational risk. These controls include components such as segregation of duties, clear management reporting lines and adequate operating procedures. Many banks expect most operational risk events to be associated with internal control weaknesses or lack of compliance with existing internal control procedures. According to KPMG (1999:3), sound internal controls are not only important but also crucial to the success of banks. The Basel Committee has identified five types of control breakdowns, which have led to recent large losses at banks. These are summarised by KPMG (1999:3) as follows:

- Lack of adequate management supervision and accountability and failure to develop a strong culture within the bank;
- Inadequate assessment of the risk of certain banking activities, whether on- or off-balance sheet;
- The absence or failure of key control activities, such as segregation of duties, approvals, verifications, reconciliation and reviews of operating performance;
- Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems; and
- Inadequate or ineffective audit programmes and other monitoring activities.

The Basel Committee also focused on principles of internal controls and stressed the importance of having bank directors; bank management; internal and external auditors; and bank supervisors who should pay considerable attention to strengthening internal control systems; and continually evaluating its effectiveness.

The Basel Committee identified thirteen main principles of internal controls for banks, which KPMG (1999:4) summarised as follows:

- Management supervision and the control culture.
  1. The board of directors should have responsibility for understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks.
  2. Senior management should have responsibility for implementing strategies and policies approved by the board; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.
  3. The board of directors and senior management is responsible for promoting high ethical and integrity standards and for establishing a culture within the
organisation that emphasises the importance of internal controls. All personnel at a banking organisation need to be fully engaged in the internal control process.

- **Risk assessment**
  4. All material risks that could adversely affect the achievement of the bank’s goals should be recognised and continually assessed.

- **Control activities**
  5. Control activities should be an integral part of the daily activities of a bank. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and a system of verification and reconciliation.
  6. There should be appropriate segregation of duties.

- **Information and communication**
  7. There should be comprehensive financial, operational and compliance data. Information should be reliable, timely, accessible and provided in a consistent manner.
  8. Reliable information systems should be in place.
  9. There should be effective channels of communication to ensure that information is reaching the appropriate personnel.

- **Monitoring activities**
  10. Monitoring of internal controls should be on an ongoing basis and a part of the daily activities of a bank.
  11. There should be an effective and comprehensive internal audit of the internal control system carried out by
operationally independent staff. The internal audit function should report directly to the board of directors or its audit committee and to senior management.

12. Internal control deficiencies should be reported in a timely manner to the appropriate management level and addressed promptly.

- Evaluation of internal control systems by supervisory authorities

13. Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity, and risk inherent in their activities and that responds to changes in the bank’s environment and conditions.

The first few principles state quite clearly that a bank’s board of directors and senior management are mainly responsible for controls and not just its internal audit and compliance departments. Apart from the board of directors’ responsibilities, however, it is evident that everyone in the bank shares these responsibilities to some extent. According to the Basel Committee (1998a:16), control activities are most effective when management and all other personnel view them as an integral part of, rather than an addition to the daily activities of the bank. When controls are viewed as an addition to the day-to-day activities, they are often seen as less important and may not be performed in situations where individuals feel pressured to complete activities in a limited amount of time. In addition, controls that are an integral part of the daily activities enable quick responses to changing conditions and avoid unnecessary costs. As part of fostering the appropriate control culture within the bank, senior management should ensure that adequate control activities are an integral part of the daily functions of all relevant personnel on all levels. KPMG (1999:5) emphasises that risk control is an ongoing process. The objectives are to ensure that risks are
continually re-evaluated and all areas continually comply with established policies and procedures.

The new environment of proactive regulatory supervision makes it crucial that banks have an in-depth, comprehensive programme of internal controls and compliance procedures.

3.4.3. **Risk Reporting**

Carr and Walsh (1999:49) state that risk management systems should provide accurate and timely information to risk managers, as well as consolidated reports regarding risk exposures. The FMAC (1999:37) states that risk management reporting outputs should be carefully tuned to the needs of the various uses of risk information. The information must be concise, unambiguous, standardised and integrated with existing reporting processes. According to The Comptroller (1994:36), however, operational errors may affect the accuracy of management reports and risk measurement systems, jeopardising the quality of management decisions. It is evident that risk reporting should be accurate and concise in order not to compromise the quality of management decisions.

Goldman *et al.* (1998:42) state that risk reporting is the process through which an organisation reports on risk through its management information systems to its internal shareholders and regulators. It is an increasingly important part of the risk management process as organisations seek ways to improve their ability to measure their performance and return on equity on a risk-adjusted basis. According to Goldman *et al.* (1998:42), there have been a number of initiatives by banking and security regulators to encourage improved regulatory reporting and risk disclosure in annual reports.
According to a survey by PwC (1999:84), it is widely recognised that current reporting needs to be improved. The survey indicates that the primary area of improvement is in strengthening the link between business strategy and operational risk reporting. Instead of being a stand-alone process, operational risk needs to become an element of the strategy. In addition, senior management reporting must include more robust risk measures and follow-up action items to improve operational risk management results.

Venkat (2000:609) concludes that an effective risk-reporting framework focuses on the generation of risk management information that meets the objectives and needs of different target audiences, including:

- Business, trading and risk managers;
- Senior and executive management; and
- Potential users such as financial controllers, middle and back office operations as well as auditors and regulators.

Figure 3.14 depicts a risk-reporting framework that may be delivered to different target audiences.

Venkat (2000:609), furthermore, mentions a word of caution when taking the best-practice approach to implementing a risk-reporting framework. It requires striking a medium between an organisation’s ultimate risk measurement and reporting goals and its current capabilities. A pragmatic first step would entail developing initial reports that appropriately capture the risk profiles of different businesses. The next step would be to design risk reports that balance “ideal” information content with current data availability and report generation capabilities. This, in turn, will highlight gaps in the current risk reporting
environment with respect to risk management information and serve as the basis for developing an action plan to address these gaps.

**Figure 3.14: Risk-Reporting Framework**

<table>
<thead>
<tr>
<th>Daily risk summaries</th>
<th>Monthly risk packages</th>
<th>Quarterly risk package</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Objectives:</strong></td>
<td><strong>Key Objectives:</strong></td>
<td><strong>Key Objectives:</strong></td>
</tr>
<tr>
<td>Identify key issues</td>
<td>Reaffirm risk appetite</td>
<td>Promote shareholder</td>
</tr>
<tr>
<td>that require immediate attention and potential management action by reviewing:</td>
<td>propositions and boundaries by assessing:</td>
<td>value creation by evaluating:</td>
</tr>
<tr>
<td>- limit excesses;</td>
<td>- risk profile;</td>
<td>- capital/resource</td>
</tr>
<tr>
<td>- risk concentration;</td>
<td>- performance; and</td>
<td>allocation decisions;</td>
</tr>
<tr>
<td>- income statement</td>
<td>- internal and external</td>
<td>- earnings reliability and</td>
</tr>
<tr>
<td>changes; and</td>
<td>business environment and</td>
<td>sustainability; and</td>
</tr>
<tr>
<td>- risk events.</td>
<td>risk implications.</td>
<td>- short and long term</td>
</tr>
<tr>
<td><strong>Target Audience:</strong></td>
<td></td>
<td>business opportunities</td>
</tr>
<tr>
<td>Business, trading and risk managers.</td>
<td></td>
<td>and their risks.</td>
</tr>
<tr>
<td><strong>Contents:</strong></td>
<td><strong>Contents:</strong></td>
<td><strong>Contents:</strong></td>
</tr>
<tr>
<td>Detailed market risk, and</td>
<td>Summary market risk,</td>
<td>Executive management.</td>
</tr>
<tr>
<td>Selected credit, liquidity, and</td>
<td>Detailed credit, liquidity, and</td>
<td><strong>Contents:</strong></td>
</tr>
<tr>
<td>operational risk metrics and</td>
<td>operational risk.</td>
<td>Summary of all business and</td>
</tr>
<tr>
<td>issues.</td>
<td>Trend analysis.</td>
<td>customer risks.</td>
</tr>
<tr>
<td><strong>Scope:</strong></td>
<td><strong>Scope:</strong></td>
<td><strong>Scope:</strong></td>
</tr>
<tr>
<td></td>
<td>Business units globally.</td>
<td></td>
</tr>
</tbody>
</table>

Source: Venkat (2000:610)

It is evident that risk reporting plays an important role in a bank's operational risk management process. It seems imperative, however, that the reports should include accurate information to ensure that management may make correct decisions based on information regarding the management of operational risk.
Kingsley et al. (1998:11) state that if the operational risk management function is to be effective, it needs to act within agreed operating principles. These principles should be aligned with the operating principles of the rest of the risk management function. According to Kingsley et al. (1998:11), these could include the following:

- **Definition of data requirements.** Operational risk management is responsible for defining and communicating its data requirements to the business units and support functions.

- **Responsibility for data capture and integrity.** The business units and support functions are responsible for ensuring the completeness and integrity of data reported to risk management. Risk management, meanwhile, is responsible for exercising the secondary independent detective and diagnostic controls over data integrity.

- **Reporting of operational risk.** Operational risk information would typically be reported weekly in summary form and in greater detail on a monthly basis. The format of the reports should be aligned with the existing risk management information.

- **Scheduling of formal operational risk committee meetings.** This will depend on the type of organisation. With the rate of market change and the need for proactive action, it is likely that meetings will be at least monthly. *Ad hoc* meetings may also be necessary in times of market turbulence.

- **Members of the operational risk committee.** A board member should be assigned responsibility for the operational risk function. The Committee members should include the most senior levels of management.
• **Empowerment.** The powers of the operational risk function should be documented and known throughout the organisation. The operational risk function should have the capacity to exercise those powers, particularly the power to reduce unauthorised levels of risk where line management has failed to do so.

It is furthermore clear that operational risk reporting needs quality information on operational risk. Hoffman (1998:39) states that much value may be gained in the decision-making process by simply reporting on areas including, but not limited to, for example, the following:

• Losses and loss-cause analysis;
• Linking analysis to outstanding control issue tracking;
• Specific risk indicators (such as compilation of extensive processing technology or other risk class data);
• Identification of candidates for accountability;
• Risk factor **comparative and trend analysis**; and
• Risk finance and insurance coverage alignment (for example, cost of risk analysis).

Mark (1997:169) states that there is a need to ensure that the necessary information associated with operational risk is transported from the operational environment (which include infrastructure, corporate governance and business units) to the risk management function (see figure 3.15). Risk management needs to generate the necessary organisation-wide and regulatory risk reports as well as work with auditing so that the audit function may exercise its responsibilities. A partnership is required to implement an operational risk policy successfully. The business unit, for example, should implement policy, run the business and manage the operational risks together with its business infrastructure group.
Corporate governance needs to participate in utilising the operational risk metrics in its reporting process. Internal audit should report on efficiency as well as comment on controls. Risk management also needs to integrate operational risk measurement into Risk-adjusted-return-on-capital (RAROC), perform residual risk management (for example, utilising insurance tools) and provide leadership in business recovery planning.

**Figure 3.15: Risk Information Flow**

![Risk Information Flow Diagram]

Source: Mark (1997:169)

Davies *et al.* (1998:68) state that when there is a failure in integrating data, a key control indicator (KCI) will show that this has occurred. The next step is to translate this failure into monetary terms. This is achieved by examining the actual losses that are incurred through operational risk. These measured losses may be classified under four categories, namely:

- Interest claims and fines;
- Operations write-offs;
- Cost of correction; and
- Profit-and-loss adjustments.

This information along with the KCI information is subsequently fed into the operational risk reporting structure (see figure 3.16). Using this structure, an error may be theoretically traced from a loss event (cause of a loss) to the eventual cost to the bank of the error/loss (such as an interest claim).

**Figure 3.16: Operational Risk Reporting Structure**

Source: Davies et al. (1998:69)

Finally, Davies et al. (1998:71) list the following requirements for the control and mitigation of operational risk:
• Clear standards across both core production functions and product support functions. Global best practices across business processes and global standards for control programme management;
• Clear definition of key control indicators. Transparency of control information across all major locations may be gained through the implementation of a standard control reporting process;
• A standard control tool set is important to manage multiple systems and a high level of data movement; and
• Clarity of responsibility, both within operations and between operations and other functions. Lack of clarity of responsibility always significantly increases the level of operational risk.

It is evident that clear roles and responsibilities should be established to ensure the effective management of operational risk. As such, the next section will address the organisational structure as the basis for determining the roles and responsibilities as it relates to operational risk management.

3.4.4. Organisational Structure, Roles and Responsibilities

One of the primary elements of control lies in the organisation itself as it will indicate the different role players and their involvement in the management of operational risk. Morgan and Andersen (1997:66) state that the foundation for an effective risk control environment is an organisation structure that provides, for example, adequate supervision of risk management activities.

According to Rachlin (1998:126), a control team of specialists, such as a group risk function, might help a bank to improve its operational risk management, apart from strengthening its control environment. He (1998:126) also states that
in order to be effective a central risk function or other specialist team need to take cognisance of the prerequisites illustrated in figure 3.17.

Figure 3.17: Prerequisites when Establishing a Central Operational Risk Unit

Source: Adapted from Rachlin (1998:126)

- **Competency.** Any central team of experts needs to have the skills to be able to help the business units master specific aspects of operational risk. These skills include technical expertise such as understanding processes, systems and human resources.

- **Authority.** Any central risk function should have the explicit authority of the board and be seen to have this authority either through policies or communications.

- **Acceptance.** Management, staff and the board must accept that the unit can add value during the control of operational risk. Without this, the unit is unlikely to be invited by the business areas to participate in decisions at an early stage and will need to rely on policies to influence decisions.
According to the Standard Bank's Annual Report (1999:47), managing risk is an integral part of the business. Comprehensive risk management policies and processes need to be developed and implemented to control and monitor risk throughout the bank. These practices rely on regular supervision by the independent group risk function, senior management and the board sub-committees as depicted in figure 3.18.

**Figure 3.18: Structure of a Group Risk Management Function**

![Diagram of Group Risk Management Structure]

According to a study by PwC (2000:38), during the past three years senior management has taken a more active role and demonstrated interest in operational risk for the following reasons:

- Senior management commitment;
- Perceived increase in operational risk;
- Reaction to major loss events that have occurred internally and to others;
- Focus on enterprise-wide risk management; and
- Regulatory attention.

Firms are restructuring their organisational structures to include operational risk. An example of such a structure for operational risk management is identified by PwC illustrated in figure 3.19.

Figure 3.19: Corporate Operational Risk Organisational Model

Source: PwC (2000:40)
According to Bryn and Grimwade (1999:20), establishing these formal organisational structures tends to follow a common development path. It starts with the application of resources to specific operational risk management initiatives, moves on to the deployment of dedicated operational risk management resources with permanent responsibilities, and the implementation of a target organisational model. This extends across the group and involves dedicated resources closely aligned with the business. Wemple (1992:57) states that all firms should develop an overall risk strategy that incorporates a well-defined structure of responsibilities.

The FMAC (1999:34) states that risk management is the responsibility of all levels of management including:

- Board of directors;
- Executive committee;
- Business unit general managers;
- Functional experts and specialists;
- Line management; and
- Key supervisors and staff.

Another organisational model for a risk management function, as presented by the FMAC (1999:34), consists of the following levels:

- **Board of Directors.** The board of directors should ensure that appropriate corporate governance frameworks are established and operating. A risk management committee may review and endorse risk management policies and strategies and provide the organisation with a clear focus on the management of risk.
- **Risk Management Group.** This group should be responsible for setting group policy and strategies and should perform a monitoring role. Risk management should be made accountable at all levels throughout the organisation and should avoid risk management becoming only a corporate responsibility. The roles and responsibilities of a risk management group should include the following:
  - To be the primary advocate for risk management at the strategic and operational levels of the organisation;
  - To provide policy, framework and methodologies to business units to identify, analyse and manage their risks more effectively to achieve objectives;
  - To develop risk response processes to assist appropriate type and level of response required and assess the adequacy of the responses;
  - To facilitate, challenge and drive risk management;
  - To provide assurance that risk management policy and strategy set by the board of directors is operating effectively to achieve the group’s business objectives;
  - To report to the board on risk management;
  - To ensure the availability of risk management skills and experience; and
  - To collate risk management information.

Holliwell (1997:7) adds that senior risk management is ultimately responsible for controlling operational risk and they should be prepared to ask questions even when they fear exposing ignorance.

- **Business Units.** Business unit managers should be responsible for risk management within their units. They are normally charged
with creating a risk awareness culture, where each employee is accountable for managing risk. Included in these responsibilities are specific risk management obligations and performance measures which focus line management’s and functional specialists’ attention on the risk management strategy and objectives. To this end, management is accountable for the implementation, operation and reporting of group risk management policies and strategies.

Bryn and Grimwade (1999:19) also state that while there is no single organisational model for dedicated operational risk management resources, there are some key principles to guide institutions. To manage operational risk more effectively, banks have created separate operational risk units, altered their committee structures and mandates and expanded the responsibilities of business units. This has led to widespread debate on issues such as the differentiation between operational risk and internal audit as well as their functions. Ong (1998:4) states that operational risk should be managed collaboratively by the different business units, corporate governance, internal and external audit, as well as risk management units. As such, the roles and responsibilities of the various role players/areas should be clearly defined.

According to Bryn and Grimwade (1999:19), responsibilities provide a greater focus on the activities of the dedicated resources. Many banks have a single board member responsible for operational risk who is actively involved in approving policy statements, communicating the bank’s risk management approach and sponsoring key projects and initiatives. Crouhy and Mark (2000:347) state that proper risk management requires that appropriate policies be in place which limit the amount of risk taken; that authority be provided to change the risk profile to those who can take action; and that timely and effective
monitoring of the risk is in place. No one group can be responsible for setting policies, taking action and monitoring the risk taken as this would result in conflicts of interest. Thus, policy should be the responsibility of senior management, even though the development of those policies may be delegated and submitted to the board of directors for approval.

According to Crouhy and Mark (2000:347), the authority to take action rests with business management, who is responsible for controlling the amount of operational risk within the business. Business management often relies on expert areas such as information technology, operations and legal to supply it with services to operate the business (refer to figure 3.20). These infrastructure and governance groups share with business management the responsibility for managing operational risk.

**Figure 3.20: Managing Operational Risk**

Source: Crouhy & Mark (2000:347)
Senior management needs to know if the delegated responsibilities are actually being followed and if the resulting processes are effective. Internal audit is usually charged with this responsibility. According to Crouhy and Mark (2000:348), Audit determines the effectiveness and integrity of the controls that business management puts in place to keep risk within tolerable levels.

Bryn and Grimwade (1999:19) also state that many banks have established committees with specific mandates for operational risk at corporate or business levels, although they are still at an embryonic stage. On a corporate level these are either stand-alone committees, that focus solely on operational risk, or integrated risk management committees, that look at market, credit and operational risks. They (1999:20) state that the corporate committees concentrate on sponsorship of operational risk initiatives, policy initiation and approval; assessment of capital allocation; and reviewing current risk issues. Business level committees looking at operational risk have also been set up by most banks. These may also be dedicated operational risk committees or integrated risk management committees. Their main task is reviewing operational risk information and they may also sponsor operational risk initiatives and instruct or approve policy.

It also seems that most banks have full-time or part-time operational risk managers. Their tasks involve tailoring and implementing the processes developed by operational risk management units; supporting business to identify and resolve operational risk issues; raising awareness of these issues; and training staff on operational risk processes. Although the background and experience of these managers differ, they are usually highly experienced in line-management authority (Bryn & Grimwade 1999:20).
According to Bryn and Grimwade (1999:19), there are three factors banks must master to ensure the successful implementation of operational risk management or structures, namely:

- **Effective communication of the commercial imperative for establishing new operational risk management resources.** This is vital to overcome business scepticism and may be achieved by highlighting examples of high-profile losses in the banking industry.

- **Outlining clear business responsibilities for managing operational risk.** Leading banks formally include operational risk in the objectives of senior management. They are also increasingly allowing business managers the flexibility to determine the level of operational risk management resources within their sector. This supports the development of tailored organisational structures appropriate to different businesses.

- **Providing strong incentives to create an effective operational risk management environment.** For example, leading banks have started to link business managers’ appraisal and financial remuneration to quantitative and verifiable operational risk metrics.

It is clear that the board of directors and internal audit play an important role in managing operational risk. It is, therefore, necessary to discuss their roles and responsibilities in more detail.
3.4.4.1. **Board of Directors**

The FMAC (1999:29) states that corporate governance is understood to be the prime responsibility of the board of directors and the chief executive officer. It combines legal duties with responsibilities to improve and monitor the performance of an organisation and is focused on three principal objectives, namely:

- To protect and reinforce the rights and interests of shareholders, particularly in areas where those rights and interests may conflict with the interests of senior management.
- To ensure that the board of directors and the chief executive officer properly fulfil their primary responsibilities to direct the strategy and monitor the performance of the organisation, particularly with regard to assessing the performance of senior management.
- To ensure that management controls and reporting procedures are satisfactory and reliable.

The management of risk forms a key part of each of the aforementioned objectives.

Bloom and Galloway (1999:6) state that building the right culture for risk management begins with instituting a disciplined approach to operational risk management. This starts with the board and filters down through every level and business unit and across every major process in the organisation. Once the infrastructure is in place, banks must learn to assess the quality of their risk management programmes and assign a value to the risks they confront.
Bryn and Grimwade (1999:19) state that making board members responsible for operational risk provides greater focus and gives sponsorship for the activities of dedicated resources. Directors may receive information on operational risk from a range of sources, including operations, internal audit and security. The effectiveness of board members is enhanced if operational risk management reports are also available. Such reports allow the board to assess the relevant levels of operational risk across the business and the major exposures and total losses resulting from operational risk breakdowns. This enables board members to take strategic decisions on resource allocation, acceptable levels of risk and priorities for improvement.

Clements (1999:34) states that the board is not just responsible for financial controls, but for all controls. This means that they must assume responsibility for the management of all risks. This approach must, according to Clements (1999:35), encompass all risks and the controls and techniques which may be required to cope with them. Care should be taken, however, not to involve the board with senior management functions. Clements (1999:35) differentiates between monitoring and management functions. He (1999:35) suggests that the board’s main role is to monitor, leaving the management to the executive team. Furthermore, it would also be counter-productive for the board to become involved in the detailed assessment and management of risk profiles.

Clements (1999:35) also refers to three activities involved in risk management and the board’s role in each of these, namely:

- **Identification.** The board should not dictate the methods to be used in this crucial first stage of the risk management process. They can, however, play a part in the process by setting some parameters. They can indicate, for example, that they expect
management to concentrate on identifying those major risks which may, if they materialise, seriously impair the achievement of the company's strategy. In effect, management should be asked to identify the major risks which may decimate those cash flows. The board may assist management by indicating just what they believe to be the principal factors which determine the size and shape of those cash flows.

- *Measurement of risk.* As with risk identification, it is once again best to leave the problem of measuring risk largely to management. The main concern of the board is the results of the measuring of the risks which they may, for example, use to set risk benchmarks to guide management.

- *Management of risk.* Here the board should provide management with a clear indication of the company's attitude towards risk.

According to Carr and Walsh (1999:48), the board should approve and issue written risk management guidelines to:

- The organisation's overall business strategies and product lines;
- Its tolerance for risk and its general risk management philosophy; and
- Any regulatory or organisational constraints.

These guidelines should also address the following issues:

- The scope of permitted treasury activity;
- Guidelines for acceptable levels of the main risk types;
- The structure and independence of the risk management processes and related organisational checks and balances; and
• Accountability at each appropriate organisational level for the results of trading activities.

These policies and guidelines should contribute to a comprehensive system of internal risk management throughout the organisation.

Clements (1999:36) summarises the main responsibilities of the board towards risk as follows:

• The board must accept ultimate responsibility for the management of risk;
• It must make its strategy clear to management, give them a benchmark to help them identify and quantify risks, and be prepared to go into detail on its attitude to risk;
• It must explain the extent to which it is delegating the problem;
• It must tell management just how it will monitor their performance; and
• It must ensure that the necessary information and communication systems are in place and functioning.

It is evident that the board of directors has an important role to play in the management of all risk types.

Another department, which has an important role to play in the management of operational risk, is internal audit. This will be discussed in the next section.
3.4.4.2. **Internal Audit**

Bjelke and Nilsson (1997:16) state that from an auditor’s point of view, risk is traditionally regarded as resulting from a weakness in the system of internal control or in the internal controls themselves. Consequently, auditors usually start their risk assessment by examining the status of internal controls. This qualitative evolution is normally a cumbersome part of the audit and, more importantly, it may not always be the most efficient approach to risk assessment in audit planning.

According to Goldman *et al.* (1998:42), the development of risk management, as a discrete discipline within organisations, has had a significant impact on the role and responsibilities of both external and internal auditors. In the case of external auditors, it means that their focus of work has to extend from verifying the integrity of the financial records to also assessing the integrity of the risk information. In the case of the internal auditor, the change is perhaps even more significant. This is because that portion of the traditional role of internal audit, which consisted of checking compliance with internal guidelines and procedures, has now been assured by the risk management function. Consequently the role of internal audit has to be focused more on the review of the integrity and completeness of the risk management process. This means that a much higher level of technical skill is now required in the internal audit function, given the type of technical skills that are required to understand and review the effectiveness of the risk management function.

Crouhy and Mark (2000:348) state that the internal audit function needs to ensure that the operational risk management process has integrity and is being implemented along with the appropriate controls. Internal audit should also offer an independent assessment of the underlying design of the operational risk
management process. This includes examining the processes surrounding the building of operational risk measurement models; the adequacy and reliability of the operational risk management systems; and compliance with external regulatory guidelines. Internal audit thus provides an overall assurance on the adequacy of operational risk management. This should include the examination of controls concerning the capturing of data. Internal audit would typically also review the adequacy and effectiveness of the processes for monitoring risk; and the documentation relating to compliance with the qualitative/quantitative criteria outlined in any regulatory guidelines (Crouhy & Mark 2000:348).

Bryn and Grimwade (1999:20) state that while most banks have established dedicated resources for managing operational risk, none has positioned these resources within internal audit. But in several banks, internal audit departments are undertaking some operational risk management responsibilities. The aforementioned separation may reflect the desire to avoid conflicts between internal audit’s independent review role and the operational responsibility for developing risk management policies, methodologies and risk reporting. It may also reflect the broader range of skills of operational risk managers.

The relationship between these two areas could, however, have positive effects, as there is scope to create incremental value from the interaction between internal audit and operational risk management. Operational risk managers, for example, use internal audit scores as proxies for the level of operational risk in a business. They also use the scores to monitor and report on the progress of business units in resolving internal audit issues. Internal audit departments, in turn, use the results of operational self-risk assessments to provide the focus of internal audits and review the effectiveness of operational risk management practices.
According to Chown (1999:8), internal audit, risk management and internal control managers should all concentrate on key risks to the organisation. The FMAC (1999:39) states that to achieve effective control, best practice requires a robust internal audit function. Thus one of the principal functions of internal audit should be the examination of control systems. In many companies internal audit has moved from the compliance function to playing a major integrating role in risk management. Internal auditors also act as facilitators and mentors to management and exercise influence over the adoption of best practice regarding risk management (FMAC 1999:39).

It seems evident that internal audit plays an important role in the procedures and control framework by providing an independent, internal assessment of the effectiveness of this framework. According to Crouhy and Mark (2000:369), the principal challenge for management is to ensure that internal audit staff have sufficient expertise to carry out work in both the front and back offices.

3.4.5. Conclusion

Risk control programmes are aimed at controlling the possible adverse effects of an event and endeavoring to eliminate it or minimise the loss after it occurs. It is also evident that a primary element of control lies in the organisational structure, which indicates the major role players as well as their responsibilities related to controlling operational risk. Although the management of operational risk is the responsibility of all levels of management, the following players are highlighted in the study:

- Board of Directors;
- Risk Management Group;
- Business units; and
The various overall elements to combat operational risk are identified as:

- Policies and procedures;
- Internal controls; and
- Risk reporting.

The operational risk mitigating techniques, such as risk-retention and risk-transfer, will be discussed in the next section as part of the last step of the operational risk management process, that is risk financing.

3.5. **Operational Risk Financing**

Risk financing is the final step of the identified risk management process. Valsamakis *et al.* (2000:171) state that the risk management process is incomplete without the element of financing.

According to Hoffman (1998:40), most financial firms arrange for risk financing and insurance programmes for two main reasons, even though they might not identify them explicitly, namely:

- To protect their earnings; and
- To protect their balance sheet; or
- Perhaps both of the above.

According to Remenyi and Heafield (1996:355), risk financing entails contemplating the financial implications of the adverse affects of a risk and concluding the financial implications of minimising the risk itself. The risk
financing function also entails reviewing the costs and benefits to an organisation in preventing or minimising risks. They (1996:355-356) also state that organisations have two fundamental options with regard to risk financing, namely:

- The organisation may decide to retain the risk. In such instance the organisation has decided that the risk may be tolerated. It should, however, be monitored to ensure that it does not become a “run-away-risk”. The organisation may also decide to adopt a self-insurance mechanism whereby it allocates its own funds to cover its own potential losses.
- The organisation may opt to transfer the risk to a third party, such as an insurance company.¹

Valsamakis et al. (2000:171) approach risk financing in a very similar way by indicating the elements of risk financing as retention and external financing (refer to figure 3.21).

When determining a risk financing programme for an organisation, it seems that risk transfer and risk retention costs are important elements to consider. It is also important, however, for a risk financing programme to fit in with the organisation’s risk reduction plan.

¹ Although many references are made about the transfer of risk in this section it must be noted that the risk itself can not be transferred, only the consequences thereof.
Zolkos (1998:50) states that risk financing programmes are practical only if they adapt to an organisation's plans and exposures. Furthermore, for a risk programme to succeed, it requires a focused risk management strategy, management commitment, constant internal communications and well-matched business partners. Zolkos (1998:50) also mentions that organisations' risk programmes vary and have different goals and needs. For instance, these programmes may help in reducing or stabilising an organisation's cost of risk, optimising calamity capacity and developing market relations.

Valsamakis et al. (2000:173) state that when an organisation considers a risk financing programme it should endeavor to achieve the following three risk management objectives:
• *Financial.* To reduce the ratio of total cost to risk and to maintain the improvement over a sustained period.

• *Resources.* To conserve assets and preserve the physical health of employees through safe working habits and work environment.

• *Customers and public.* To improve the organisation's image to the people it serves through the reduction of accident-causing conditions which affect the product it makes and the services it delivers.

In figure 3.22, Valsamakis *et al.* (2000:175) illustrate how the total cost of risk, against a yardstick of revenue, is used to ascertain the effectiveness by which the pure risk area is controlled. Initially the costs will increase as capital is spent on risk control. Then, as risk control begins to affect losses, a reduction in self-insured losses and insured losses results, with a consequent reduction in self-insurance costs and premiums. The central issue becomes one of optimal financing so that while the risk control process is being addressed, the financing of risk and losses as they occur does not introduce any inefficiencies. The model illustrates the integrative path in the risk management process. If cost of risk is defined as expenditure on risk control, expenditure relating to retained risk/self-funding, and expenditure on insurance cover, then one objective of risk management may be stated as the long-run minimisation of the cost of risk to an organisation. There are various risk financing mechanisms available to ensure the minimisation of the cost of risk.
Figure 3.22: The Cost of Risk

Source: Valsamakis et al. (2000:175)

According to Valsamakis et al. (2000:177), these risk financing mechanisms may be categorised broadly into two strategies, namely:

- *Pre-loss financing*, for example, through insurance and retention funding.
- *Post-loss financing*, for example, by means of cash resources, debt and equity finances.

Consideration is mostly given to pre-loss financing and particularly to insurance. A reason for this might be that managers tend to adopt a more risk averse attitude when making corporate decisions. This also adds a further dimension to the reasons why insurance is purchased and could also explain the more conventional orientation towards insurance as a risk-financing technique.
Conway (1999:85) states that good risk management means finding the right coverage vehicles and making sure exposures remain limited. The compatible marriage of two strategies – reducing the insurance costs through highly visible and creative alternative risk financing practices, and minimising losses through sound control and prevention measures (retention) – is critical to a successful risk management programme. He (1999:85) states that with pressure on companies to reduce costs and improve asset management, risk managers are not simply relying on lower premium rates to meet their targets. They are striving, instead, to change their roles in managing their companies’ risks. They are doing this by improving not only their financial analysis skills, but also their knowledge of creative risk financing products that cover non-traditional losses. McDonald (2001:1) states that risk managers will make greater use of creative ways to finance their risks. They will, for example, expand the risks currently financed and consider new methods of risk-transfer such as capital markets products.

Hoffman (1998:41) states that a risk financing strategy might suggest using an integrated programme of risk financing, such as:

- Self-funding of losses and captive insurance vehicles for relatively low-level risk types; and
- Conventional insurance where the firm needs to be covered against the risk of medium- to high-level losses.

Hoffman (1998:41) states that some strategic application of risk finance tools can certainly increase the odds of a more palatable result for a firm. That is, a selective use of funded self-insurance, captive insurance companies and funded deals, when woven into a risk finance programme instead of or as a supplement to conventional insurance.
It seems that risk transfer and risk retention decisions play a major role in a risk financing programme. These elements will be discussed in the following sections.

3.5.1. **Risk Transfer**

PwC (1999:77) views risk transfer as the moving of risk from one entity to another that is more willing to take the risk for a price.

According to PwC (1999:77), insurance is one of the oldest forms of risk mitigation (risk transfer). Although most organisations use insurance to mitigate a wide variety of risks, most operational risks remain uninsured and, in many cases, have been traditionally uninsurable. According to a survey by PwC (1999:77), the relationship between the insurance companies and banks with regards to operational risk is still in the development stage. It seems, however, that the operational risk-transfers in the banking industry are increasing. PwC (1999:79) identifies two possible explanations for this, namely:

- *The recognition of new risks.* The insurance industry has created new products and services or broadened existing coverage to respond to changing market needs, which include:
  - Electronic computer crime.
  - Unauthorised trading.
  - Professional indemnity.
  - Employment liability practices.
- *The possibility that market economics in the insurance industry may be causing the increase.* The insurance industry is currently experiencing a “soft” market and is offering more competitive
pricing or more comprehensive terms and cover under most programmes.

Conley (2000:10) confirms that there is a change in the market regarding risk-transfers: “We use insurance both in the traditional sense and as a corporate finance tool addressing pure balance sheet issues. We try to understand the real volatility issues and then structure a risk transfer to accommodate them. The transfer could be conventional insurance, a capital market instrument, or a combination.” According to Conley (2000:10), these developments in the insurance market create opportunities to transfer risk more cost-effectively and efficiently.

Douse (1999:6-7) also states that insurance companies are broadening their risk management services through innovation and partnership with clients. According to the FSA (1999:75), however, it is important that the purchase of these insurance products is linked to an overall strategic approach to risk. The challenge will be to link those responsible for the purchase of insurance to those charged with the overall responsibility for operational risk.

According to PwC (1999:81), once insurance companies reach a common understanding with the financial services industry on operational risk management issues, they will be able to offer better tailored and more cost-effective mitigation products.

It is important, however, that the cost of the risk-transfer be acceptable or affordable for the organisation. To ensure this, Lam (1999:16) states that it is imperative to optimise the return-on-risk management investments by linking risk management processes and risk-transfer strategies. Linking internal risk processes and external risk-transfer can help an organisation reach its risk
objectives at the lowest possible cost. Lam (1999:16) also states that to reduce undesirable risks, management should evaluate derivatives, insurance and hybrid products regularly and select the most cost-effective alternative.

Before deciding if a risk should be transferred, Valsamakis et al. (1996:304-305) list the following examples of criteria that may be applied to determine the feasibility of transferring a risk:

- There must be a large number of homogeneous exposures. These exposures are those that display similar expectations of loss;
- The insured group must be independent and hence not exposed to a catastrophe, the consequences of which cannot be estimated;
- The occurrence of the event insured against must be fortuitous; This means that the timing and severity of the loss should be entirely out of the control of the insured;
- If the peril insured against produces a loss, this must be definite in time and quantum; and
- The premium must be reasonable in relation to the potential financial loss.

According to the FSA (1999:78) risk transfer (insurance) has traditionally played only an unsatisfactory role in risk mitigation for banks for the following reasons:

- Traditional policies address only very specific and limited areas of operational risk;
- There is only a limited amount of insurance capacity available to each institution;
- Often the financial stability of the insurance capacity is questionable and the bank exchanges its operational risk for a counterparty risk;
- Insurance is illiquid - after a loss, there is neither certainty of payment nor payment sufficiently swift to protect the quarterly earnings statement;
- The insurance markets themselves are fragmented; and
- Pricing is not transparent.

The FSA (1999:78) also states that the insurance industry is ideally equipped to respond to operational risk requirements for the following reasons:

- An insurer is essentially a specialised asset manager – holding a diversified portfolio of risks, which may or may not correlate with operational risk losses in banks;
- This diversified portfolio of risk is set against a capital base much the same as a bank would do for credit and market risks;
- Pricing models have been developed to enable a wide variety of risks to be assumed into the portfolio; and
- Once sufficient data is available, the insurance industry should be able to develop both policies and actuarial models to enable an arm’s length pricing for operational risk in banks.

PwC (1999:82) states that close coordination of risk assessments with insurance may help ensure that low risks do not receive high coverage and that high risks, above the risk appetite of the organisation, receive the scrutiny needed to determine if they are insurable. Furthermore, when organisations collect their own loss data and build quantification models, they may perform their own cost-benefit analysis of insurance alternatives by weighing the cost of the premium
against the risk capital saved by insurance. It is also important to note that when risk is transferred through an insurance policy (or other means), it is only logical to reduce the associated risk capital.

3.5.2. Risk Retention

Valsamakis et al. (2000:186) state that when risk is not insured it is retained and such retained risk may be funded or unfunded. A risk is unfunded and retained when no specific provision is made for the financial consequences of a loss. Unfunded retained risks may be divided into two broad categories, namely:

- Risks which are insurable but retained; and
- Risks which are uninsurable.

Generally, the first category may be characterised by high-frequency/low-severity losses. The primary reason why risks are not funded may be that the cost of making provision to fund the risk through insurance, often exceeds the perceived benefit to the insured. In such cases, although insurance is available, the cost-to-perceived benefit prompts the risk manager to ignore the risk. In South Africa, for example, the risk of earthquakes is so small that the risk manager will decide not to insure the risk or make any other provision for it.

On the other hand, Valsamakis et al. (2000:187) argue that an organisation may find that a particular type of risk consists of a large number of independent and homogeneous exposure units, and that the historical loss patterns display a well-defined loss distribution. In such cases, aggregate annual losses may be fairly accurately estimated. This amount may be prepaid into a fund and in this manner the predicted losses may be economically retained.
According to Valsamakis et al. (2000:189), there are two fundamental reasons for retention funding, namely:

- It may not be possible to fully transfer the risk through insurance or any other device, for example, there may not exist a specific insurance market for a specific risk;
- It may be less expensive than conventional insurance "risk-transfer" techniques. This reasoning applies particularly to what have been termed high-frequency/low-severity risks where conventional transfer devices, such as insurance, may prove to be relatively expensive, given the cost structures of commercial insurance companies.

In these circumstances, retention funding may permit substantial savings in insurance premiums, with an opportunity to reduce loss costs and motivation to prevent losses by implementing sound risk control programmes.

According to Howard (1998:19), changing the organisation's level or quantity of retained risk may generate savings. Scherzer and Mackay (1998:30) state that risk controllers are often concerned with whether they should retain or transfer risk and how to do so in the most cost-efficient manner. They (1998:30) also state that organisations are retaining more risks of all types as part of their daily operations. Virtually all large companies retain more operational and hazard risk as they become more comfortable with their risk control processes and as insurance markets encourage increased risk retention.

According to Valsamakis et al. (2000:189-190), there are several practical issues that must be considered when implementing a retention programme, namely:
• Determine the opportunity and feasibility of retention funding. This includes the determining of the risk financing techniques available to the risk bearer. It also entails classifying the risks as insurable or uninsurable, which will facilitate any evaluation of a retention strategy. The organisation’s risk-retention capacity is essential. This determines the degree to which the organisation’s cash flow may be diverted from its usual uses to meet losses without significantly disrupting normal operations.

• Analysis of the statistical properties of the retained risks. In order to make decisions on retention funding, an analysis of historical patterns is necessary to estimate possible future loss costs. The statistical analysis involves determining loss distributions and using these to predict the likely future costs of losses. As a general rule, risks displaying high-loss frequency with relatively low severity are predictable and therefore amenable to retention. It is important to establish how a retention fund will stand up to claims, hence the importance of assessing the probability that the fund will be insufficient to meet these demands. This involves the determining of the destruction probability of the retention fund.

• Evaluating the appropriate retention strategy. This activity compares the funded risk-retention vis-a-vis the alternative risk-financing techniques of insurance. Basically, the process begins at one extreme by comparing the total cost of risk under a retention strategy with conventional insurance cover. Thus the intention is to determine the optimal trade-off between risk retained and risk transferred.
3.5.3. Capital Adequacy and Operational Risk

Rattaggi (2000:690) states that capital is a buffer against losses. Focusing on banking and on capital adequacy, regulators substituted the gearing ratio and the percentages-weighted assets approaches with a new paradigm, namely risk-based capital adequacy. The international regulatory intervention on risk management has evolved since then, complementing quantitative capital adequacy rules with qualitative risk management organisational standards.

According to Quick (1999:8), the banking world has undergone a series of important changes since the original Basel Accord of 1988 on capital adequacy. For the purposes of operational risk, Quick (1999:8) mentions the following two key changes:

- The shift by some banks away from traditional banking towards a more trading-orientated environment. This has meant that new types of operational risk have emerged and the likelihood of extensive losses has increased.
- The increasing concentration of processing risk in some banks. This is caused partly by the outsourcing some functions, but also by economies of scale created by new technology.

These two key developments mean that banks may be more vulnerable to sudden, extreme losses than before (Once again the Barings bank saga attests to this). It seems that the senior management of banks has an intensified interest in the everyday operational losses in order to reduce the large losses, improve general risk awareness and generally contribute to a well-run, profitable institution. On the other hand, the regulator is also looking at good systems and controls, hence
the focus on capital charges. According to Quick (1999:8), capital has two purposes from an operational risk point of view, namely:

- To provide a second line of defence to systems and controls, that is, a buffer for unexpected losses; and
- To encourage banks to invest in better systems and controls.

Currently, the regulator also faces problems with regard to operational risk. They are determining the main risks, how they can best be controlled and what level of capital may reasonably be required from banks.

According to Davies et al. (1998:71), banks and financial services have long recognised the important role that risk-based capital allocation techniques play in the overall management of their business. In the case of banks, much of the original impetus for such an approach originated with the work of the Basel Committee through the 1988 Basel Accord. The Accord established for the first time a common international standard for setting regulatory capital for banks. The Basel Accord of 1988 was an initial broad-brush approach, however, which required an overall cushion of capital for both the measured risks (credit and market) and other (unmeasured) risks. With the new Basel Capital Accord (2001:1), the Basel Committee is proposing the explicit inclusion of risks other than credit and market risks. The new Basel Accord of 2001 focuses on operational risk and is offering a range of approaches for assessing capital against this risk. The Committee’s goal is to develop methodologies that increasingly reflect an individual bank’s risk profile. The three methodologies/approaches are:

- **The Basic Indicator Approach.** According to Basel (2001:6), this is the most basic approach for allocating operational risk capital. It
uses a single indicator as a proxy for an organisation’s overall operational risk exposure. Gross income is proposed as the indicator, with each bank holding capital for operational risk equal to the amount of a fixed percentage (α), multiplied by its individual amount of gross income (α = provisional multiplication factor of 30%, determined by the Basel Committee). This simplistic approach, however, may only be suitable for smaller banks. Banks with a significant operational risk would probably use a more sophisticated approach like the Standardised Approach (see next point).

- The Standardised Approach. According to Basel (2001:6), this approach represents a further refinement along the evolutionary spectrum of operational risk capital. It differs from the Basic Indicator Approach in that a bank’s activities are divided into a number of standardised business units and business lines (see Table 3.17 for an example). In each business line, regulators have specified a broad indicator that is intended to reflect the size or volume of a bank’s activity in this area. The indicator is intended to serve as a rough proxy for the amount of operational risk within each of these business lines. In each business line, the capital charge is calculated by multiplying a bank’s broad financial indicator by a “beta” factor (β). This factor serves as a rough proxy for the relationship between the industry’s operational risk loss experience for a given business line, and the broad financial indicator representing the bank’s activity in that business line, calibrated to a desired supervisory soundness standard. For example, for the Retail Brokerage business line, the regulatory capital charge would be calculated as follows:
The total capital charge is calculated as the simple summation of the capital charges across each of the business lines. According to Basel (2001:8), the primary motivation for the Standardised Approach is that most banks are in the early stages of developing organisation-wide data on internal losses by business lines and risk types. In addition, the industry has not yet been able to show a causal relationship between risk indicators and loss experience. As a result, banks that have not developed internal loss data by the time of the implementation period of the revised new Basel Accord, and/or do not meet the criteria for the Internal Measurement Approach will require a simpler approach to calculate their regulatory capital charge. A final important feature of the Standardised Approach, identified by the Basel Committee (2001:8), is that it provides a basis for moving on a business line-by-business line basis towards the more sophisticated approaches, and will help to encourage the development of better risk management in banks.
Table 3.17: Example of Business Units, Business Lines and Indicators

<table>
<thead>
<tr>
<th>Business Units</th>
<th>Business Lines</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investment banking</td>
<td>Corporate Finance</td>
<td>Gross Income</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gross Income</td>
</tr>
<tr>
<td></td>
<td>Trading Sales</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retail Banking</td>
<td>Annual Average Assets</td>
</tr>
<tr>
<td>Banking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Commercial Banking</td>
<td>Annual Average Assets</td>
</tr>
<tr>
<td></td>
<td>Payment and Settlement</td>
<td>Annual Settlement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Throughput</td>
</tr>
<tr>
<td>Others</td>
<td>Retail Brokerage</td>
<td>Gross Income</td>
</tr>
<tr>
<td></td>
<td>Asset management</td>
<td>Total Funds Under Management</td>
</tr>
</tbody>
</table>


- **The Internal Measurement Approach.** According to the Basel Committee (2001:8), the Internal Measurement Approach provides discretion to individual banks regarding the use of internal loss data, while the method to calculate the required capital is uniformly set by supervisors. In implementing this approach, supervisors would impose quantitative and qualitative standards to ensure the integrity of the measurement approach, data quality and the adequacy of the internal control environment. According to the Basel Committee (2001:8-9), a capital charge for operational risk under this approach would be determined using the following procedures:

A bank’s activities are categorised into a number of business lines, and a broad set of operational loss types is defined and applied across business lines.
In each business line/loss type combination, the supervisor specifies an exposure indicator (EI), which is a proxy for the size of each business line's operational risk exposure.

In addition to the exposure indicator, for each business line/loss type combination banks measure, based on their internal loss data, a parameter representing the probability of loss event (PE) as well as a parameter representing the loss given that event (LGE). The product of $EI \times PE \times LGE$ is used to calculate the expected loss (EL) for each business line/loss combination.

The supervisor supplies a factor ($\gamma$ gamma) for each business line/loss type combination, which translates the expected loss (EL) into a capital charge. The gamma term represents a constant that is used to transform EL into risk or a capital charge. This is defined as the maximum amount of loss per holding period in a certain confidence interval. The overall capital charge for a particular bank is the simple sum of all the resulting products. This can be expressed in the following formula:

$$\text{Required Capital} = \sum_i \sum_j [\gamma_{(i,j)} \times EI_{(i,j)} \times PE_{(i,j)} \times LGE_{(i,j)}]$$

Where:
- $i =$ business line
- $j =$ the risk type

To facilitate the process of supervisory validation, banks supply their supervisors with the individual components of the expected loss calculation (that is, EI, PE, LGE) instead of just the product EL. Based on this information, supervisors calculate EL and then adjust for unexpected loss through the gamma factor to achieve the desired soundness standard.
The Internal Measurement Approach allows the capital charge to be driven by a bank’s own operational loss experiences within a supervisory assessment framework, while the first two approaches are pre-determined by regulators. According to the Basel Committee (2001:2), a bank’s ability to meet specific criteria would determine the framework used for its regulatory operational risk capital calculation. The Committee intends to calibrate the spectrum of approaches so that the capital charge for a typical bank would be less at each progressive step in the spectrum of these approaches. This is consistent with the Committee’s belief that increasing levels of sophistication of risk management and precision of measurement methodology should generally be rewarded with a reduction in the regulatory operational risk capital requirement.

The Basel Committee (2001:3) states that, in line with other banking risks, a capital charge for operational risk should conceptually cover unexpected losses due to operational risk. Provision should cover expected losses.

According to the New Basel Accord (2001:4), there are three pillars that play an important role in the operational risk capital framework, namely:

- **Minimum capital requirements.** This is used to determine eligibility to use a particular capital assessment technique. The Committee believes that a rigorous control environment is essential to the prudent management of, and the limiting of exposure to operational risk.

- **Supervisory review process.** This pillar recognises the supervisory review process as an integral and critical component of the capital framework. It sets out a framework in which banks are required to assess the economic capital they need to support their risks.
Market discipline. This pillar has the potential to reinforce capital regulation and other supervisory efforts to promote safety and soundness in banks and financial systems. It imposes strong incentives on banks to conduct their business in a safe, sound and efficient manner. It can also provide a bank with an incentive to maintain a strong capital base as a cushion against potential future losses arising from its risk exposures.

According to Basel (2001:4), the above-mentioned framework presents the three approaches for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity.

Taking into account the above approaches proposed by the Basel Committee, it is clear that operational risk forms an important part of a bank’s capital charge. Although it seems that the process of determining operational risk capital is still in its early stages and there are still unresolved problem areas, it is clear that banks should actively get involved in the process of adopting the proposed approaches.

3.5.4. Conclusion

It is evident that risk financing forms an integral part of the operational risk management process. It is also clear that when management makes a decision on how to effectively minimise operational risk in the most cost-effective way, it may do so by means of two methods. These methods are risk retention and risk transfer. Both methods may have a significant impact on the profit of a bank. A decision may result in a cost to the bank in terms of external insurance, internal retention funding or a loss, if uninsured.
There also seems to be external pressure on banks from international and national regulatory committees (such as the Basel Committee) to play a proactive role in the management of operational risk capital adequacy. Although this issue is still in its planning phase and a number of questions are still unanswered, it seems imperative that all banks become actively involved in the process to decide on the most appropriate approach in determining their capital charge for operational risk.

3.6. Summary

This chapter focused on the theory and concepts of operational risk. From this literature study it is evident that operational risk management is currently an important topic in the banking industry. It seems that the main operational exposures to a bank fall within the broad categories of people, processes, systems, and those factors outside the direct control of the organisation (external factors). These exposures may also be termed the "underlying operational risk factors". The research indicates that there is a vast number of sub-risks for each primary risk factor and that the dynamic nature of operational risk and its underlying risk factors, make it a near impossible task to specify all such sub-risks.

Evaluation of operational risk, as the second step in the risk management process, includes the measurement and assessment of operational risk. Different qualitative and quantitative methodologies for measuring operational risk exist, however, it seems that the current problem area for operational risk lies in the quantification thereof. It is also evident that a risk manager should consider the outcome of more than one result methodology before making crucial risk management decisions in order to ensure sound decision-making.
Control, as the third step in the risk management process, is discussed in terms of the different role players and their subsequent risk-management responsibilities. The roles of the board of directors, line managers and internal audit are emphasised in these discussions. Policies and procedures, internal controls, and risk reporting are the other elements of risk control which are identified as forming an important part of operational risk control.

Finally, risk financing also forms an integral and important part of the operational risk management process. Risk retention and risk-transfer are the two primary risk-mitigating techniques, which are discussed as part of the cost of risk for the organisation. Capital adequacy, in accordance with the new 2001 Basel Committee proposals, is also addressed. From the research it is evident that banks will have to play an active role in this process of determining their capital adequacy in terms of operational risk as the calculation of capital charges, required by the regulators, will become compulsory in the near future.

This chapter concludes the literature study, as the first phase, of the research. The next phase is the planning and conducting of the empirical research. Here information will be obtained from various banks in the national and international banking environment. The following chapter will deal with the research methodology as well as the design of a questionnaire for the empirical research. The results will be analysed and integrated with the theories and concepts identified during the literature study, to develop a structured approach to operational risk management in a banking environment.
CHAPTER 4

RESEARCH METHODOLOGY

4.1. Introduction

The first phase of this study dealt with the literature research and is based on a qualitative exploratory research framework. It includes the identification and analysis of key concepts regarding risk management. Clear definitions were set for applicable concepts and the relevant risk factors were identified. In addition, documented approaches to the management of operational risk were also analysed to form the basis for the empirical research.

The aim of this chapter is to provide the research methodology used for the gathering and analysing of the data for this study. This chapter firstly deals with the theory of research design; secondly, with the actual research methods used in this study; and finally, with the statistical techniques used for the analysis of the data.

4.2. Research Design

Mouton (1996:176) states that the aim of a research design is to employ various measures to control systematic bias, confounding variables and other sources of error. Zikmund (1997:48) defines research design as a master plan specifying the methods and procedures for collecting and analysing the required information. He (1997:49) mentions that the four basic design techniques are surveys, experiments, secondary data and observation with the most common method of generating primary data, being surveys. A survey is a research technique in which information is gathered from a sample of people through, for example,
questionnaires or interviews. Leedy (1993:122) states that there are four discrete research methodologies which are dictated by the type of data required, namely:

- **The descriptive survey method.** This method is appropriate for data derived from simple observational situations, such as, physical observations or observations by means of questionnaires or poll techniques.
- **The historical method.** This method is appropriate for the primary data that are primarily documentary or literary in form.
- **The analytical survey method.** This method is appropriate for data that are quantitative in nature and that require statistical techniques to extract their meaning.
- **The experimental method.** This method is appropriate for data derived from an experimental control situation or a pre-test/post-test design in which two separate groups, or one group, from which data are derived at two separate intervals, are involved.

According to Zikmund (1997:202), surveys require asking people or "respondents" for information, using either verbal or written questioning. Questionnaires or interviews are used to collect data. Although it has been suggested that surveys be conducted to quantify certain factual information, certain aspects of surveys may also be qualitative. Zikmund (1997:203) also states that surveys provide a quick, inexpensive, efficient and accurate means of assessing information about the population. For the purpose of this study, however, the focus is more on a quantitative approach. Thus, the analytical survey method will be applied as the data will be subjected to statistical analysis to extract its meaning.
There are basically two methods of gathering data, that is, interviews and questionnaires. These will be discussed in the following section.

4.2.1. Interviews

The structured interview is closely related to the questionnaire which is, according to Leedy (1993:192), a data-gathering technique that needs careful planning. Zikmund (1997:232) lists the following advantages and disadvantages of interviews:

- **Advantages**
  - The opportunity for feedback to the respondent exists. The interviewer may provide feedback in clarifying questions about the instructions or the questions;
  - Complex answers may be clarified with the respondent;
  - A lengthy questionnaire may be dealt with in more detail during an interview;
  - Responses to all the questions may be generated ensuring the completeness of the survey; and
  - The presence of an interviewer generally increases the percentage of people willing to complete the interview.

- **Disadvantages**
  - Respondents are not anonymous and therefore may be reluctant to provide confidential information;
  - Demographic characteristics of the interviewer may influence respondents’ answers;
  - Differential interviewer techniques may be a source of interviewer bias;
• Personal interviews are generally more expensive than mail interviews; and
• Interviews can be time consuming;

Before using this technique to gather data, it may be necessary to consider the above-mentioned advantages and disadvantages to determine whether it is the most suitable technique.

4.2.2. Questionnaires

In many situations an interview is not essential and questionnaires may be used to gather data. According to Bethlehem (1999:95), a questionnaire is an instrument to collect the survey information on persons, enterprises and so on. He (1999:95) also lists different object types which may be included in a questionnaire, namely:

• Question. Each question may have an identification, a question text, a specification of the type of answer that is expected and a field in which the answer is stored.
• Routing instruction. The result of the evaluation of one or more conditions will determine the next question.
• Check. Each check may have identification, that is, a logical expression describing a condition that must be fulfilled and an error message (which is displayed when the condition is not met when using an electronic questionnaire).
• Computation. Each computation may have an identification, an arithmetic expression and a reference to a field in which the result must be stored.
Jenkins and Solomonides (1999:79) state that almost all research surveys use some form of questionnaire as a data collection mechanism. It is important, however, that the questions in a questionnaire be arranged in a perfect sequence to form a "well-routed" questionnaire. Jenkins and Solomonides (1999:79) list the following pragmatics of a well-routed questionnaire:

- The general flow of control always moves from the beginning to the end of the questionnaire;
- Each question appears only once in the questionnaire;
- The respondent is asked only once for each item of information; and
- Changes in topics are avoided and broad topics are covered first.

It is possible to arrange the composition of the questionnaire to minimise routing paths by grouping questions with the same context.

It is essential that questions be clear. Zimmerman and Schultz (2000:177) state that when constructing questions for a questionnaire, the following must be kept in mind:

- Readers must interpret the meaning and intent of the question;
- They must recall relevant information and integrate that information into a single answer; and
- They must translate that answer into an appropriate response on the form.

They (2000:17) state that when readers are motivated to perform these necessary cognitive tasks in a careful and objective manner, they are said to be "optimising". When the cognitive task of completing a questionnaire becomes
too demanding, however, respondents may be less diligent in some or all parts of the response process and provide satisfactory answers rather than optimal ones.

According to Bagin and Rose (1991:64-66), a survey of questionnaires indicated the following general complaints:

- Forms too complicated;
- Instructions unclear;
- Form too long;
- Type too small;
- Not enough room for answers;
- Words too difficult; and
- Information requested too personal.

To ensure that the above-mentioned problems are eliminated, it is necessary to pretest a questionnaire before it is sent out. This should, according to Schriver (1989:316), be performed by experts and users in order to evaluate the questionnaire in terms of:

- Unfamiliar terminology;
- Insufficient directions and how to complete the form; and
- Insufficient space for writing answers.

According to Zikmund (1997:244), questionnaires present several advantages and disadvantages, for example:

- *Geographic flexibility.* Mail questionnaires may reach geographically dispersed samples simultaneously and at a
relatively low cost. They may also be widely distributed to a large number of respondents;

- **Cost.** Mail questionnaires are relatively low in cost compared to personal interviews and telephone surveys. Mail surveys, however, are not inexpensive;

- **Respondent convenience.** Mail and self-administered questionnaires may be completed whenever the respondent has time. Thus, there is a better chance that respondents will take time to think about their replies;

- **Interviewers absence.** Although the absence of an interviewer induces respondents to reveal sensitive or socially undesirable information, it may also be a disadvantage. Once the respondent receives the questionnaire, the answering process is beyond the control of the researcher. The respondent does not have the opportunity to ask questions of an interviewer. Problems that may be clarified in an interview, remain misunderstandings in a mail survey;

- **Standardised questions.** Mail questionnaires are highly standardised and the questions quite structured. Questions and instructions must be clear-cut and straightforward;

- **Time is money.** If time is a factor in management’s interest in the research result or if attitudes are rapidly changing, mail surveys may not be the best research option. A minimum of two – three weeks is necessary to receive the majority of the responses;

- **Length of mail questionnaires.** Mail questionnaires vary considerably in length, ranging from extremely short post card questionnaires to lengthy, multi-paged booklets. A general rule of thumb is that a mail questionnaire should not exceed six pages in length;
• **Response rates.** Surveys that are boring, unclear or too complex get discarded. A poorly designed survey may be returned by only 15% of those sampled; and

• **Increasing response rates to mail surveys.** Non response error is always a potential problem in mail surveys. Individuals who are interested in the subject matter of the survey tend to respond at a higher rate than those with less interest or experience. Examples of how to ensure response returns are postpaid return envelopes; designing attractive questionnaires; and wording questions so they are easy to understand.

Leedy (1993:188) states that questionnaires should be designed to fulfil a specific research objective and that the respondent should be considered when constructing the questions. In this regard, he (1993:188) lists the following considerations:

• Be courteous;
• Make the questions as simple as possible;
• Think of the other person (respondent);
• Concentrate on the universal rather than specifics relating to personal matters;
• Make it brief;
• Check for consistence;
• Send return postage;
• Offer the results of the study to the respondent; and
• Think ahead and decide up-front how the results of the questionnaire will be processed.
The phrasing of questions is another important issue to consider when constructing a questionnaire for data gathering. There are many ways to phrase questions. Zikmund (1997:380) states that there are two basic types of questions which are based on the amount of freedom respondents are given in answering questions, namely:

- **Open-ended response questions.** These questions allow respondents to answer the questions in their own words; and
- **Fixed-alternative questions (closed questions).** These questions give respondents specific and limited alternatives and request respondents to choose the one closest to their own viewpoint.

According to Zikmund (1997:383), the means of data collection (mail or interviews) will influence the question format and question phrasing. In general, mail questions should be less complex than those used in personal interviews. He (1997:385) lists the following guidelines when developing a questionnaire:

- Avoid complexity by using simple, conventional language;
- Avoid leading and loaded questions;
- Avoid ambiguity by being as specific as possible;
- Avoid double-barreled items;
- Avoid making assumptions; and
- Avoid burdensome questions that may tax the respondent's memory.

Cooper and Emory (1995:132) state that research questions should follow logically from the research problem and must provide the required answers.
4.3. **Data Measuring**

Huysamen (1994:9) states that measurement consists of the assignment according to fixed rules, of numbers to indicate differences in the magnitude of some attribute of people or objects.

Zikmund (1997:333) states that before the measurement process may be initiated, the researcher must identify the concepts relevant to the problem. A concept is a generalised idea about a class of objects, attributes, occurrences or processes. Concepts such as age, sex and number of children are relatively concrete properties and present few problems in definition or measurement. Other characteristics of individuals or properties of objects may be more abstract. A concept must be made operational in order to be measured. An operational definition gives meaning to a concept by specifying the activities or operations necessary to measure it. Operational definitions help the researcher specify the rules for assigning numbers. The values assigned in the measuring process may be manipulated according to certain mathematical rules. The properties of the scale of numbers may allow the researcher to add, subtract or multiply answers. In certain cases there may be problems with the simple addition of the numbers or other mathematical manipulations because these are not permissible within the mathematical system (Zikmund 1997:336).

Thus, for a question to be of any value, it must be measurable. There are various scales which may be used to ensure the measurability of questions. Zikmund (1997:336) states that a scale may be defined as any series of items which is progressively arranged according to value or magnitude into which an item may be placed according to its quantification. The purpose of scaling is to represent, usually quantitatively, an item’s, person’s or event’s place in the spectrum. In business research there are many scales or number systems. Traditionally scales
of measurement are clarified on the basis of the mathematical comparisons that are allowable with these scales. Zikmund (1997:336) and other authors such as Leedy (1993:249), Smith (1981:146), McCallon and McCray (1975:29) and Leach et al. (1986:9) agree on four types of scales, which are described as follows:

- **Nominal Scale.** This scale is the simplest type of scale. The numbers or letters assigned to objects serve as labels for identification or classification. These are scales in name only and no numerical value is attached to them.

- **Ordinal Scale.** This scale arranges objects or alternatives according to their magnitude in an ordered relationship. When respondents are asked to rank their investment preferences, ordinal values are assigned. A typical ordinal scale in business research asks respondents to rate items such as career opportunities, brands and companies as “excellent”, “good”, “fair”, or “poor”. We know “excellent” is higher than “good”, but we do not know by how much. This scale may effectively be used for questionnaires where the attitude or viewpoint of individuals may be determined.

- **Interval Scale.** This scale not only indicates order, it also measures order in units of equal intervals. The classic example of an interval scale is the Fahrenheit temperature scale. If a temperature is 80 degrees, it cannot be said that it is twice as hot as 40 degrees. The reason for this is that 0 degrees does not represent the lack of temperature, but a relative point on the Fahrenheit scale. Due to the lack of an absolute zero point, the interval scale does not allow the conclusion that 36 is three times as great as 12, only that the interval distance is three times greater.
• *Ratio Scale.* These scales have absolute rather than relative quantities. For example, money and weight are ratio scales because they possess an absolute zero and interval properties. The absolute zero represents a point on the scale where there is an absence of the given attribute. Because the scale of measurement is ratio, financial researchers are allowed to construct ratios derived from the original scales. For most behavioral research, however, interval scales are typically the highest forms of measurement.

The type of scale that is utilised in business research will determine the form of statistical analysis. For example, a number of operations, such as the calculation of the mean, may be conducted only if the scale is of an interval or ratio nature; they are not permissible with normal or ordinal scales (Zikmund 1997:338). Refer to paragraph 4.5.3 for the measuring scale used in this study.

Various techniques are used to measure the attitude of respondents. According to Zikmund (1997:353), to obtain statements from respondents generally requires that the respondent perform a task such as ranking, rating, sorting or making a choice or a *comparison.*

• A *ranking* task requires that respondents rank a small number of items in overall preference or on the basis of some characteristics of the stimulus.

• *Rating* asks respondents to estimate the magnitude of a characteristic or quality that an object possesses. Quantitative scores, arranged along a continuum that has been supplied to the respondents, are used to estimate the strength of the attitude or
belief. In other words, respondents indicate the position, on a scale, where they would rate the object.

- A sorting technique might present respondents with several product concepts printed on cards and require that the respondents arrange the cards into a number of piles or otherwise classify the product concept.
- The choice technique requires respondents to select one or more alternatives. If a respondent chooses an object over another, it is assumed the chosen object is preferred over the other.

According to Zikmund (1997:353), using rating scales to measure attitudes is perhaps the most common practice in business research. He (1997:353) distinguishes between the following types of scaling:

- **Simple Attitude Scaling.** This scaling requires that an individual agrees or disagrees with a statement or responds to a single question. For example, respondents in a political poll may be asked whether they agree or disagree with a statement. Because this type of self-rating scale merely classifies respondents into one of two categories, it has only the properties of a nominal scale.
- **Category Scale.** Some rating scales have only two response categories: agree or disagree. Expanding the response categories provides the respondent more flexibility in the rating task. Even more information is provided if the categories are ordered according to a descriptive or evaluative dimension.
- **Summated Ratings Method: The Likert Scale.** With the Likert scale, respondents indicate their attitudes by checking how strongly they agree or disagree with carefully constructed statements that range from very positive to very negative toward
the attitudinal object. Individuals generally choose from five alternatives: strongly agree, agree, uncertain, disagree and strongly disagree. To measure the attitude, researchers assign scores or weights to the alternative responses. A Likert scale may include several scale items to form an index. The total score is the summation of the weights assigned to an individual's total response.

- **Semantic Differential.** The semantic differential is a series of attitude scales. This technique consists of identifying a company, product, brand, job or other concept, followed by a series of seven-point bipolar rating scales. Bipolar adjectives, such as "good and bad", "modern and old-fashioned" or "clean and dirty" anchor the beginning and end of the scale. Respondents are instructed to check the place that indicates the nearest appropriate adjective on the following example:

  Fast _____ _____ _____ _____ _____ Slow

- **Numerical Scales.** Numerical scales have numbers as response options rather than "semantic space" or verbal descriptions to identify categories. If the scale items have five response positions, the scale is called a five-point numerical scale, for example:

  Extremely satisfied 5 4 3 2 1 Extremely dissatisfied

This numerical scale uses bipolar adjectives in the same manner as the semantic differential.

- **Other Scales.** Other scales (not applicable to this study) are:
  - Constant-Sum Scale;
• Stapel Scale;
• Graphical Rating Scales;
• Thurstone Equal-Appearing Interval Scale; and
• Scales measuring Behavioral Intentions and Expectations.

Amoo and Friedman (2000:301) state that, like all measuring devices, the rating scale is only useful if it provides reliable and valid measures. Therefore, before conducting a survey, it may be necessary to pretest the measuring instrument and the data to be gathered in order to evaluate it in terms of validity and reliability. Refer to paragraph 4.5.4 for the methods applied to determine the validity and reliability of the measuring instrument for this study.

4.4. Pretesting for Validity and Reliability

According to Zikmund (1997:402), a questionnaire is usually tested on a group that is selected on a convenience basis and is similar in make-up to the one that ultimately will be sampled. A group should be selected that is not too divergent from the actual respondents. The pretesting process allows the researcher to determine if respondents have any difficulty understanding the questionnaire or if there are any ambiguous or biased questions. Zikmund (1997:404) states that pretests are typically conducted to answer questions about the questionnaire, such as:

• Can the interviewers follow the questionnaire format?
• Does the questionnaire flow naturally and conversationally?
• Can respondents answer the questions easily?
• Which alternative forms of questions work best?
Pretests also provide the means to test the sampling procedures. They may also provide estimates for the response rate for mail surveys and completion rate for surveys.

Over and above the above-mentioned pretesting of questions, it is also necessary to measure the questionnaire in terms of validity and reliability.

4.4.1. **Validity**

Huysamen (1994:35) states that the validity of test scores refers to the extent to which the scores satisfy their intended purpose. Leedy (1993:40) states that validity is concerned with the soundness and the effectiveness of the measuring instrument. Zikmund (1997:342) states that researchers want to know if this measure is valid. The question of validity expresses their concern with accurate measurement. Validity addresses the problem of whether a measure measures what it is supposed to measure.

Leedy (1993:41), Zikmund (1997:343), Huysamen (1994:35) and Dillon *et al.* (1987:164) agree that there are several types of validity, such as the following:

- **Face Validity.** This type of validity relies on the subjective judgement of the researcher. Researchers must answer two questions in accordance with their judgement, namely:
  - Is the instrument measuring what it is supposed to measure?
  - Is the sample being measured adequate to be representative of the behavior or trait being measured?
• **Criterion Validity.** Criterion validity is an attempt to answer the question: “does the measure correlate with other measures of the same construct?”

• **Content Validity.** This type of validity is sometimes equated with face validity. It is the accuracy with which an instrument measures the factors or situations under study.

• **Construct Validity.** A construct validation concerns the degree to which the construct itself is measured. Establishing construct validity occurs during the statistical analysis of the data. With construct validity, the empirical evidence is consistent with the theoretical logic about the concepts. In its simplest form, if the measure behaves the way it is supposed to (in a pattern of inter-correlation with a variety of other variables) there is evidence of construct validity (Sonquist & Dunkelburg 1977:355).

• **Discriminant Validity.** A measure has discriminant validity when it has a low correlation with measures of dissimilar concepts.

• **Internal Validity.** This is the freedom from bias in forming conclusions in view of the data. It seeks to ascertain that the changes in the dependent variable are the result of the influences of the independent variable rather than the manner in which the research was designed.

• **External Validity.** This type of validity is concerned with the generalisation of conclusions reached through observation of a sample of the universe; or to what extent do samples represent the population.

It appears that validity looks at the end results of measurement and the principle question that validity poses is: “are we really measuring what we think we are measuring?”.
4.4.2. Reliability

Huysamen (1994:24) states that reliability of a test refers to how consistently it measures whatever it measures. Zikmund (1997: 340) broadly defines reliability as the degree to which measures are free from error and therefore yield consistent results. For example, ordinal-level measures are reliable if they consistently rank-order subjects in the same manner; reliable interval-level measures consistently rank-order and maintain the distance between subjects. Low reliability results from imperfections in the measuring process that affect the assignment of scores or numbers in different ways each time a measure is taken, such as a respondent who misunderstands a question.

Leedy (1993:42) states that reliability asks one question above all others: “With what accuracy does the measure (test, instrument, inventory, questionnaire) measure what it is intended to measure?”. There are various methods to measure reliability. Zikmund (1997:341) and other authors such as Williamson et al. (1977:98) and Schmitt and Klimoski (1991:89) describe the following methods:

- **The test-retest method.** This method involves administering the same scale or measure to the same respondents on two separate occasions to test for stability. If the measure is stable over time, the reported test, administered under conditions similar to the first test, should obtain similar results. For example, suppose a researcher measures job satisfaction and finds 64% of the population is satisfied with their jobs. If the study is repeated a few weeks later, under similar conditions, and the researcher again finds that 64% of the population is satisfied with their jobs, the measure would then appear to be reliable.
- **The Split-half method.** This technique of splitting halves is the most basic method of checking consistency when a measure contains a large number of items. Here the researcher may take the results obtained from one half of the scale items and check them against the results from the other half of the items.

- **The Equivalent-form method.** Two alternative instruments are designed to be as equivalent as possible. Each of the two measurement scales is administered to the same group of subjects. If there is a high correlation between the two forms, the researcher concludes that the scale is reliable.

Schmitt and Klimoski (1991:92) state that researchers are frequently faced with a situation in which two forms of an instrument are unavailable and for a second administration of a test is not possible. One solution in this case is to take the items in the test and split them randomly in two halves and correlate the scores of the examinees of these two half tests. This correlation would be the reliability of a test one-half as long as the original. To obtain the reliability of the full length test, one needs to apply the *Spearman-Brown* correction formula which is as follows:

\[ r_{\text{full}} = \frac{2r}{1+r} \]

Where:  
\( r_{\text{full}} = \) the reliability of the full length  
\( r = \) the correlation between the two half tests.

Hussey and Hussey (1997:231) refer to the *Spearman's correlation coefficient* as another measure of the association between variables. It is described as a nonparametric technique used to measure the association between variables comprising of bivariate data and ordinal status. The formula is as follows:
\[ r_s = 1 - \frac{\text{d}^2}{n(n^2-1)} \]

Where: \( d \) = difference between the two ranked variables
\( n \) = number of data pairs
\( \Sigma \) = the sum of

The results of the above may be the following:

- \( r_s = 1 \) there is perfect positive linear association
- \( r_s = 0 \) there is no linear association
- \( r_s = -1 \) there is perfect negative linear association

According to the critical value of \( r_s \) the association and the significance at a certain percentage level (for example, 5%) between the variables could be established. The Statplus analysis programme of Berk and Carey (2000:321) can be used to compute this test to determine the significance level of the variables.

Another form of internal consistency is called coefficient alpha. According to Schmitt and Klimoski (1991:92), if one were to split the items in a test in all possible ways and average the split-half reliabilities obtained in this manner, one would have coefficient alpha. The formula for the calculation is as follows:

\[ r_a = \frac{n^2 \bar{r}_{ij}}{C} \]

Where: \( r_a = \text{coefficient alpha} \)
\( n \) = number of items in the test
\( \bar{r}_{ij} \) = the average inter-correlation between different items in the test
\( C \) = the sum of all the items in the item inter-correlation matrix including items above and below the diagonal and
the diagonal values (all 1.00 in the case of a correlation matrix).

Huysamen (1994:27) states that with the internal-consistency methods (split-half and coefficient alpha) only a single test is involved. He (1994:31) also mentions that Cronbach developed the following equation for the mean split-half reliability coefficient, a quantity which is called coefficient alpha:

\[
\text{Coefficient Alpha} = \left\{ \frac{\sum_{j=1}^{k} \text{variances of the item variances}}{k} \right\} \left\{ 1 - \frac{\text{sum of the item variances/variances of the total test}}{\text{total number of items in the test}} \right\}
\]

Thus if the variance of the five-item test equals 1.00 and the five item variances are 0.16; 0.13; 0.16; 0.22 and 0.21 then:

\[
\text{Coefficient Alpha} = \left\{ \frac{0.88}{5-1} \right\} \left\{ 1 - \frac{0.88/1.00}{5} \right\} = 0.15
\]

Coefficient alpha can be determined for dichotomous items (that is, items which can earn a mark of either 0 or 1 only, such as correct/incorrect items) as well as multi-point items (that is, items which may be assigned more than two values as in the case of rating scales). Like the split-half reliability coefficient, coefficient alpha represents a coefficient of internal consistency. Instead of being determined from a single split of the total test, however, coefficient alpha is based on all possible splits. It thus reflects the degree to which all possible splits measure the same thing, that is, the internal consistency of the test. The more different groups of items measure different attributes, the more coefficient alpha will be reduced.

According to Amoo and Friedman (2000:301), the result of Cronbach's coefficient alpha averages close to a value of 1, thus indicating a high degree of
internal consistency. It, therefore, poses a reliable measure which may be accepted for a reliability test.

Taking the above-mentioned theory into account, the following section deals with the data gathering method used in this study as well as the methods applied to determine validity and reliability of the chosen gathering method.

4.5. **Data Gathering Method Used in this Study**

Considering the various advantages and disadvantages of interviews and questionnaires, a self-administered questionnaire is regarded as the best method of gathering data for this research for the following reasons:

- It is the most efficient way to reach foreign banks which form part of the survey;
- Personal interviews will be too time consuming;
- Questionnaires may be distributed via e-mail and post. All the banks, identified for the survey, are approachable via this method;
- Questionnaires will be more feasible than personal interviews if the time and costs to visit foreign banks are considered; and
- Respondents can complete the questionnaire in their own time and thus be more objective.

The questionnaire consisted of mostly close-ended questions where the respondent only has to select an answer. However, to give the respondents the opportunity to respond outside the given alternatives and give them a chance to give their personal opinions, some open-ended questions has been included.
4.5.1. Target Population

Zikmund (1997:417) describes the target population as the complete group of specific population elements relevant to the research project. For the purposes of this research, the target population comprises local and foreign banks. The local banks, included in the survey, are those applicable banks affiliated to the Payments Association of South Africa. The reason for this selection is that it includes all the larger and most of the smaller banks in South Africa, which ensures an even spread of all banks (The banks excluded are, for example, the South African Reserve Bank and Regal Treasury). The foreign banks were chosen from a list of top financial institutions in the world as identified in a previous study by Van der Merwe (1996:22). These banks also represent financial institutions over a wide spectrum of countries across the world. The banks identified to be included in the target population are set out in table 4.1.

Table 4.1: Target Population for the Research

<table>
<thead>
<tr>
<th>Local Banks</th>
<th>Foreign Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSA Bank Ltd</td>
<td>Barclays Bank – London UK</td>
</tr>
<tr>
<td>BoE Bank Ltd</td>
<td>Canadian Imperial Bank of Commerce</td>
</tr>
<tr>
<td>FirstRand Bank Ltd</td>
<td>CITI Group</td>
</tr>
<tr>
<td>HBZ Bank Ltd</td>
<td>Common Wealth Bank of Australia – Australia</td>
</tr>
<tr>
<td>Investec Bank Ltd</td>
<td>De Nederlandsche Bank – Amsterdam</td>
</tr>
<tr>
<td>Mercantile Bank Ltd</td>
<td>Deutsche Bank</td>
</tr>
<tr>
<td>Nedcor Bank Ltd</td>
<td>Lloyds Bank – London UK</td>
</tr>
<tr>
<td>Old Mutual Bank Ltd</td>
<td>Royal Bank of Scotland</td>
</tr>
<tr>
<td>Saambou Bank Ltd</td>
<td>Standard Bank London</td>
</tr>
<tr>
<td>Standard Bank of South Africa Ltd</td>
<td>Union Bank of Switzerland – Zurich</td>
</tr>
<tr>
<td>Peoples Bank Ltd</td>
<td>Westpac Banking Corporation Australia</td>
</tr>
<tr>
<td>Unibank Ltd</td>
<td></td>
</tr>
</tbody>
</table>
The perspectives and personal experience of senior managers and executives employed by the above-mentioned banks were targeted, with focus on the following specialised areas and positions:

- Business Unit Managers (Line managers);
- Internal Audit staff;
- Risk Managers; and
- Operational Risk Managers.

A total of 25 banks were identified. Focusing on the above-mentioned specialised areas and positions, a total of 94 questionnaires were distributed. The questionnaires were mailed and e-mailed to the targeted respondents on 26 June 2001 under a cover letter (see Annexure A). A total of 63 completed questionnaires were returned by the target date of 31 July 2001, representing a total response of 67%.

4.5.2. Format of the Questions

As mentioned previously, the questions are mostly close-ended, supported by open-ended questions when it is necessary to determine the opinions of respondents. The main reasons for the close-ended structured questions are as follows:

- Structured questions are usually self-explanatory and do not require the presence of an interviewer;
- Structured questions may be answered faster and will not waste a respondent’s time;
- Structured questions require fewer instructions; and
• Structured questions may focus the respondent’s attention to a specific issue.

During the development of the questions the following requirements, listed by Zikmund (1997:385), were adhered to:

• Avoid complexity by using simple, conventional language;
• Avoid leading and loaded questions;
• Avoid ambiguity by being as specific as possible;
• Avoid double-barreled items;
• Avoid making assumptions; and
• Avoid burdensome questions that may tax the respondent’s memory.

4.5.3. Choice of Measuring Scale

In paragraph 4.3, various measuring scales were discussed. The ordinal scale seems the most appropriate measuring scale for the close-ended questions as this scale, according to Zikmund (1997:337), is ideal for questionnaires where the attitude or viewpoints of individuals may be determined. The Likert-type ordinal scale, therefore, seems the best scale to measure the attitudes of respondents to determine to what degree they agree or disagree with the close-ended questions/statements, which varies from “no degree” to “total degree”. According to Zikmund (1997: 357), a single scale item on a summated rating scale is an ordinal scale, while the Likert measurement may include several scale items to form an index. Each statement is assumed to represent an aspect of a common attitudinal domain.
The respondents could choose from five alternatives, which are coupled to values from 1 to 5 as illustrated in table 4.2. Strong agreement indicates the most favorable attitudes on the statement, and the value of 5 is assigned to this response. If the statement/question is negative, the value is reversed.

**Table 4.2: Likert-type Scale to Measure the Response**

<table>
<thead>
<tr>
<th>Scale Value</th>
<th>Scale Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>To no degree. Indicates that the statement is of no relevance, unimportant or not implemented according to the respondent’s view and experience.</td>
</tr>
<tr>
<td>2</td>
<td>To a lesser degree. Indicates that the statement could be relevant, important or is in an early stage of development according to the respondent’s view and experience.</td>
</tr>
<tr>
<td>3</td>
<td>To a fair degree. Indicates that the statement is relevant, important or in the process of being developed and implemented according to the respondent’s view and experience.</td>
</tr>
<tr>
<td>4</td>
<td>To a higher degree. Indicates that the statement is relevant, very important and implemented to a high degree according to the respondent’s view and experience.</td>
</tr>
<tr>
<td>5</td>
<td>Totally. Indicates that the statement is absolutely relevant, highly important and in an advanced stage of implementation according to the respondent’s view and experience.</td>
</tr>
</tbody>
</table>

The questions/statements were subsequently formulated based on the literature study on operational risk management (see Annexure B). The next step was the
pretesting of the questionnaire to determine its validity and reliability. This is discussed in the ensuing section.

4.5.4. Pretesting of the Questionnaire

The questionnaire was pretested to determine its validity and reliability in cooperation with 15 senior managers of Standard Bank of South Africa in various specialised areas and positions, representing 16% of the respondents.

4.5.4.1. Validity

Content validity is the best validity criteria for this study, because the questionnaire measures the attitude and opinions of individuals on operational risk management. According to Schmitt and Klimoski (1991:102), content validity refers to the degree to which the responses, required by the test items, are a representative sample of the knowledge to be exhibited in the domain about which inferences need to be made. Consequently, the researcher must:

- Carefully specify the area of performance or behavior about which inferences are desired;
- Clearly formulate the intended uses of the test; and
- Consider and carefully specify the degree to which the test items sample the behavior or performance domain of interest.

In addition, Huysamen (1994:42) states that content validity should be evaluated by experts in the field involved. Their task is to evaluate whether the chosen items adequately represent the tasks in the universe as defined by the test constructor; and whether the written items indeed require the execution of those
tasks. The content validity of the test is then satisfactory to the extent that such experts agree that these two requirements have been met.

The above-mentioned was adhered to and the pretesting of the questionnaire was performed with a representative group of 16% of the sample group, consisting of senior managers in the following specialised fields:

- Risk management – 3.
- Operational risk management – 4.
- Internal Audit – 2.
- Line management – 2.
- HR management – 1.
- Bank Payment Services – 1.
- Bank consultants – 2.

During the pretesting, the respondents firstly completed the questionnaire and then a diagnostic questionnaire and commentary notes (see Annexure C).

The following results indicate the validity of the research and the questionnaire:

- All the respondents agreed that all the questions were totally applicable to operational risk management. This indicated that the selected items adequately represented the area of performance about which inferences were made; and
- All the respondents indicated that they understood the intended use of the questionnaire.

The pretesting also indicated the following:
There was no negative feedback on the understandability of the questions;

- The questionnaire highly motivated the respondents to complete it;

- The instructions for completing the questionnaire were clear;

- The sequence of the questions was logical and easy to follow;

- The Likert-type scale to indicate the answers of the respondents was adequate and easy to follow;

- The average time taken to complete the questionnaire was 15 to 20 minutes; and

- Those respondents who had to complete the questionnaire electronically experienced no problems in doing so and returning it according to the instructions.

According to the above-mentioned results there were no negative comments on the questionnaire and according to the writer there are no similar questionnaires available to which a comparison can be made. The questionnaire may, therefore, be regarded as being valid, based on the results of the pretest.

4.5.4.2. Reliability

For the purpose of this study, the split-half method was selected to test the questionnaire for reliability. This was mainly as the questionnaire was sent to respondents only once as time restrictions prevented a follow-up survey exercise, which is a prerequisite of the test-retest method. Therefore, the questionnaire was divided into two equal halves by putting the responses (of the pretest) to the odd numbered questions in one pile; and the responses to the even numbered questions in another, as suggested by Hussey and Hussey (1997:173). The arithmetic mean (X) of the two groups was subsequently calculated and compared
to check for internal consistency. The results of this test, depicted in table 4.3, show an internal consistency between the two groups. The *Spearman’s Correlation Coefficient*, determined by the Statplus Analysis Programme (Berk & Carey 2000:321), for the two sets of data is 0.662932. According to the critical values of the *Spearman’s Correlation* tables, this result is significant at the 1% level, which means there is a high correlation between the two sets of data, confirming the reliability of the questionnaire for the purposes of this study.

<table>
<thead>
<tr>
<th>Question</th>
<th>X</th>
<th>Question</th>
<th>X</th>
<th>Question</th>
<th>X</th>
<th>Question</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.789</td>
<td>27</td>
<td>3.891</td>
<td>2</td>
<td>3.391</td>
<td>28</td>
<td>3.723</td>
</tr>
<tr>
<td>3</td>
<td>3.169</td>
<td>29</td>
<td>3.975</td>
<td>4</td>
<td>3.3</td>
<td>30</td>
<td>4.071</td>
</tr>
<tr>
<td>5</td>
<td>3.428</td>
<td>31</td>
<td>3.652</td>
<td>6</td>
<td>3.479</td>
<td>32</td>
<td>4.75</td>
</tr>
<tr>
<td>7</td>
<td>4.312</td>
<td>33</td>
<td>4.812</td>
<td>8</td>
<td>3.812</td>
<td>34</td>
<td>4.25</td>
</tr>
<tr>
<td>9</td>
<td>3.453</td>
<td>35</td>
<td>4.687</td>
<td>10</td>
<td>3.25</td>
<td>36</td>
<td>4.5</td>
</tr>
<tr>
<td>11</td>
<td>3.25</td>
<td>37</td>
<td>4.052</td>
<td>12</td>
<td>3.021</td>
<td>38</td>
<td>3.729</td>
</tr>
<tr>
<td>13</td>
<td>2.875</td>
<td>39</td>
<td>3.843</td>
<td>14</td>
<td>2.734</td>
<td>40</td>
<td>4.5</td>
</tr>
<tr>
<td>15</td>
<td>3.75</td>
<td>41</td>
<td>4.25</td>
<td>16</td>
<td>3.771</td>
<td>42</td>
<td>4.312</td>
</tr>
<tr>
<td>17</td>
<td>4.187</td>
<td>43</td>
<td>4.687</td>
<td>18</td>
<td>4.625</td>
<td>44</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>4.063</td>
<td>45</td>
<td>4.312</td>
<td>20</td>
<td>3.687</td>
<td>46</td>
<td>4.5</td>
</tr>
<tr>
<td>21</td>
<td>3.937</td>
<td>47</td>
<td>3.75</td>
<td>22</td>
<td>3.104</td>
<td>48</td>
<td>3.75</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
<td>49</td>
<td>3.458</td>
<td>24</td>
<td>2.854</td>
<td>50</td>
<td>3.687</td>
</tr>
<tr>
<td>25</td>
<td>3.125</td>
<td></td>
<td>95.707</td>
<td>26</td>
<td>3.906</td>
<td></td>
<td>94.697</td>
</tr>
</tbody>
</table>

*Spearman’s Correlation Coefficient* = 0.662932  
*(n = 16; critical value 1%)*


4.6. **Statistical Analysis**

Reid (1987:10) states that statistical techniques may aid the researcher in three important respects, namely:

- Measurement;
- Comparison; and
- Control of uncertainty.

Zikmund (1997:448) states that there are two applications of statistics, namely:

- **Descriptive statistics**, which describe the characteristics of the population or sample; and
- **Inferential statistics**, which are used to make an inference about a population of a sample.

According to Reid (1987:42), statistical procedures may be categorised as follows:

- **Descriptive Statistics**. These are techniques which enable the researcher to undertake the first task of analysis, that is, the measuring, ordering and summarising data. It basically describes the characteristics of a sample or population in terms of one variable;
- **Inductive Statistics**. The main aims of inductive statistics are to assist the researcher in the production of a representative sample and to enable the researcher to assess how representative a sample is. They are also known as **inferential statistics**; and
- **Multivariate Statistics**. Most social scientific enquiries are concerned not just with description, but with the relationship between variables. Bivariate data deals with two variables, while multivariate data deals with more than two variables.

According to Zikmund (1997:566), there are a number of factors which will determine the appropriate statistical techniques to assist the researcher in interpreting data:
The type of question to be answered. The type of question the researcher is attempting to answer is a consideration in the choice of a statistical technique. For example, a researcher may be concerned about the central tendency of a variable or the distribution of that variable. The choice of research design and the type of data to be collected should indicate the method of statistical analysis.

The number of variables. The number of variables that will be simultaneously investigated is a primary consideration in the choice of statistical techniques. A researcher who is interested in only the average number of times a prospective homebuyer, for example, visits financial institutions to shop for interest rates, concentrates on investigating only one variable at a time. Univariate data analysis is conducted when the researchers wish to generalise from a sample about one variable at a time. Statistically describing the relationship between two variables at one time, such as the relationship between gross national product and sales volume, requires bivariate data analysis. Multivariate data analysis is the simultaneous investigation of more than two variables, for example, predicting sales volumes on the basis of advertising, expenditure and other variables, such as, gross national product and number of people in the sales area. Leedy (1993:250) describes the above as follows:

- Univariate data involves one variable within a population. All variables are held constant except the one being studied.
• **Bivariate** data contains two variables. Studies that measure areas for each individual within a certain population are of this type.

• **Multivariate** data contains a number of variables that are usually isolated and then studied by the multivariate analysis technique.

• **The scale of measurement.** The scale of measurement on which the data is based or the type of measurement reflected in the data, determines the permissible statistical technique and the appropriate empirical operation that may be performed. Table 4.4 indicates the measures of central tendency and dispersion permissible with each type of measurement scale.

**Table 4.4: Measures of Central Tendency and Dispersion Permissible with Each Type of Measurement Scale**

<table>
<thead>
<tr>
<th>Type of Scale</th>
<th>Measure of Central Tendency</th>
<th>Measure of Dispersion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal</td>
<td>Mode</td>
<td>None</td>
</tr>
<tr>
<td>Ordinal</td>
<td>Median</td>
<td>Percentile</td>
</tr>
<tr>
<td>Interval or Ratio</td>
<td>Mean</td>
<td>Standard distribution</td>
</tr>
</tbody>
</table>

Source: Zikmund (1997:567)

Leedy (1993:262) states that if data is expressed as numerical values, then statistics may assist you in four ways, namely:

• It may indicate the central point around which the data revolve;

• It may indicate how broadly the data are spread;
• It may show the relationship of one kind of data to another kind of data; and
• It may provide certain techniques to test the degree to which the data conform to or depart from the expected operations of the law of chance or approximate and anticipated standard.

According to Bolch and Huang (1974:64), there are two broad classes of statistical inference, namely parametric and nonparametric. Parametric statistical inference is generally the more "powerful" of the two when the assumptions, which underpin the model, are satisfied. In nonparametric inference less strict assumptions about specific configuration of the population distribution are needed. A clear-cut advantage of some nonparametric techniques is their ability to handle problems when the measurement level is only on a nominal or ordinal scale. This is confirmed by Hayslett (1995:168) who also mentions that there are two important advantages of nonparametric tests, namely, they do not require many assumptions and they are relatively quick and easy to apply, requiring few computations. Similarly, Cooper and Emroy (1995:469) state that nonparametric tests do not require stringent assumptions about population distributions and are useful with less powerful nominal and ordinal measures.

Leedy (1993:260) states that statistics divide qualitatively into parametric and nonparametric statistics. Parametric and nonparametric statistics refer to the two major groupings of statistical procedures. The major distinction between these two groups of procedures lies in the underlying assumptions about the data to be analysed. When the data are interval- or ratio-scaled and the sample size is large, parametric statistical procedures are appropriate. Data analysis of both nominal and ordinal scales typically uses nonparametric statistical tests.
As this study mostly concerns two variables, the bivariate analyses is used. This allows the effects of two variables to be considered at one time. According to Zikmund (1997:586), bivariate statistics comprises tests of differences or measures of association between two variables at one time. As the questionnaire for this study comprises an ordinal scale, the Spearman correlation coefficient is used to measure the significance of the two variables (see paragraph 4.4.2).

As the questionnaire comprises an ordinal scale, the statistical analysis lends itself more to the descriptive analysis. This is, according to Zikmund (1997:533), the transformation of raw data into a form that will make it easy to understand and interpret by rearranging, ordering and manipulating it to provide descriptive information.

In order to interpret the data, the arithmetic mean forms an important part of the analysis. The Likert scale, which is used to determine the attitude of the respondents, is used in accordance with the arithmetic mean to reach conclusions regarding the various responses.

The questionnaire comprises three sections which were statistically analysed as follows:

- **Section 1**: The demographic data, which will be used to distinguish between the respondents in terms of the type of bank, portfolio of respondents, years of experience and location;

- **Section 2**: This data indicates the current situation regarding operational risk management within the various banks and will
serve as the first variable during the computation of the Spearman correlation coefficient to determine the level of significance; and

- **Section 3:** This data determines what the approach of the banks towards operational risk management should be according to the experience and knowledge of senior managers in the banking industry. It will serve as the second variable during the computation of the Spearman correlation coefficient to determine the level of significance.

Figure 4.1 depicts a diagrammatical illustration of the research methodology used for this research.
Figure 4.1: Diagrammatical Illustration of the Research Methodology for this Study

Analytical Survey Method

Structured Questionnaire

Ordinal Type Scale
(Attitude/Viewpoints)

Pre-test

Validity
Content Validity Method
Accuracy with which an instrument measures the factors

Rating Technique
Summated Ratings Method:
Likert Type Scale – (5 point scale)

Reliability
Split-half Method
Checking for consistency when a measure contains a large number of items

Spearman's correlation coefficient

STATISTICAL ANALYSIS
Inferential Statistics

Nonparametric Analysis

Bivariate Data

Descriptive Data Analysis

Inferential Data Analysis

Arithmetic mean (\(\bar{X}\))
Determine the central tendency of respondents

Spearman's correlation coefficient
Determine the significance and confidence level of the response
4.7. Conclusion

Based on the aforementioned theoretical discussion on research design, a questionnaire was developed to gather the data from the identified respondents. The questionnaire was pretested and was accepted in terms of the methods used to determine its validity and reliability.

Subsequently, the various statistical approaches were researched in order to determine the most appropriate statistical methodology to use during the analysis of the data acquired through the questionnaire.

The next chapter focuses on the interpretation of the empirical research results by means of the identified statistical methodologies. The results of the statistical analysis are integrated with the theories and concepts identified during the literature study, to develop a structured approach to operational risk management in a banking environment.
CHAPTER 5

STATISTICAL ANALYSIS OF RESULTS

5.1. Introduction

In chapter four the research and statistical methodology as well as the development of the questionnaire used for this research were described.

This chapter deals with the analysis and the interpretation of the data gathered through the questionnaire. It comprises a summary of the demographic data that will form an integral part of the descriptive analysis; the grouping of the questions to simplify their statistical analysis; and the statistical analysis of the data from the completed questionnaires.

5.2. Demographic Data

5.2.1. Responses Received from Local and Foreign Banks

A total of 94 questionnaires were sent to the banks listed in chapter 4. The returned questionnaires totaled 63, which represent a 67% response rate. Of the questionnaires returned, 46 were returned from respondents from local banks, which represents 73.1% of the returned questionnaires. Seventeen questionnaires were returned from foreign banks, representing 26.9% of the returned questionnaires (see figure 5.1).
Figure 5.1: Response Rate of Foreign and Local Banks

<table>
<thead>
<tr>
<th>Distributed</th>
<th>Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Pie Chart" /></td>
<td><img src="image2.png" alt="Pie Chart" /></td>
</tr>
</tbody>
</table>

- **Distributed:**
  - Foreign: 26 (27.6%)
  - Local: 62 (72.4%)

- **Returned:**
  - Foreign: 17 (26.9%)
  - Local: 48 (73.1%)

5.2.2. **Different Types of Banks that Responded**

The different types of banks from which responses were received are depicted in figure 5.2. It is evident that all types of banks have responded to the questionnaire, although they are not equally represented. “All banks” in figure 5.2 depict banking groups that have retail, investment, commercial and merchant bank divisions. This category of banks improves the percentage representation of all types of banks in the sample. It can therefore be deduced that all types of banks are well represented in the sample and findings may thus be generalised to be relevant to all types of banks, unless significant differences exist between the responses of banks included in the sample.

Figure 5.2: Response from the Types of Banks

<table>
<thead>
<tr>
<th>Foreign</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3.png" alt="Pie Chart" /></td>
<td><img src="image4.png" alt="Pie Chart" /></td>
</tr>
</tbody>
</table>

- **Foreign:**
  - Retail: 18 (33%)
  - Investment: 6 (11%)
  - Commercial: 6 (11%)
  - Merchant: 12 (22%)
  - All Banks: 58 (100%)

- **Local:**
  - Retail: 11 (22%)
  - Investment: 4 (8%)
  - Commercial: 5 (10%)
  - Merchant: 1 (22%)
  - All Banks: 26 (52%)

- The values are percentages of the respective categories.
5.2.3. **Occupation/Positions of Persons that Completed Questionnaires**

The specific occupations/positions of the respondents (see figure 5.3) indicate that mostly risk managers (50%) completed the questionnaire. From the large percentage of risk managers who completed the questionnaire, it can be deduced that risk management is being regarded as an overall responsibility rather than consisting of separate specialised areas. Only 20.5% of the questionnaires were completed by operational risk managers. This is an indication that operational risk management in many banks is still not a recognised risk area. The number of internal auditors (16%) that completed the questionnaire is a further indication that operational risk management is in some instances still regarded as part of the internal audit function of banks.

**Figure 5.3:** Specific Occupations/Positions of the Respondents that Completed the Research Questionnaires

![Pie charts showing occupation/positions of respondents](chart.png)

5.2.4. **Experience of Persons that Completed the Questionnaires**

The practical experience in risk management of persons who have completed the questionnaire is graphically depicted in figure 5.4. As the majority of the respondents fall in the categories of 5 – 7 and 8 – 10 years of banking experience,
it can be inferred that the questionnaire was completed by mostly experienced managers.

Figure 5.4: Years of Experience of the Respondents

<table>
<thead>
<tr>
<th>Foreign</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>18%</td>
<td>9%</td>
</tr>
<tr>
<td>12%</td>
<td>7%</td>
</tr>
<tr>
<td>12%</td>
<td>4%</td>
</tr>
<tr>
<td>29%</td>
<td>2%</td>
</tr>
<tr>
<td>29%</td>
<td>13%</td>
</tr>
<tr>
<td>More than 16 years</td>
<td>More than 16 years</td>
</tr>
</tbody>
</table>

The following section deals with the grouping of the questions contained in the questionnaire.

5.3. Grouping of Questions

To simplify the statistical analysis, questions with a similar underlying construct are grouped together into eight descriptive items (refer to table 5.1). The grouping of the items ensures that the various questions relating to a specific topic are combined. This will contribute to a more structured analysis of the research data.
Table 5.1: Grouping of Questions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Questions</th>
<th>Construct</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk Types</td>
<td>1 &amp; 2</td>
<td>Risk types</td>
</tr>
<tr>
<td>2</td>
<td>Operational risk factors and definition</td>
<td>2 &amp; 27, 3 &amp; 28, 4 &amp; 29, 5 &amp; 30, 6 &amp; 31, 8 &amp; 33</td>
<td>Operational risk factors</td>
</tr>
<tr>
<td>3</td>
<td>Operational risk management process</td>
<td>7 &amp; 32, 9 &amp; 34, 10 &amp; 35, 11 &amp; 36</td>
<td>Risk management process</td>
</tr>
<tr>
<td>4</td>
<td>Operational risk identification</td>
<td>12 &amp; 37, 15 &amp; 40</td>
<td>Methods to identify risk Risk identification</td>
</tr>
<tr>
<td>5</td>
<td>Operational risk measurement</td>
<td>13 &amp; 38, 14 &amp; 39</td>
<td>Qualitative methods Quantitative methods</td>
</tr>
<tr>
<td>6</td>
<td>Operational risk control</td>
<td>16 &amp; 41</td>
<td>Control measures</td>
</tr>
<tr>
<td>7</td>
<td>Operational risk structure</td>
<td>17 &amp; 42, 18 &amp; 43, 19 &amp; 44, 20 &amp; 45, 21 &amp; 46</td>
<td>Operational risk structure  Reporting lines Internal audit Delegation Responsibilities</td>
</tr>
<tr>
<td>8</td>
<td>Operational risk financing</td>
<td>22 &amp; 47, 23 &amp; 48, 24 &amp; 49, 25 &amp; 50</td>
<td>Risk financing techniques Capital charge for operational risk Approaches to assess operational risk Capital charge and Basel Committee</td>
</tr>
</tbody>
</table>

The following section deals with the statistical analysis of the responses contained in the completed questionnaires.

5.4. Statistical Analysis of the Data from the Completed Questionnaires

Each item, identified in the above table, is discussed separately in the ensuing sections.
5.4.1. Item 1: Risk Types

The aim of this item is to determine which risk types are currently being managed as primary risk types by banks and, secondly, to determine whether the respondents regard the current situation as optimal or not. It also indicates the approach by various banks to operational risk management as a primary risk type.

The risk types that were included in the questionnaire and the applicable responses are as follows:

- **Credit Risk.** According to the respondents' rating of credit risk as a primary risk type to be managed by a bank, there is no doubt that it is regarded as the most important risk type. Ninety percent of the respondents rated it as a primary risk type currently being managed by banks. This percentage increased to 97% according to their response to how it should be managed. These viewpoints of the respondents are also congruent with the literature study as credit risk forms an integral part of a bank’s core business. It is thus evident that credit risk is a primary risk type of a bank.

- **Market Risk.** Eighty-one percent of the respondents indicated that their banks manage this risk type as a primary risk. According to the respondents' recommendations, 94% indicated that it should be managed by a bank as a primary risk type. Market risk evolves when a bank takes trading, banking and investment positions which may also be regarded as a bank’s primary business activities. It can, therefore, be concluded that market risk is also a primary risk type of a bank.
- **Liquidity Risk.** This risk type was identified by 60% of the respondents as currently being managed as a primary risk type, while 94% indicated that it should be managed as a primary risk type. Liquidity risk is described as a bank’s ability to meet deposit withdrawals and provide for the legitimate credit needs of its customers. It is clear that this risk type is also coupled to the crucial functions of a bank and can, therefore, be regarded as one of the primary risk types of a bank.

- **Operational Risk.** Fifty-nine percent of the respondents indicated that operational risk is being managed as a primary risk type by their banks, while all the respondents rated it as a primary risk that should be managed by banks. It can, therefore, be deduced that although not all the banks are currently managing it as a primary risk, operational risk is seen by most banks as a primary risk factor and many banks are in the process of establishing it accordingly. Thus, it can be concluded that operational risk should be regarded as a primary risk type of a bank.

- **Interest-rate Risk.** Although this risk type was rated by 52% of the respondents as an important risk type, only 17% of the respondents regarded it as a primary risk type currently being managed by their banks, although 68% viewed it as a primary risk that should be managed by banks. As this risk type also concerns a bank’s earnings, expenses and the economic value of its assets, it may also be regarded as a risk which relates to a bank’s primary business. It can, therefore, be deduced that interest-rate risk should also be regarded as a primary risk type of a bank.

- **Country Risk.** This risk type was rated by only 54% of the respondents as a primary risk type that should be managed by a bank. As this risk type is often related to credit and market risk, it
may be deduced that these two risk types address some of the exposures of country risk. This risk type is not currently regarded as a primary risk type that a bank should be managing.

- **Legal Risk.** Legal risk is rated by only 46% of the respondents as being a primary risk type that should be managed by a bank. It can, therefore, be deduced that, although legal risk is an important risk type, it should not be regarded as a primary risk type of a bank.

- **Reputation Risk.** As the success of banks depend to a certain degree on their customer base, this risk type is also becoming an important management issue, although only 17% of the respondents rated it as currently being managed as a primary risk type by banks. Sixty-five percent of the respondents, however, indicated that it is a primary risk type that should be managed by banks. It can be deduced, however, that this risk type has no direct relation to a bank's primary business such as, for example, credit and market risk. Therefore, it can be currently regarded as a secondary risk type of a bank.

The response shows that the following percentage of respondents indicated the risks as primary risk types of banks:

- Credit risk - 97%.
- Market risk - 94%.
- Liquidity risk - 94%.
- Operational risk - 100%.
- Interest-rate risk - 68%.
- Country risk - 54%.
- Legal risk - 46%.
• Reputation – risk 65%.

Thus, the average percentage is 77%. For the purposes of this study a 10% deviation on the average percentage was accepted as the cut-off point (67%) to be classified as a primary risk. Therefore, according to the above, credit, market, liquidity, operational and interest-rate risks are viewed as the primary risk types of a bank. Reputation, legal and country risks are also regarded as important risk types, but not as important as the former. As an integrated relationship may exist between operational risks and the other primary risks, it may be deduced that this aspect should form part of a structured approach to operational risk management in a banking environment.

According to the arithmetic mean of the rating of the various risk types (see figure 5.5) it is evident that the credit, market, liquidity, interest-rate and operational risks are regarded as the primary risk types that should be managed by banks. On the other hand, country, reputation and legal risks are generally not rated as primary risk types.

The percentage variance (see figure 5.6) of how the risk types are currently being managed opposed to how they should be, is the highest for interest-rate risk (33.7%), operational risk (27.9%) and reputation risk (21.8%). It may be deduced that these risk types require more dedicated attention or are in the process of being developed as primary risk types of banks. The risk types which show a minimum variance between how they are currently managed opposed to how they should be managed are credit, market and liquidity risk. It may be deduced that these latter risk types are already being managed on an acceptable level by banks.
Figure 5.5: Arithmetic Mean – Current and Recommended Classification of Primary Risk Types

Although the respondents rated operational risk as a primary risk type of a bank, they also indicated that it is one of the risk types that still needs to be refined to reach an optimum level of acceptance as a primary risk type. This statement is also supported by the literature study where it is mentioned that operational risk is not a clearly defined concept, although most banks recognise it as an important aspect of risk management (see chapter 3 paragraph 3.1).
Figure 5.7 depicts the Spearman correlation coefficient at a 95% level of significance. Two of the individual scores (country risk and reputation risk) exceed the critical value of 0.738, indicating a significant difference between the current and the recommended classification of these risk types. It may be deduced that country and reputation risks are not regarded as primary risk types of banks. The remaining risk types, however, indicate no significant differences, confirming their importance as primary risk types of a bank. Legal risk also falls in this category. The reason may be the minimal difference between the current and recommended rating (2%), indicating that the respondents are satisfied with how legal risk is currently being classified and managed as a secondary risk type.

Figure 5.7: Spearman Correlation Coefficient – Correlation of Current and Recommended Classification of Primary Risk Types

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Correlation Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit</td>
<td>* -0.2682</td>
</tr>
<tr>
<td>Market</td>
<td>* -0.1037</td>
</tr>
<tr>
<td>Liquidity</td>
<td>* 0.2617</td>
</tr>
<tr>
<td>Interest Rate</td>
<td>* 0.6497</td>
</tr>
<tr>
<td>Country</td>
<td>* 0.9219</td>
</tr>
<tr>
<td>Reputation</td>
<td>* 0.7623</td>
</tr>
<tr>
<td>Legal</td>
<td>* -0.9155</td>
</tr>
<tr>
<td>Operational</td>
<td>* 0.5947</td>
</tr>
</tbody>
</table>

Significance at 5% acceptance level 0.738

5.4.2. Item 2: Operational Risk Factors and Defining Operational Risk

The aim of this item is, firstly, to determine to what extent banks currently recognise the primary operational risk factors identified in the literature study
and to what degree the situation differs from what they believe it should be. Secondly, to determine which exposures, relating to these operational risk factors, are currently being recognised by banks and the extent to which they should be managed as part of the underlying risk factors of operational risk. Finally, this section focuses on a formal definition of operational risk by determining whether banks have formulated such a definition and whether they regard a formal definition of operational risk as imperative.

5.4.2.1. Primary Operational Risk Factors

The primary risk factors of operational risk were identified as people, processes, systems and external events in the literature study. The response concerning how important banks currently regard these primary operational risk factors, as opposed to how important they should be, is depicted in table 5.2.

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td>0</td>
</tr>
<tr>
<td>Processes</td>
<td>0</td>
</tr>
<tr>
<td>Systems</td>
<td>0</td>
</tr>
<tr>
<td>External events</td>
<td>0</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td>0</td>
</tr>
<tr>
<td>Processes</td>
<td>0</td>
</tr>
<tr>
<td>Systems</td>
<td>0</td>
</tr>
<tr>
<td>External events</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 5.2: Response – Current and Recommended Rating of the Primary Risk Factors of Operational Risk
People. Most respondents indicated that people risk is currently regarded and managed as a primary risk factor of operational risk by banks. All the respondents, however, indicated that it should be a primary risk factor of operational risk.

Processes. The majority of the respondents indicated that this factor is currently regarded and managed as a primary risk factor of operational risk by banks, while 98% of the respondents indicated that it should be regarded a primary risk factor of operational risk.

Systems. Seventy-nine percent of the respondents indicated that systems were a primary factor of operational risk currently managed by banks, while 81% indicated that it should be a primary factor of operational risk.

External Events. Although external events were identified as the fourth primary factor of operational risk in the literature study, only 43% of the respondents indicated that it is currently regarded and managed as such by banks. Seventy-three percent of the respondents, however, are of the opinion that it should be a primary factor of operational risk.

Although the responses vary, the view of most of the respondents is that people, processes, systems and external events should be regarded and managed as primary risk factors of operational risk.

The arithmetic means for the current importance organisations place on the primary risk factors of operational risk versus the recommendations on the actual importance of these factors are depicted in figure 5.8.
Figure 5.8: Arithmetic Mean – Current and Recommended Importance and Implementation of Primary Operational Risk Factors

The arithmetic means indicate that in general, only the people factor is currently implemented and managed to a high degree as an operational risk factor. The other factors are implemented and managed to a fair degree. All the factors are, however, highly rated as primary operational risk factors and should form an integral part of a structured approach to operational risk management. The process factor earned the highest average score (4.7), indicating that it is the most important factor that should be managed during an operational risk management process.

The percentage variance between the current and recommended importance of the factors is depicted in figure 5.9. The processes factor has the highest variance (21.76%), followed by the external events factor (20%). As such, it can be deduced that, although rated as primary operational risk factors, the management approach to these two factors has to be greatly improved to achieve the desired level of management. The results also indicate that even though the people factor is currently the best managed, it also requires improvement. The systems factor is the only factor where the perceived current and recommended importance differ very little (0.51%).
Figure 5.9: Percentage Variance – Current and Recommended Importance and Management of Primary Operational Risk Factors

Figure 5.10 depicts the *Spearman correlation coefficient* at a 95% confidence level. This indicates no significant difference between the current and recommended implementation and management of the primary risk factors (people, processes, systems and external events) of operational risk. As such, it can be deduced that people, processes, systems and external events should, based on the responses, all be viewed as primary risk factors of operational risk. The responses to the open-ended questions revealed no additional primary risk factors.

**Figure 5.10: Spearman Correlation Coefficient – Correlation of Current and Recommended Implementation and Management of Primary Operational Risk Factors**

<table>
<thead>
<tr>
<th></th>
<th>People</th>
<th>Processes</th>
<th>Systems</th>
<th>External Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>0.0386</td>
<td>* 0.3598</td>
<td>0.0802</td>
<td>* 0.0162</td>
</tr>
<tr>
<td><em>Significance at 5% critical value</em></td>
<td>0.811</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.4.2.2. Operational Risk Exposures

Each primary risk factor comprises a number of sub-factors or exposures that should be managed. The research, therefore, determined to what extent banks currently recognise various exposures underlying people, processes, systems and external events and to what degree the current recognition differs from exposures which should be regarded as part of an operational risk management process.

*People Exposures.* The sub-factors of the people exposures that were identified in the literature study are the following:

- Incompetence.
- Negligence.
- Human error.
- Low morale.
- High staff turnover.
- Fraudulent activities.
- Lack of training.

The response in table 5.3 indicates the view of the respondents on the current recognition these sub-factors enjoy by banks opposed to the recommended recognition they should enjoy.

<p>| Table 5.3: Response – Current and Recommended Recognition of People Exposure Sub-Factors |
|---------------------------------|-----|-----|-----|-----|-----|
| Current                        | Scale |
| Incompetence                   | 0   | 24% | 62% | 14% | 0   |
| Negligence                     | 0   | 13% | 71% | 16% | 0   |</p>
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>6%</th>
<th>75%</th>
<th>19%</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human error</td>
<td>0</td>
<td>20%</td>
<td>48%</td>
<td>32%</td>
<td>0</td>
</tr>
<tr>
<td>Low morale</td>
<td>0</td>
<td>31%</td>
<td>56%</td>
<td>13%</td>
<td>0</td>
</tr>
<tr>
<td>High staff turnover</td>
<td>0</td>
<td>13%</td>
<td>10%</td>
<td>56%</td>
<td>21%</td>
</tr>
<tr>
<td>Fraudulent activities</td>
<td>13%</td>
<td>33%</td>
<td>27%</td>
<td>27%</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recommended**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>22%</th>
<th>57%</th>
<th>21%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incompetence</td>
<td>0</td>
<td>0</td>
<td>24%</td>
<td>73%</td>
<td>3%</td>
</tr>
<tr>
<td>Negligence</td>
<td>0</td>
<td>0</td>
<td>40%</td>
<td>52%</td>
<td>8%</td>
</tr>
<tr>
<td>Human error</td>
<td>0</td>
<td>0</td>
<td>17%</td>
<td>73%</td>
<td>10%</td>
</tr>
<tr>
<td>Low morale</td>
<td>0</td>
<td>0</td>
<td>19%</td>
<td>57%</td>
<td>24%</td>
</tr>
<tr>
<td>High staff turnover</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10%</td>
<td>90%</td>
</tr>
<tr>
<td>Fraudulent activities</td>
<td>0</td>
<td>0</td>
<td>9%</td>
<td>56%</td>
<td>35%</td>
</tr>
</tbody>
</table>

The respondents rated fraudulent activities as the current most important sub-factor of people exposure, while low morale and the lack of training were viewed to be second and third in terms of importance. As respondents from the local banks outnumber those representing foreign banks, it can be deduced that the current political situation in South Africa plays a dominant role on the rating of these sub-risks. As South African banks are in a process of transformation, it is understandable that a lack of training and low morale, for example, will be focus areas for management. Fraudulent activities, as a sub-factor of people exposure, will always be one of the focus areas for management, as the business of a bank is always vulnerable to internal fraud. Therefore, this sub-risk should be regarded as a continuous focus area for risk management and control.

Ninety percent of the respondents rated fraudulent activities as the most important sub-factor of people exposures that a bank should be managing. This indicates and confirms the importance of this sub-factor. Of the other sub-factors, the lack of training (35%) and a high staff turnover (24%) are also rated as
important concerns that should be addressed by management. Low morale of the staff, however, is only recognised by 10% of the respondents as an important sub-factor. As such, it can be deduced that the high current rating of this sub-factor is a short-term concern which should become less important if managed correctly. It seems that the current importance of high staff turnover differs vastly from its recommended importance. It can be deduced that high staff turnover can be regarded as a concern to the respondents and as such, should be managed as an important sub-factor of operational risk.

The arithmetic means of the current and recommended recognition of people exposures is depicted in figure 5.11. According to this analysis, the sub-risks that are currently the most recognised and managed as sub-factors of people exposure are fraudulent activities (3.84), human error (3.13) and low morale (3.11). Lack of training, on the other hand, is currently recognised and managed as the least important sub-factor, but recommended to be the second most important sub-factor after fraudulent activities. High staff turnover is identified as the third most important sub-factor that a bank should manage. The respondents also identified the remaining sub-factors as important elements of people exposures, but to a lesser degree than those mentioned above.

Figure 5.11: Arithmetic Mean – Current and Recommended Recognition of People Exposure Sub-Factors
The percentage variance between the current and recommended recognition of the people exposure sub-factors is indicated in figure 5.12. It illustrates that lack of training (58.6%), high staff turnover (44.1%) and incompetence (37.2%) have the highest variance between the current and recommended situations. As previously mentioned, high staff turnover and lack of training are also perceived as two of the three most important sub-factors of people exposure. As such, it can be deduced that they should be regarded as key focus areas during the risk management process. It can also be concluded that if the lack of training is adequately managed, the level of training should improve and consequently have a positive effect on the other sub-factors such as incompetence, human error and negligence.

Figure 5.12: Percentage Variance – Current and Recommended Recognition of People Exposure Sub-Factors

The Spearman correlation coefficients for the sub-factors of the people exposures are depicted in figure 5.13.
Figure 5.13: *Spearman Correlation Coefficient* – Correlation of Current and Recommended Recognition of People Exposure Sub-Factors

<table>
<thead>
<tr>
<th>Factor</th>
<th>Correlation Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incompetence</td>
<td>* 0.3939</td>
</tr>
<tr>
<td>Negligence</td>
<td>* 0.0882</td>
</tr>
<tr>
<td>Human error</td>
<td>* 0.1349</td>
</tr>
<tr>
<td>Low morale</td>
<td>* 0.0673</td>
</tr>
<tr>
<td>High staff turnover</td>
<td>* 0.0598</td>
</tr>
<tr>
<td>Fraudulent activities</td>
<td>* 0.0633</td>
</tr>
<tr>
<td>Lack of training</td>
<td>* -0.331</td>
</tr>
</tbody>
</table>

Significance at 5% critical value 0.666

At a 95% confidence level, there are no significant differences between the current and recommended ratings of the people exposure sub-factors. As such, it can be deduced that all the above-mentioned sub-risks are recognised as people exposures that should be managed during an operational risk management process. Although there were no additional sub-risks listed in the open-ended questions, it should be kept in mind that the above-mentioned list is not exhaustive and could change according to changing circumstances.

*Process Exposures.* The process exposures that were identified in the literature study are:

- Errors in procedures.
- Execution error.
- Documentation errors.
- Product complexity.
- Security risks.

The view of the respondents on the current and the recommended recognition of the exposures of processes as a primary factor of operational risk are depicted in table 5.4.

Table 5.4: Response – Current and Recommended Recognition of Process Exposure Sub-Factors

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors in procedures</td>
<td>0</td>
<td>0</td>
<td>24%</td>
<td>62%</td>
<td>14%</td>
<td></td>
</tr>
<tr>
<td>Execution errors</td>
<td></td>
<td>0</td>
<td>13%</td>
<td>52%</td>
<td>30%</td>
<td>5%</td>
</tr>
<tr>
<td>Documentation errors</td>
<td></td>
<td>0</td>
<td>13%</td>
<td>44%</td>
<td>43%</td>
<td>0</td>
</tr>
<tr>
<td>Product complexity</td>
<td></td>
<td>13%</td>
<td>8%</td>
<td>44%</td>
<td>35%</td>
<td>0</td>
</tr>
<tr>
<td>Security risks</td>
<td>0</td>
<td>0</td>
<td>35%</td>
<td>65%</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>1</td>
</tr>
<tr>
<td>Errors in procedures</td>
<td>0</td>
</tr>
<tr>
<td>Execution errors</td>
<td>0</td>
</tr>
<tr>
<td>Documentation errors</td>
<td>0</td>
</tr>
<tr>
<td>Product complexity</td>
<td>0</td>
</tr>
<tr>
<td>Security risks</td>
<td>0</td>
</tr>
</tbody>
</table>

The respondents rated errors in procedures as the most important process exposure, while execution errors and security risks were respectively identified as the second and third most important sub-factors currently recognised by banks. Although documentation errors and product complexity were also rated as sub-factors of process exposures, they are rated as less important in terms of existing management practices. In terms of the recommended recognition, errors in procedures and execution errors remain the two most important sub-factors.
Although the importance ratings of documentation errors, security risk and product complexity are higher than their existing level of recognition, they are still viewed as less important sub-factors of process exposures. It can, therefore, be deduced that errors in procedures and execution should be the focus of management during the operational risk management process. The other factors, however, should not be neglected.

The arithmetic means for the current and recommended recognition of the process exposure sub-factors are depicted in figure 5.14. The arithmetic means indicate that errors in procedures are currently recognised as the most important sub-factor of process exposures, followed closely by all the other sub-factors. From the average high ranking of the sub-risks, it can be deduced that all of them are currently recognised as sub-factors of process exposures. In terms of the recommended recognition, errors in procedures are again regarded as the most important sub-factor, with errors in execution the second most important. This finding emphasises that errors in procedures and errors in execution are the most important sub-factors that should be recognised and managed during an operational risk management process.

Figure 5.14: Arithmetic Mean – Current and Recommended Recognition of Process Exposure Sub-Factors
The percentage variance (see figure 5.15) between the extent to which the sub-risks are currently being recognised as opposed to their recommended recognition, indicates that product complexity (27.8%), execution errors (23.9%) and documentation errors (22.1%) need the most improvement.

**Figure 5.15: Percentage Variance – Current and Recommended Recognition of Process Exposure Sub-Factors**

The *Spearman correlation coefficients* of the sub-factors of process exposures are depicted in figure 5.16. At a 95% confidence level, there are no significant differences between the current and recommended recognition of the sub-factors of process exposures. As such, it can be deduced that all the identified sub-factors are recognised by the respondents as important factors that should be managed during an operational risk management process. Although there were no additional sub-factors identified by the open-ended questions, the above list should not be regarded as exhaustive.
Figure 5.16: *Spearman Correlation Coefficient* – Correlation of Current and Recommended Recognition of Process Exposure Sub-Factors

<table>
<thead>
<tr>
<th>Sub-Factor</th>
<th>Correlation Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors in procedures</td>
<td>* 0.1065</td>
</tr>
<tr>
<td>Execution errors</td>
<td>* 0.1191</td>
</tr>
<tr>
<td>Documentation errors</td>
<td>* -0.3754</td>
</tr>
<tr>
<td>Product complexity</td>
<td>* -0.5869</td>
</tr>
<tr>
<td>Security risks</td>
<td>* 0.23079</td>
</tr>
</tbody>
</table>

Significance at 5% critical value

*System Exposures.* The sub-factors of the system exposures that were identified in the literature study are depicted in table 5.5. According to the rating scale, the respondents rated system infiltration as currently the most recognised and managed sub-factor. Other important sub-factors that are currently recognised by banks are fraud and obsolescence of systems. The remainder of the sub-factors were rated lower, but were all recognised as sub-factors of system exposures. As such, it can be deduced that most banks currently recognise all the identified sub-factors as part of system exposures. The views of the respondents regarding the recommended recognition of these sub-factors indicates that system infiltration is the most important sub-risk, followed by fraud, system failures and information risk. The remainder of the sub-factors are also regarded as important but to a lesser degree than the above-mentioned.
Table 5.5: Response – Current and Recommended Recognition of System Exposure Sub-Factors

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td></td>
</tr>
<tr>
<td>System infiltration</td>
<td>0</td>
</tr>
<tr>
<td>System failures</td>
<td>0</td>
</tr>
<tr>
<td>Fraud</td>
<td>0</td>
</tr>
<tr>
<td>Programming errors</td>
<td>0</td>
</tr>
<tr>
<td>Information risk</td>
<td>9%</td>
</tr>
<tr>
<td>Telecommunication risk</td>
<td>10%</td>
</tr>
<tr>
<td>Obsolescence of systems</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td></td>
</tr>
<tr>
<td>System infiltration</td>
<td>0</td>
</tr>
<tr>
<td>System failures</td>
<td>0</td>
</tr>
<tr>
<td>Fraud</td>
<td>0</td>
</tr>
<tr>
<td>Programming errors</td>
<td>0</td>
</tr>
<tr>
<td>Information risk</td>
<td>0</td>
</tr>
<tr>
<td>Telecommunication risk</td>
<td>0</td>
</tr>
<tr>
<td>Obsolescence of systems</td>
<td>0</td>
</tr>
</tbody>
</table>

As such, it can be deduced that all the identified sub-factors should be recognised as part of system exposures and managed accordingly. It can also be concluded that as banks progress with, for instance, the implementation of e-commerce products, the risk exposures of, for example, system infiltration and fraud will increase. As such, the effective management of these sub-factors should form an integral part of an operational risk management process.
The arithmetic mean (see figure 5.17) confirms the importance of system infiltration as currently the most recognised sub-factor of system exposures by banks. The remainder is regarded of fair importance in terms of existing management practices. With regard to the recommended recognition and management of these exposures, the sub-factors: fraud, system failures and information risk are rated as very important; while the rest of the sub-factors are rated as fairly important. According to these ratings, therefore, it can be deduced that system infiltration, information risk and fraud are the most important sub-factors of system exposures.

Figure 5.17: Arithmetic Mean – Current and Recommended Recognition of System Exposure Sub-Factors

The percentage variance between the current recognition of the sub-factors, as opposed to their recommended recognition, is depicted in figure 5.18. According to the responses, information risk, programming errors and telecommunication
risk are the sub-factors that require the largest increases in recognition to achieve the desired level of importance.

The *Spearman correlation coefficients* for the sub-factors of system exposures are depicted in figure 5.19. At a 95% confidence level there are no significant differences between the current and recommended recognition of the sub-factors. Therefore, it can be deduced that all the identified sub-factors form, according to the respondents, an integral part of the system exposures which should be managed during an operational risk management process. Although there were no additional sub-factors identified in the open-ended questions, the identified sub-factors should not be regarded as the only sub-factors of system exposures.

**Figure 5.18: Percentage Variance – Current and Recommended Recognition of System Exposure Sub-Factors**
Figure 5.19: Spearman Correlation Coefficient – Correlation of Current and Recommended Recognition of System Exposure Sub-Factors

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System infiltration</td>
<td></td>
<td>0.1785</td>
<td></td>
</tr>
<tr>
<td>System failures</td>
<td>* -0.0732</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td>* -0.1371</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programming errors</td>
<td>* -0.0760</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information risk</td>
<td></td>
<td></td>
<td>0.4623</td>
</tr>
<tr>
<td>Telecommunication risk</td>
<td>* -0.1398</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obsolescence of Systems</td>
<td></td>
<td></td>
<td>* 0.5991</td>
</tr>
</tbody>
</table>

Significance at 5% critical value

External Event Exposures. The sub-factors of the external event exposures that were identified in the literature study, and the views of the respondents regarding the current importance assigned to it by banks, opposed to its recommended importance, are depicted in table 5.6. Money laundering is currently recognised as the most important sub-factor by banks. As such, it can be deduced that money laundering is currently an international phenomenon that affects all banks. The importance of money laundering can be furthermore substantiated by the fact that, if not prevented, it could have a substantial negative affect on a bank’s business. As such, it can be deduced that money laundering is an important sub-factor of a bank’s external exposures.

The second most important sub-factor in terms of current recognition by banks is regulatory and compliance. In this regard it can be deduced that a reason for this sub-factor’s important rating, could, for example, be the recent developments in
determining a regulatory capital charge for operational risk. As a capital charge for operational risk could affect a bank’s economic capital, this factor is currently regarded as a contentious issue that requires management’s attention. In this regard it is important that a realistic regulatory capital charge for operational risk is determined to ensure a sufficient level of strategic capital for a bank.

Table 5.6: Response – Current and Recommended Recognition of External Event Exposure Sub-Factors

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Recommended</th>
<th>0</th>
<th>14%</th>
<th>67%</th>
<th>19%</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Acts of God</td>
<td>0</td>
<td>32%</td>
<td>63%</td>
<td>5%</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>External criminal activities</td>
<td>0</td>
<td>3%</td>
<td>16%</td>
<td>78%</td>
<td>3%</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Domestic political upheaval</td>
<td>14%</td>
<td>4%</td>
<td>65%</td>
<td>17%</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Regulatory and compliance</td>
<td>0</td>
<td>0</td>
<td>17%</td>
<td>68%</td>
<td>15%</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Legal action</td>
<td>0</td>
<td>0</td>
<td>33%</td>
<td>67%</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Business environment changes</td>
<td>0</td>
<td>0</td>
<td>57%</td>
<td>43%</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Reputation risk</td>
<td>0</td>
<td>0</td>
<td>5%</td>
<td>81%</td>
<td>14%</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Strikes</td>
<td>8%</td>
<td>26%</td>
<td>49%</td>
<td>17%</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Money laundering</td>
<td>0</td>
<td>0</td>
<td>22%</td>
<td>43%</td>
<td>35%</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scale</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>0</td>
<td>14%</td>
<td>67%</td>
<td>19%</td>
<td>0</td>
</tr>
</tbody>
</table>
Although the respondents rated the current recognition of the other sub-factors lower, all the sub-factors are, to some degree, regarded as important factors of external events. Respondents identified money laundering as well as regulatory and compliance as the most important sub-factors in terms of recommended recognition. A third important sub-factor identified by respondents is external criminal activities. A possible reason for the importance of the latter sub-factor is that South African banks are experiencing increased criminal activity, for example, branch robberies and cash heists. As such, it can be deduced that it is also important for banks to regard this sub-factor as an important part of risk management.

The arithmetic means (see figure 5.20) depict the current recognition by banks of the external event sub-factors, as opposed to their recommended recognition. According to the responses, the sub-factor currently recognised as the most important is money laundering, followed by the regulatory and compliance sub-factor. As none of the other factors were discarded by the respondents, it can be deduced that all of them currently form part of external exposures that are managed by banks, although to a lesser degree. Based on the response regarding the recommended recognition of external exposures, it is found that money laundering, regulatory and compliance, external criminal activities and deterioration of reputation are regarded as the most important sub-factors that should be managed. This rating confirms the above-mentioned conclusion regarding the increase of criminal activities in South Africa. Banks should, however, keep in mind that external events are beyond their direct control, therefore the importance of these sub-factors could change overnight. For example, strikes as a factor is currently rated as an unimportant factor, but if there should be a strike involving bank employees, this factor could be regarded as the most important factor at that stage. It can, therefore be deduced that it is
important for banks to continuously monitor the developments surrounding these factors to be prepared to deal with them as their importance fluctuates.

Figure 5.20: Arithmetic Mean – Current and Recommended Recognition of External Event Exposure Sub-Factors

The percentage variance between the current and recommended recognition of the sub-factors is depicted in figure 5.21. According to the responses, the deterioration of a bank’s reputation is regarded as the sub-factor that requires the largest increase in recognition to achieve the required level of importance. A reason for this may be the increase in the number of smaller banks in South Africa, which increases the competition and banks’ reliance on their reputation. In general, the other variances fluctuate between 2% and 14%, which indicates
that the difference between the current and recommended recognition of their importance does not require significant attention to achieve the desired level of management.

**Figure 5.21: Percentage Variance – Current and Recommended Recognition of External Event Exposure Sub-Factors**

![Bar Chart]

The *Spearman correlation coefficients* of the sub-factors of external exposures are depicted in figure 5.22. There are no significant differences at a 95% confidence level, indicating that all the identified sub-factors are recognised by the respondents as external event exposures. Although no additional factors were identified in the open-ended questions, the above-mentioned factors cannot be
regarded as a final list and could be expanded or even reduced as the circumstances of a bank change.

Figure 5.22: *Spearman Correlation Coefficient* – Correlation of Current and Recommended Recognition of External Event Exposure Sub-Factors

<table>
<thead>
<tr>
<th>Acts of God</th>
<th>*-0.0608</th>
</tr>
</thead>
<tbody>
<tr>
<td>External criminal activities</td>
<td>*-0.1670</td>
</tr>
<tr>
<td>Domestic political upheaval</td>
<td>*-0.1046</td>
</tr>
<tr>
<td>Regulatory &amp; compliance</td>
<td>*-0.0713</td>
</tr>
<tr>
<td>Legal actions</td>
<td>* 0.1445</td>
</tr>
<tr>
<td>Business environment Changes</td>
<td>* 0.1099</td>
</tr>
<tr>
<td>Deterioration of a bank’s Reputation</td>
<td>* 0.0497</td>
</tr>
<tr>
<td>Strikes</td>
<td>*-0.2098</td>
</tr>
<tr>
<td>Money laundering</td>
<td>* 0.1695</td>
</tr>
</tbody>
</table>

Significance at 5% critical value

5.4.2.3. **Definition**

This section focuses on a formal definition of operational risk. According to the literature study, it is evident that banks should adopt a formal definition of operational risk in order to be able to manage it as a primary risk type. As such, this item aims to determine to what extent banks have currently adopted a formal definition of operational risk and, secondly, to confirm according to the
experience and viewpoints of senior managers, to what degree banks should adopt a formal definition of operational risk.

The response regarding the current and the recommended situation are depicted in table 5.7.

Table 5.7: Response – Current and Recommended Adoption of a Formal Definition of Operational Risk by Banks

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1 2 3</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adoption of a formal</td>
<td>0 0</td>
<td>0.1723</td>
<td>0.47</td>
<td>18%</td>
</tr>
<tr>
<td>definition of operational risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td>0 0</td>
<td>4.82</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adoption of a formal</td>
<td>0 0</td>
<td>0.47</td>
<td>0.82</td>
<td></td>
</tr>
<tr>
<td>definition of operational risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

According to the research, 29% of the respondents indicated that their banks have adopted a formal definition of operational risk. On the other hand, 51% indicated that their banks have adopted some form of definition or are in the process of composing a formal definition. Finally, 20% of the respondents indicated that they have not as yet adopted a formal definition of operational risk. Furthermore, as most banks have not finally adopted a formal definition, it can be deduced that they are still in the process of demarcating the area of operational risk. The demarcation of the operational risk management function goes hand in hand with defining the area of operational risk.
From the above-mentioned it can be deduced that, in general, operational risk management is still in an early stage of development as the majority of banks have not yet formally adopted a definition of operational risk and therefore have not yet completely demarcated the area of operational risk.

Notwithstanding the fact that only a few banks have adopted formal definitions, 82% of them indicated that a formal definition of operational risk is imperative. As such, it can be deduced that although the majority of the banks have not adopted a formal definition of operational risk, most of them do recognise its importance and are serious in their approach to defining it.

The arithmetic means for the current and recommended situations confirm that the majority of the banks regard the adoption of a formal definition of operational risk as an important issue.

The *Spearman correlation coefficient* of the current and recommended ratings indicates no significant difference at a 95% confidence level. This confirms that banks should adopt a formal definition of operational risk as part of a structured approach to its management.

5.4.3. Item 3: Operational Risk Management Process

The aim of this item is, firstly, to determine the current approach of banks to a formal risk management process and the views of respondents on its recommended importance. Secondly, to obtain their views on the elements of an operational risk management process and, finally, to determine to what extent operational risk management processes are aligned with the organisation's strategies, objectives and overall management processes.
5.4.3.1. Formal Risk Management Approach

The responses to the current and recommended recognition of a formal risk management approach by banks are depicted in table 5.8.

Table 5.8: Response – Current and Recommended Recognition of the Importance of a Formal Risk Management Process

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1 2 3</td>
<td>4.03</td>
<td>0.2228</td>
<td>18%</td>
</tr>
<tr>
<td>Importance of a formal risk management process</td>
<td>0 0 16% 65% 19%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td>4.77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Importance of a formal risk management process</td>
<td>0 0 0 22% 78%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Nineteen percent of the respondents indicated that their banks currently recognise the importance of a formal risk management process and have implemented it. Sixty-five percent of the respondents indicated that their banks recognise the importance of a formal risk management process and are in the process of implementing it within their organisations. Sixteen percent indicated that their banks are still in an early stage of developing a formal risk management process, however, they do recognise its importance. According to the recommended rating, 78% of the respondents agreed that banks should recognise the importance and the implementation of a formal risk management process. From this response it can be deduced that most banks recognise the importance of implementing a formal risk management process. A possible reason for this attitude could be attributed to, for example, the recent developments on corporate
governance issues regarding risk management, such as, the recommendation that
the board of directors should be responsible for the total process of risk
management and management should be accountable to the board for designing,
implementing and monitoring such a process (King 2001:99).

The arithmetic means for the current and recommended situations confirm that
the majority of the banks regard the implementation of a formal risk management
process as important. Although, according to the percentage variance between
the current and recommended views, this situation still requires an improvement
of 18% to ensure an effective risk management process according to the
recommended situation.

The Spearman correlation coefficient of the current and recommended rating of
the recognition of the importance and implementation of a formal risk
management process indicates no significant difference at a 95% confidence
level. This emphasises the fact that the respondents regard the development and
implementation of a formal risk management process by banks as an important
issue.

5.4.3.2. Elements of an Operational Risk Management Process

This section of the research focuses on the elements of an operational risk
management process. According to the literature study, an operational risk
management process should consist of various elements to ensure a structured
approach during its implementation. As such, the elements were identified as risk
identification, risk evaluation, risk control and risk financing. This item aims to
determine the current importance assigned by banks to these elements, as part of
an operational risk management process as opposed to its recommended
importance. The response is depicted in table 5.9.
Table 5.9: Response – Current and Recommended Recognition of the Importance and Implementation of the Elements of an Operational Risk Management Process

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Current</td>
<td></td>
</tr>
<tr>
<td>Risk identification</td>
<td>0</td>
</tr>
<tr>
<td>Risk evaluation</td>
<td>0</td>
</tr>
<tr>
<td>Risk control</td>
<td>0</td>
</tr>
<tr>
<td>Risk financing</td>
<td>0</td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>Risk identification</td>
<td>0</td>
</tr>
<tr>
<td>Risk evaluation</td>
<td>0</td>
</tr>
<tr>
<td>Risk control</td>
<td>0</td>
</tr>
<tr>
<td>Risk financing</td>
<td>0</td>
</tr>
</tbody>
</table>

According to the response, it is only risk identification that is currently fully recognised and implemented, but only by a few banks (4%), as an important element of an operational risk management process. The remainder of the elements are recognised as important, but to a lesser degree, as they are not fully implemented by any of the banks. The research, however, shows that although risk identification is only fully implemented by a few banks, it is being developed and implemented by most of them as part of a formal operational risk management process.

Risk control is identified by most of the respondents as the current second-most important element. Therefore, risk identification and control are currently viewed by most banks as the most important elements of an operational risk management process. A possible reason for this rating could be the fact that as soon as a bank identifies a risk exposure, the exposure is directly subjected to a control measure.
without being evaluated. In this regard the literature study indicates that the quantitative measurement of operational risk is difficult to implement. Another possibility is that most banks still regard operational risk factors as traditional threats, such as, fire hazards, floods, accidents and thefts, and control these by means of emergency plans and insurance. However, as banks move towards the recognition of the primary risk factors of operational risk these traditional viewpoints are diminishing.

Risk evaluation, which includes the qualitative and quantitative measuring of the identified exposures, is currently not regarded as important as risk identification and control due to the above reasons. Risk financing is currently rated as the least important element of operational risk. This element can be regarded as the final step in the risk management process. As the first three steps are still in a development phase, it is difficult for banks to determine the cost of operational risk and its financing.

Based on the views of the respondents on the recommended importance of the elements of the operational risk management process, risk identification is rated as the most important element by 65% of the respondents. As such, it can be deduced that risk identification should form a crucial part of an operational risk management process as it identifies the risk exposures. These exposures should be subjected to the other elements of the process.

Risk financing is identified by the respondents as the second most important element of an operational risk management process ahead of evaluation and control. A possible reason for this high rating may be the result of the current focus of regulators on a capital charge for operational risk. In this sense there are various initiatives within the banking industry concerning the cost of operational risk and its financing. As such, it can be deduced that the high rating of risk
financing, as an element of an operational risk management process, may change
as solutions to the financing problems are found. It should, however, remain an
integral part of the risk management process.

Risk control is recognised by the respondents as the third most important element
that should be part of an operational risk management process. A possible reason
for the lower rating may be the uncertainty of the available control measures for
operational risk exposures.

Risk evaluation is rated by only 30% of the respondents as an important element
that should form part of an operational risk management process. As mentioned
above, the difficulty in quantifying operational risk could have influenced the
rating of this element. As such, it can be concluded that although current views
differ, the measuring process will become an important element of the
management process only when banks clearly demarcate the areas and exposures
of operational risk. This is because operational risk forms the basis to determine
the exposures that should be controlled and financed.

In addition to the above-mentioned, the arithmetic means (see figure 5.23)
confirm the current recognition by banks of the importance of the identified
elements and the recommended importance of implementing them, as an integral
part of an operational risk management process.

The differences between the current and recommended situation (see figure
5.24), seem to indicate that risk financing requires the most improvement to be
established as an integral element of an operational risk management process.
Figure 5.23: Arithmetic Mean – Current and Recommended Recognition and Implementation of Elements of an Operational Risk Management Process

Figure 5.24: Percentage Variance – Current and Recommended Recognition and Implementation of Elements of an Operational Risk Management Process
The Spearman correlation coefficients of the elements of an operational risk management process are depicted in figure 5.25. There is no significant difference at a 95% confidence level between the current and recommended situations. This confirms that the identified elements are all recognised as important elements of an operational risk management process. There were no additional elements identified by the open-ended questions. It can, therefore, be deduced that the identified elements should form the basis of and be an integral part of an operational risk management process.

Figure 5.25: Spearman Correlation Coefficient – Correlation of Current and Recommended Recognition and Implementation of Elements of an Operational Risk Management Process

<table>
<thead>
<tr>
<th>Risk identification</th>
<th>* 0.0936</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk evaluation/measurement</td>
<td>* -0.07213</td>
</tr>
<tr>
<td>Risk control</td>
<td>* -0.0167</td>
</tr>
<tr>
<td>Risk financing</td>
<td>* -0.02271</td>
</tr>
</tbody>
</table>

Significance at 5% critical value

0.754

5.4.3.3. Alignment of the Operational Risk Management Processes with the Strategies and Objectives of Banks

This item aims to determine the current and recommended alignment of operational risk management processes with banks’ strategies and objectives. In the literature study, it was determined that if risk management is incorporated in
an organisation's strategy, it improves the effectiveness of risk management. As such, it can be deduced that it is becoming imperative for banks to align their risk management processes, including that of operational risk, with their strategy and objectives to ensure the exploitation of the resulting benefits.

The responses to the current and recommended alignment of operational risk management processes with banks’ strategies and objectives are depicted in table 5.10.

**Table 5.10: Response – Current and Recommended Alignment of an Operational Risk Management Process with Strategies and Objectives**

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1 2 3</td>
<td>4 5</td>
<td>3.68</td>
<td>0.0915</td>
</tr>
<tr>
<td>Importance of aligning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>an operational risk</td>
<td>0</td>
<td>9% 35% 37% 19%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>management process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>with a bank’s strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td></td>
<td>4.69</td>
<td></td>
</tr>
<tr>
<td>Importance of aligning</td>
<td>0</td>
<td>0 0 30% 70%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>an operational risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>management process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>with a bank’s strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Nineteen percent of the respondents indicated that their banks currently recognise the importance of aligning their operational risk management processes to their strategies and objectives and have done so. Thirty-seven percent have recognised the importance of doing so, but are still in a process of aligning it. Thirty-five
percent recognised the importance thereof, but are still at an early stage of development. The remaining 9% recognised the importance, but have not started with any development. According to the recommended situation, the majority of the respondents indicated that it is of the utmost importance that an operational risk management process should be aligned with their banks' strategies and objectives. A high average score of 70% by the respondents for the recommended situation supports this viewpoint. According to the percentage variance, the current situation requires extensive improvement (27%) to achieve the desired level of alignment of the operational risk management processes with the strategies and objectives of banks.

According to the Spearman correlation coefficient of the current and recommended situations, there is no significant difference at a 95% confidence level, emphasising the perceived importance of aligning a bank's operational risk management process with its strategy and objectives.

5.4.3.4. The Operational Risk Management Process as an Integral Part of the Overall Risk Management Process

In the literature study, it was indicated that organisations encounter new types of risks while pursuing their business objectives. They, therefore, require integrated risk management frameworks to ensure that all possible risks are covered. This emphasises that banks should approach operational risk management as an integral part of their overall risk management processes.

The aim of this item is to determine to what degree the operational risk management processes of banks are integral parts of their overall risk management processes as opposed to their views on whether or not it should be. Eleven percent of the respondents indicated that operational risk management
currently forms an integral part of their overall risk management processes (see table 5.11), whereas 41% indicated that they are still in a development phase. The remaining respondents indicated that their organisations are still in the early stages of developing operational risk management processes, although they have overall risk management processes in place. From the above, it can be deduced that although most banks are still developing their operational risk management processes, they are aware that such processes should form an integral part of an overall risk management process. As such, 70% of the respondents recommended that operational risk management processes should form an integral part of banks’ overall risk management processes. It is, thus, evident that banks should be aware of operational risk as a separate risk type that should be managed in an integrated way with the other risk types to ensure an enterprise-wide approach to risk management.

Table 5.11: Response – Current and Recommended Rating of Operational Risk Management as an Integral Part of the Overall Risk Management Process

<table>
<thead>
<tr>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Operational risk management process as integral part of an overall risk management process</td>
<td>0</td>
<td>0</td>
<td>48%</td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational risk management process as integral part of an overall risk management process</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The arithmetic means for the current and recommended situations confirm that the majority of the banks regard operational risk management as an integral part of the overall risk management process. However, the percentage variance between the current and recommended situations confirms that most banks are still developing their operational risk management processes.

The Spearman correlation coefficient of the current and recommended situations indicate no significant differences at a 95% confidence level. This confirms again that an operational risk management process should, according to the respondents, form an integral part of a bank's overall risk management process.

In conclusion, it is thus evident that most banks are in the process of developing an operational risk management process and are aware that it should form an integral part of an overall risk management process of a bank.

5.4.4. Item 4: Identification of Operational Risk

The aim of this item is, firstly, to determine to what degree banks currently recognise the importance of risk identification as an ongoing process and whether this viewpoint differs from their recommended views. Secondly, to establish the currently used and recommended methods for the identification of risks.

5.4.4.1. Risk Identification as an Ongoing Process

Fourteen percent of the respondents (see table 5.12) indicated that their banks recognise the importance of risk identification as an ongoing process. Fifty-four percent recognised it as important, but to a lesser degree as an ongoing process. As such, it can be concluded that most banks recognise the importance of risk
identification, but only a few banks currently regard it as an ongoing process. According to the recommended situation, however, the majority of the respondents recognised the importance of risk identification as an ongoing process to continuously identify risk exposures.

Table 5.12: Response – Current and Recommended Recognition of the Importance of Risk Identification as an Ongoing Process

<table>
<thead>
<tr>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1 2 3 4 5</td>
<td>3.83</td>
<td>0.2506</td>
</tr>
<tr>
<td>Risk identification as an ongoing process</td>
<td>0 0 32% 54% 14%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td>4.63</td>
<td></td>
</tr>
<tr>
<td>Risk identification as an ongoing process</td>
<td>0 0 0 37% 63%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The arithmetic means of the current and recommended situations confirm that, on average, the majority of the banks recognise the importance of implementing risk identification as an ongoing process. The percentage variance, however, indicates that the current situation still differs substantially from the recommended situation.

The *Spearman correlation coefficient* indicates no significant differences at a 95% confidence level between the current and recommended recognition of risk identification as an ongoing process. It is, therefore, confirmed that banks should establish risk identification as an ongoing process to be able to determine the risk exposures on a continuous basis.
5.4.4.2. **Methods to Identify Risks**

The survey focused on six methods, identified in the literature study, which can be used to identify risks. The aim is to determine and compare the current and recommended importance of the methods.

The responses (see table 5.13) and the arithmetic means of the responses (see figure 5.26) indicate that the current most recognised method to identify risks is workshops, followed by brainstorming sessions. Although the remainder of the methods were rated lower, they were all recognised as methods of identifying risks. Respondents indicated that workshops should be regarded as the most important method of identifying risks, followed by brainstorming. Process mapping is recognised as the third most important method. The remainder of the methods are all regarded as relevant methods, but with a lesser degree of importance.

**Table 5.13: Response – Current and Recommended Recognition of Methods for Risk Identification**

<table>
<thead>
<tr>
<th>Method</th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td></td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
</tr>
<tr>
<td>Brainstorming</td>
<td>1%</td>
</tr>
<tr>
<td>Questionnaires</td>
<td>8%</td>
</tr>
<tr>
<td>Process mapping</td>
<td>9%</td>
</tr>
<tr>
<td>Comparison with other</td>
<td>13%</td>
</tr>
<tr>
<td>organisations</td>
<td></td>
</tr>
<tr>
<td>Discussions with peers</td>
<td>11%</td>
</tr>
<tr>
<td><strong>Proposal</strong></td>
<td></td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
</tr>
</tbody>
</table>
The percentage variance between the current and recommended recognition (see figure 5.27) of the methods of identifying risks indicate that discussions with peers and comparison with other organisations require the largest increases in recognition to achieve the desired level of importance. However, it was found that substantial improvement in terms of the recognition of importance of all the methods are required.
Figure 5.27: Percentage Variance – Current and Recommended Recognition of Methods for Risk Identification

The Spearman correlation coefficients (depicted in figure 5.28) indicate no significant differences at a 95% confidence level between the current and recommended recognition of the methods of identifying risks. There were no additional methods identified in the open-ended questions. It can, therefore, be deduced that the above-mentioned methods should, according to the respondents, be regarded as the most appropriate methods that a bank should use for risk identification.

Figure 5.28: Spearman Correlation Coefficient – Correlation of Current and Recommended Recognition of Methods for Risk Identification

<table>
<thead>
<tr>
<th>Method</th>
<th>Correlation Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workshops</td>
<td>0.3962</td>
</tr>
<tr>
<td>Brainstorming</td>
<td>0.3947</td>
</tr>
<tr>
<td>Questionnaires</td>
<td>0.2261</td>
</tr>
<tr>
<td>Process mapping</td>
<td>-0.0433</td>
</tr>
<tr>
<td>Comparisons with other organisations</td>
<td>0.4296</td>
</tr>
<tr>
<td>Discuss with peers</td>
<td>0.2321</td>
</tr>
</tbody>
</table>

Significance at 5% critical value: 0.707
5.4.5. **Item 5: Measurement of Operational Risk**

The aim of this item is to determine the qualitative and quantitative methods that are currently recognised as important methods to measure operational risk as well as the methods that respondents recommend.

5.4.5.1. **Qualitative Methods**

The responses to the qualitative methods, identified in the literature study, are depicted in table 5.14. According to the responses as well as the arithmetic means of the responses (see figure 5.29), the self-risk assessment method is currently recognised as the most important method to measure operational risk, followed by historical data and risk maps/process flows. In terms of the recommended recognition, self-risk assessment and historical data remain the two most important qualitative methods to measure operational risk, with risk maps/process flows being rated less important.

| Table 5.14: Response – Current and Recommended Recognition of Qualitative Methods to Measure Operational Risk |
|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|
| Current                                         | Scale                                           | Scale                                           | Scale                                           | Scale                                           | Scale                                           |
| Historical data                                 | 9% 28% 52% 11% 0                               | 9% 28% 52% 11% 0                               | 9% 28% 52% 11% 0                               | 9% 28% 52% 11% 0                               | 9% 28% 52% 11% 0                               |
| Self-risk assessment                            | 0 9% 43% 43% 5%                               | 0 9% 43% 43% 5%                               | 0 9% 43% 43% 5%                               | 0 9% 43% 43% 5%                               | 0 9% 43% 43% 5%                               |
| Risk maps/process flows                         | 14% 25% 56% 5% 0                              | 14% 25% 56% 5% 0                              | 14% 25% 56% 5% 0                              | 14% 25% 56% 5% 0                              | 14% 25% 56% 5% 0                              |
| Recommended                                     |                                                 |                                                 |                                                 |                                                 |                                                 |
| Historical data                                 | 0 0 28% 51% 21%                               | 0 0 28% 51% 21%                               | 0 0 28% 51% 21%                               | 0 0 28% 51% 21%                               | 0 0 28% 51% 21%                               |
| Self-risk assessment                            | 0 0 9% 58% 33%                               | 0 0 9% 58% 33%                               | 0 0 9% 58% 33%                               | 0 0 9% 58% 33%                               | 0 0 9% 58% 33%                               |
| Risk maps/process flows                         | 0 0 24% 73% 3%                               | 0 0 24% 73% 3%                               | 0 0 24% 73% 3%                               | 0 0 24% 73% 3%                               | 0 0 24% 73% 3%                               |
It can be deduced that self-risk assessment is the best qualitative method to apply to measure operational risk.

**Figure 5.29: Arithmetic Mean – Current and Recommended Recognition of Qualitative Methods to Measure Operational Risk**

The percentage variance between the current and the recommended situation (see figure 5.30) indicates that risk mapping/process flows require the most improvement to achieve the recognised level of importance, followed by historical data and self-risk assessment.

**Figure 5.30: Percentage Variance – Current and Recommended Qualitative Methods to Measure Operational Risk**
The Spearman correlation coefficients (depicted in figure 5.31) indicate no significant differences at a 95% confidence level for the current and recommended qualitative methods for measuring operational risk. As there were no additional methods identified by means of the open-ended questions, it can be deduced that the above-mentioned methods are, according to the respondents, the most important methods that should be implemented to qualitatively measure operational risk.

Figure 5.31: Spearman Correlation Coefficient – Correlation for the Current and Recommended Qualitative Methods to Measure Operational Risk

<table>
<thead>
<tr>
<th>Historical data</th>
<th>* -0.05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-risk assessment</td>
<td>* 0.235</td>
</tr>
<tr>
<td>Risk mapping/process flows</td>
<td>* -0.23</td>
</tr>
</tbody>
</table>

Significance at 5% critical value

0.878

5.4.5.2. Quantitative Methods

The quantitative methods identified in the literature study to measure operational risk are depicted in table 5.15. The respondents indicated that risk indicators is the current most-recognised quantitative method, followed by escalation triggers, loss-event databases and causal modeling. Although the risk indicator method is regarded as the currently most-recognised method, all the methods are regarded as important. In terms of the recommended recognition of the methods, the loss-event database is regarded as the most important, followed by risk indicators, causal modeling and escalation triggers. A possible reason for rating the loss-
event database as the most important quantitative method that banks should use could be ascribed to the latest developments relating to the Basel Committee. According to the Committee, banks should allocate a capital charge to operational risk. For banks to be able to determine a realistic capital charge for operational risk, they require a loss-event database.

Table 5.15: Response – Current and Recommended Recognition of Quantitative Methods to Measure Operational Risk

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Current</td>
<td></td>
</tr>
<tr>
<td>Causal modeling</td>
<td>13%</td>
</tr>
<tr>
<td>Risk indicators</td>
<td>8%</td>
</tr>
<tr>
<td>Escalation triggers</td>
<td>11%</td>
</tr>
<tr>
<td>Loss-event database</td>
<td>9%</td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>Causal modeling</td>
<td>0</td>
</tr>
<tr>
<td>Risk indicators</td>
<td>0</td>
</tr>
<tr>
<td>Escalation triggers</td>
<td>0</td>
</tr>
<tr>
<td>Loss-event database</td>
<td>0</td>
</tr>
</tbody>
</table>

The arithmetic means for the current and recommended situations (see figure 5.32) indicate that all the quantitative methods to measure operational risk are currently rated at an average lower ranking. This is indicative of banks not quantifying operational risk satisfactorily. However, the respondents indicate in terms of recommended importance that all the methods are applicable and could be applied. The loss-event database and risk indicator methods are rated the highest, but the importance of the other methods is also confirmed.
According to the percentage variance of the current and recommended situations (see figure 5.33), the loss-event database, recognised as the most important method, also requires the most development to achieve the desired level of implementation. Substantial differences also exist between the current and recommended levels of implementation and importance of the other methods.

There were no additional methods identified in the open-ended questions. According to the Spearman correlation coefficients (see figure 5.34) there are no
significant differences at a 95% confidence level for the current and recommended situations. This confirms the identified methods as the most appropriate methods to be used by banks to quantitatively measure operational risk.

**Figure 5.34: Spearman Correlation Coefficient – Correlation for the Current and Recommended Quantitative Methods to Measure Operational Risk**

<table>
<thead>
<tr>
<th>Method</th>
<th>Correlation Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Causal modeling</td>
<td>* 0.1426</td>
</tr>
<tr>
<td>Risk indicators</td>
<td>* 0.0608</td>
</tr>
<tr>
<td>Escalation triggers</td>
<td>* 0.0208</td>
</tr>
<tr>
<td>Loss-event database</td>
<td>* -0.0445</td>
</tr>
</tbody>
</table>

Significance at 5% critical value 0.811

5.4.6. **Item 6: Operational Risk Control**

Policies, internal controls and reporting are the control measures for operational risk identified in the literature study. The aim of this item is to determine the banks’ current and recommended recognition of the identified control measures.

The responses are depicted in table 5.16 and the arithmetic means of the responses in figure 5.35. The respondents rated policies as the current most important control measure of operational risk, while internal controls and reporting were rated as the second and third most important methods respectively.
Table 5.16: Response – Current and Recommended Recognition of Control Measures for Operational Risk

<table>
<thead>
<tr>
<th>Scale</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>0</td>
<td>0</td>
<td>27%</td>
<td>44%</td>
<td>29%</td>
</tr>
<tr>
<td>Internal controls</td>
<td>0</td>
<td>0</td>
<td>16%</td>
<td>70%</td>
<td>14%</td>
</tr>
<tr>
<td>Reporting</td>
<td>0</td>
<td>13%</td>
<td>14%</td>
<td>59%</td>
<td>14%</td>
</tr>
<tr>
<td>Recommended Policies</td>
<td>0</td>
<td>0</td>
<td>2%</td>
<td>41%</td>
<td>57%</td>
</tr>
<tr>
<td>Recommended Internal controls</td>
<td>0</td>
<td>0</td>
<td>3%</td>
<td>70%</td>
<td>27%</td>
</tr>
<tr>
<td>Recommended Reporting</td>
<td>0</td>
<td>0</td>
<td>8%</td>
<td>73%</td>
<td>19%</td>
</tr>
</tbody>
</table>

Figure 5.35: Arithmetic Mean – Current and Recommended Recognition of Control Measures for Operational Risk

Although policies, as a control measure, is recognised as the most important method, the percentage variance (see figure 5.36) indicates that it also requires the largest increase in recognition to achieve the required level of importance. The existing and recommended situations for reporting and internal controls also indicate that their recognition should increase.
Figure 5.36: Percentage Variance – Current and Recommended Recognition of Control Measures for Operational Risk

The *Spearman correlation coefficients* (see figure 5.37) indicate no significant differences at a 95% confidence level for the current and recommended situations. As such, it can be deduced that the three control measures are recognised as important measures for operational risk and should be implemented by banks during an operational risk management process.

Figure 5.37: *Spearman Correlation Coefficient* – Correlation for the Current and Recommended Control Measures for Operational Risk

<table>
<thead>
<tr>
<th>Policies</th>
<th>Internal controls</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>* 0.2196</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* 0.2476</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* -0.0447</td>
</tr>
</tbody>
</table>

Significance at 5% critical value 0.878
5.4.7. Item 7: Operational Risk Structure

The literature study indicates that it is essential for a risk management function to be established and operated as a controlling or monitoring function independently from the business areas. Therefore, the aim of this item is, firstly, to determine to what degree separate operational risk management structures have been established and whether respondents are of the opinion that separate operational risk management structures should be established. Secondly, it is to determine the current and the recommended roles of internal audit in the management of operational risk. Lastly, it is to determine the current and recommended involvement of business managers in an operational risk management process.

5.4.7.1. Operational Risk Management Structure

According to the response (see table 5.17), 49% of the respondents indicated that their banks have established a separate operational risk management structure, while 38% indicated that their banks are in a process of establishing such a structure. Thirteen percent indicated that their banks have not implemented a separate structure, although they recognise its importance. It can, therefore be deduced that most banks are moving towards the establishment of a separate operational risk structure. According to the responses relating to the recommended situation, most of the respondents indicated a separate structure for operational risk management as an absolute necessity, while the rest regard it as necessary, but to a lesser degree.
Table 5.17: Response – Current and Recommended Structure for Operational Risk Management

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Structure for operational risk management</td>
<td>0</td>
<td>0</td>
<td>13%</td>
<td>38%</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structure for operational risk management</td>
<td>0</td>
<td>0</td>
<td>6%</td>
<td>29%</td>
</tr>
</tbody>
</table>

The arithmetic means of the responses for the current and recommended situations confirm the importance of establishing a separate operational risk management structure. In terms of the percentage variance for the current and recommended recognition of a separate operational risk management structure, the relatively low variance indicates that banks currently realise the importance of a separate structure and are in the process of restructuring their organisations to accommodate an operational risk management structure.

The Spearman correlation coefficient indicates no significant differences at a 95% confidence level for the current and recommended situations in terms of a separate structure for operational risk management. This confirms that banks should, according to the respondents, implement a separate structure for operational risk management.

5.4.7.2. Reporting Lines

In the literature study, the importance of effective risk reporting is emphasised as an increasingly important part of the risk management process. Therefore, the
aim of this item is to determine if banks recognise the importance of formal reporting lines between risk managers and top management, such as, the CEO. Thirty-seven percent of the respondents (see table 5.18) indicated that their risk managers have a direct reporting line to the CEO, while the remaining indicated that their banks recognised the importance of and were in an advanced process of formalising similar reporting lines. This emphasises that risk management is, according to the respondents, rated as one of the key management functions of banks. In terms of the recommended viewpoints, most of the respondents indicated that risk managers should have a direct reporting line to the CEO, again emphasising its importance.

Table 5.18: Response – Current and Recommended Recognition of Reporting Lines between the Risk Manager and the CEO

<table>
<thead>
<tr>
<th>Scale</th>
<th>Current</th>
<th></th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 2 3 4 5</td>
<td>Formal reporting lines between risk managers and the CEO</td>
<td>4.63</td>
<td>0.1785</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>0 0 0</td>
<td>63% 37%</td>
<td>4.68</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 0 0</td>
<td>Formal reporting lines between risk managers and the CEO</td>
<td>30% 70%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Both the arithmetic means of the current and recommended situations rate a direct reporting line between the risk manager and the CEO as very important. There is a mere 1% variance between the current and the recommended ratings, which emphasises that most banks regard it as an important part of a risk management approach.
According to the Spearman correlation coefficient, there are no significant differences at a 95% confidence level for the current and recommended situations. This indicates that it is imperative that banks should, according to the respondents, establish formal risk reporting lines between risk managers and top management.

5.4.7.3. Responsibility for Operational Risk

According to the literature study, the involvement of different role players in the management of operational risk should add to the awareness of operational risk throughout the organisation. However, it is important that the roles and responsibilities of the various role players regarding the management of operational risk are clearly stipulated. Therefore, this section, firstly, deals with the responsibility of internal audit towards operational risk. Secondly, it determines the involvement of the board of directors in operational risk management and, lastly, it determines the involvement of business managers in operational risk management.

*Internal Audit.* Twenty-three percent of the respondents (see table 5.19) indicated that their banks involve their internal audit departments to some degree in managing their operational risk, while 63% indicated that internal audit departments play an important role, but more in an advisory capacity. Fourteen percent of the respondents indicated that their banks do not use their internal audit departments to manage their operational risk. Thirteen percent of the respondents were of the opinion that operational risk should be an internal audit function, while 50% indicated that it should be a separate function. It can, therefore, be concluded that most banks do not regard the internal audit department as responsible for the day-to-day management of operational risk, although internal audit is still currently actively involved in managing it. As the
operational risk management process develops, however, internal audit is becoming less involved.

The arithmetic means and the percentage variance of the current and recommended ratings of the involvement of internal audit in operational risk management indicate that their involvement should be reduced by 13% to achieve the recommended level of involvement. It can, therefore, be deduced that although internal audit is still involved in the management of operational risk, its involvement should be reduced as a bank progresses in establishing a formal operational risk management process.

**Table 5.19: Response – Current and Recommended Situation Regarding the Involvement of Internal Audit in the Management of Operational Risk**

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Involvement of internal audit in the management of operational risk</td>
<td>0 0 14% 63% 23%</td>
<td>4.11</td>
<td>0.0037</td>
<td>13%</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Involvement of internal audit in the management of operational risk</td>
<td>0 0 50% 37% 13%</td>
<td>3.56</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

According to the *Spearman correlation coefficient* there are no significant differences at a 95% confidence level between the current and recommended situations. This emphasises that internal audit should not be involved in the management of operational risk.
Board of directors. The current involvement of members of the board of directors in the management of operational risk is depicted in table 5.20. Fourteen percent of the respondents indicated that a member of their board of directors has been allocated the responsibility of operational risk management, while 67% indicated that their banks are in a process of finalising a similar approach. Sixty-five percent of the respondents indicated that a member of the board should be allocated the responsibility of operational risk management. It is evident that most banks agree to the active involvement of a member of the board of directors in operational risk. This approach is also in line with the latest developments in corporate governance.

Table 5.20: Response – Current and Recommended Involvement of the Board of Directors in the Management of Operational Risk

<table>
<thead>
<tr>
<th>Current</th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Involvement of the board of directors in the management of operational risk</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Recommended

| Involvement of the board of directors in the management of operational risk | 0 | 0 | 0 | 35% | 65% |

According to the arithmetic means, the involvement of the board of directors in operational risk management is regarded as important and should, according to
the percentage variance, be improved by 11% to achieve the recommended level of involvement.

The *Spearman correlation coefficient* indicates no significant differences at a 95% confidence level for the current and recommended situations. As such, it confirms that the board of directors should be actively involved and responsible for the management of operational risk.

**Business managers.** The responses regarding the involvement of business managers in the management of operational risk are depicted in table 5.21.

**Table 5.21: Response – Current and Recommended Involvement of Business Managers in the Management of Operational Risk**

<table>
<thead>
<tr>
<th>Involvement of business managers in the management of operational risk</th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Involvement of business managers in the management of operational risk</td>
<td>0</td>
<td>3%</td>
<td>13%</td>
<td>49%</td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Involvement of business managers in the management of operational risk</td>
<td>0</td>
<td>0</td>
<td>6%</td>
<td>29%</td>
</tr>
</tbody>
</table>

Thirty-five percent of the respondents indicated that their banks have currently involved business managers extensively in the management of operational risk, while 49% indicated that their banks are in a process of finalising the operational risk management process, which will include the involvement of business
managers. It can, therefore, be deduced that most banks recognise the importance of involving business managers in an operational risk management process. This viewpoint is substantiated by the recommended situation where the majority of the respondents indicated that business managers should be involved to a large extent in the management of operational risk. According to the percentage variance, the current involvement of business managers should be improved by 19% to achieve the recommended level of involvement.

The Spearman correlation coefficient, furthermore, indicates no significant differences at a 95% confidence level between the current and recommended situations. As such, it confirms that banks should, based on the responses, involve business managers in the operational risk management process.

5.4.8. Item 8: Financing of Operational Risk

The aim of this item is to determine the respondents' attitude towards risk financing techniques as it relates to operational risk and to establish the banks' perceived involvement in the Basel Committee's proposals to determine a regulatory capital charge for operational risk.

5.4.8.1. Risk Financing Techniques

Three techniques were identified in the literature study, namely, risk transfers (refer to footnote 2 in chapter 3), risk retention (funded) and risk retention (unfunded).

The responses (see table 5.22) indicate that 44% of the banks recognise risk transfer to a third party as the most important risk financing technique, followed by risk retention (funded) and risk retention (unfunded). It can, furthermore, be
deduced that most banks are currently relying on insurance companies to minimise operational risk. According to the recommended situation, the majority of the respondents confirm the importance of the financing techniques. It can, therefore, be deduced that the risk financing techniques form an important part of an operational risk management process in order to minimise the risk exposures.

Table 5.22: Response – Current and Recommended Recognition of Risk Financing Techniques

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td></td>
</tr>
<tr>
<td>Risk transfers</td>
<td>0</td>
</tr>
<tr>
<td>Risk retention (funded)</td>
<td>0</td>
</tr>
<tr>
<td>Risk retention (unfunded)</td>
<td>0</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td></td>
</tr>
<tr>
<td>Risk transfers</td>
<td>0</td>
</tr>
<tr>
<td>Risk retention (funded)</td>
<td>0</td>
</tr>
<tr>
<td>Risk retention (unfunded)</td>
<td>0</td>
</tr>
</tbody>
</table>

The arithmetic means for the current and recommended situations (see figure 5.38) as well as the percentage variance (see figure 5.39) indicate that all the identified financing techniques of operational risk should be improved to achieve the required levels of recognition as risk financing techniques. Although risk retention (unfunded) is regarded as the least important technique, it is deduced that this technique should improve with the establishment of a formal operational risk management process. Stricter control measures should allow management to accept a certain amount of operational risk as part of the bank’s risk appetite.
Figure 5.38: Arithmetic Mean – Current and Recommended Recognition of Operational Risk Financing Techniques

![Graph showing arithmetic mean for risk transfer, risk retention (funded), and risk retention (unfunded).]

Figure 5.39: Percentage Variance – Current and Recommended Recognition of Operational Risk Financing Techniques

![Graph showing percentage variance for risk transfers, risk retention (funded), and risk retention (unfunded).]

The Spearman correlation coefficients (see figure 5.40) indicate no significant differences at a 95% confidence level for the current and recommended situations. Therefore, banks should, based on the responses, implement the above-mentioned risk financing techniques to manage operational risk.
5.4.8.2. Basel Committee’s Proposals

The Basel Committee’s proposal to allocate a minimum capital requirement for operational risk has been identified in the literature study. This item aims to determine the banks’ awareness and acceptance of the Basel Committee proposals relating to a capital charge for operational risk as well as their progress to comply with the requirements of the Basel Accord of 2001.

Sixty-two percent of the respondents indicated that their banks were aware of the initial proposals of the Basel Committee (see table 5.23) and had studied the content of the proposals that were circulated for comment. Thirty-three percent indicated that their banks were aware of the proposals, but had not spent time on the detail content thereof, while 5% were only vaguely aware of the proposal. However, the majority of the respondents indicated that their banks regard the proposal of the Basel Committee, to implement a capital charge for operational risk, as a necessity.
The arithmetic means of the current and the recommended situations as well as the percentage variance indicate that banks should become more proactive in determining the implications of allocating a capital charge for operational risk. As such, it is deduced that banks would be more prepared to accept and implement the Basel proposals if they were aware of the implications and their potential benefits.

The Spearman correlation coefficient indicates no significant differences at a 95% confidence level for the current and recommended situations. This confirms that banks should, according to the respondents, be more proactive in determining the implications regarding the allocation of a capital charge for operational risk.

**Table 5.23: Response – Current and Recommended Awareness of the Basel Proposals by Banks**

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1 2</td>
<td>3 4 5</td>
<td>2.66</td>
<td>-0.3378</td>
</tr>
<tr>
<td>Involvement of banks in the Basel Committee’s proposals to allocate capital to operational risk</td>
<td>5% 33% 62% 0 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Involvement of banks in the Basel Committee’s proposals to allocate capital to operational risk</td>
<td>0 0 8% 35% 57%</td>
<td>4.49</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Regarding the recommended approaches to assess operational risk to determine a capital charge, 29% of the respondents (see table 5.24) indicated that their banks
are currently evaluating the basic indicator approach, 25% the standardised approach and 20% the internal measurement approach. On the other hand, the majority of the banks are, according to the respondents, aware of, but are currently not actively evaluating all the different approaches. Regarding the recommended evaluation of the approaches to assess capital for operational risk, the majority of the respondents indicated that their banks should actively evaluate all the approaches to prepare themselves to implement the best method by 2005, when the regulators plan to implement this proposal in the banking industry.

The arithmetic means (see figure 5.41) as well as the percentage variance for the current and recommended situations indicate that all three methods require increased management attention in order to determine their significance to assess capital for operational risk. It is, furthermore, recommended that the internal measurement approach be regarded as the preferred method to assess capital for operational risk, followed by the standardised and then the basic indicator approaches.

Table 5.24: Response – Current and Recommended Recognition of the Approaches to Assess Capital for Operational Risk

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td></td>
</tr>
<tr>
<td>Basic indicator approach</td>
<td>19%</td>
</tr>
<tr>
<td>Standardised approach</td>
<td>29%</td>
</tr>
<tr>
<td>Internal measurement approach</td>
<td>37%</td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
<td></td>
</tr>
<tr>
<td>Basic indicator approach</td>
<td>0</td>
</tr>
<tr>
<td>Standardised approach</td>
<td>0</td>
</tr>
<tr>
<td>Internal measurement approach</td>
<td>0</td>
</tr>
</tbody>
</table>
Figure 5.41: Arithmetic Mean – Current and Recommended Recognition of the Approaches to Assess Capital for Operational Risk

With regard to how essential respondents view the determining of a minimum regulatory capital for operational risk (see table 5.25), it was found that 17% of the respondents currently regarded it as essential, while 52% indicated it was important, but not essential. The rest of the respondents did not regard it as important. Generally though, it can be deduced that banks should regard a minimum capital requirement for operational risk as an important part of their management process.

Table 5.25: Response – Current and Recommended Recognition of the Essentiality of a Minimum Capital Requirement for Operational Risk

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Arithmetic mean</th>
<th>Spearman</th>
<th>% variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1 2 3 4 5</td>
<td>3.81</td>
<td>0.4373</td>
<td>16%</td>
</tr>
<tr>
<td>Essentiality of a minimum capital requirement for operational risk</td>
<td>0 4% 27% 52% 17%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
<td>4.43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Essentiality of a minimum capital requirement for operational risk</td>
<td>0 0 10% 38% 52%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.5 Conclusion

This chapter dealt with the statistical analysis of the research according to the methodology which was discussed in chapter 4.

A total of 63 questionnaires were returned, which represents 26.9% of foreign banks and 73.1% of local banks included in the survey. The responses were grouped into eight items according to the questions with a similar construct in order to simplify the statistical analysis. The main conclusions for each item are summarised as follows:

Item 1: Risk types

- The primary risk types of a bank are perceived to be market, credit, liquidity, interest-rate and operational risk.
- Legal, reputation and country risk are still at an early stage of development and are not currently regarded as primary risk types of banks.
- A structured approach to operational risk management of a bank should include the primary risk types to indicate the potential interactivity between them.

Item 2: Operational risk factors and definition

- The primary operational risk factors are perceived to be people, processes, systems and external events. It can, therefore, be concluded that these factors are the pillars of operational risk
which should form an integral part of an operational risk management process.

- The primary risk factors of operational risk consist of various sub-factors that must be addressed during an operational risk management process. Although such main sub-factors were identified during the literature study and research, they are subject to continuous changes as a result of changes in a bank’s environment and circumstances, making their standardisation nearly impossible. Furthermore, the number of sub-factors for each primary risk factor is not exhaustive and new exposures to a bank may often change the importance of these sub-factors in terms of priority. However, it is crucial that these sub-risks be identified as early as possible to be controlled and managed. As such, a structured approach to an operational risk management process for a bank should ensure a proactive attitude towards managing and controlling risks.

- The research indicates that it is imperative that a bank adopts a formal definition of operational risk which will form the platform of a structured approach.

**Item 3: Operational risk management process**

- It is important that banks follow a formal risk management process.
- The basic elements of an operational risk management process were identified as risk identification, risk evaluation, risk control and risk financing.
- It is also imperative that an operational risk management process be aligned to a bank’s strategies and objectives to ensure that the
applicable risk exposures are identified and subsequently controlled and managed.

- It is also important that an operational risk management process be managed as an integral part of an overall risk management process to ensure an enterprise-wide risk management framework.

**Item 4: Identification of risk**

- Risk identification was identified as an ongoing process to ensure a dynamic approach to operational risk management. This will ensure that new risk exposures will be continuously identified at an early stage and subsequently be managed.

- A variety of methods to identify operational risk were identified. The methods that proved to be the most widely recognised were workshops, brainstorming sessions and process mapping. Questionnaires, discussion with peers and comparison with other organisations were also regarded as useful methods, but less important than the aforementioned.

**Item 5: Measurement of operational risk**

- Self-risk assessments were identified as the most relevant qualitative method to measure operational risk along with risk mapping/process flows and historical data.

- Loss-event databases were regarded as the most relevant and important method to quantify operational risk, although the other methods, such as causal modeling, risk indicators and escalation triggers were also found to be applicable and useful methods.
Item 6: Operational risk control

- The primary control measures for an operational risk management process are policies, internal controls and reporting. As risk control forms a crucial part of a structured approach to operational risk management process, it is imperative to include these control measures as well.

Item 7: Operational risk structure

- In order to effectively manage operational risk, it is important to have a separate organisational structure for operational risk management. This will ensure a coordinated structured approach to manage operational risk at all management levels.

- It is also imperative that there should be an explicit reporting line for risk managers to the CEO. This should ensure the active involvement of top management in the operational risk management process.

- The allocation of responsibility for operational risk management to a member of the board of directors is found to be imperative for its effective management on a strategic level. This would also ensure the board’s active involvement in the management process and adherence to the requirements of corporate governance.

- The daily management activities of operational risk should not be the responsibility of the banks’ internal audit departments. As the forming of a formal operational risk management structure progresses, the active management role of the internal audit departments should reduce.
**Item 8: Financing of operational risk**

- The primary risk financing techniques were identified as risk transfers and risk retention (funded and unfunded).
- Risk retention (unfunded) is regarded as the least important technique. It should, however, become more applicable with the establishment of a formal risk management process, whereby stricter control measures should allow management to accept the risk as part of the bank’s risk appetite.
- The implementation of a capital charge for operational risk is a necessity and an important part of a bank’s risk management process. However, banks should be more proactive in determining the implications of allocating such a charge to operational risk.
- Banks should also be more proactive in the evaluation of the different approaches to assess capital for operational risk in order to prepare themselves to implement the most applicable method by 2005.
- The internal measurement approach is the preferred method to assess capital for operational risk, although the other two methods, namely, the basic indicator and the standardised methods, are also found to be applicable.

It is evident that a structured approach to operational risk management in a banking environment should be established to ensure its effective and efficient management. In this regard, a framework for a structured approach to operational risk management based on the literature study and the results of the empirical research are recommended in the next chapter.
CHAPTER 6

A FRAMEWORK FOR A STRUCTURED APPROACH TO
OPERATIONAL RISK MANAGEMENT IN A BANKING
ENVIRONMENT

6.1. Introduction

In chapter 5 the results of the research were subjected to statistical and inferential analysis. Deductions were made and conclusions drawn regarding a structured approach to operational risk management in a banking environment. This chapter deals with the development of such a framework based on theoretical concepts from the literature study and the findings from the empirical research.

6.2. Components of a Structured Approach to Operational Risk Management

Based on the literature study and the empirical research, a structured approach to operational risk management in a banking environment should include the following components:

- The primary risk types of a bank.
- A formal definition of operational risk.
- The primary operational risk factors and sub-factors.
- The elements of the operational risk management process, namely, risk identification, risk evaluation, risk control and risk financing.
- Operational risk management structures.
- A capital adequacy methodology for operational risk.
Each of the aforementioned will be discussed in the ensuing sections.

6.2.1. The Primary Risk Types of a Bank

In chapter 2 the classification of risk types was discussed and it was found that different authors classify risks differently. The first objective of this study, therefore, was to determine the primary risk types relevant to a bank. These were identified as credit, market, liquidity, interest-rate and operational risks. It was, furthermore, concluded that reputation, country and legal risks are also regarded as risk types that a bank should manage. According to the empirical research, however, they were not viewed as primary risk types and thus excluded for the purposes of this study. Although the literature study indicated that operational risk, as a primary risk type, is still in a development phase, the empirical research proved and confirmed it as a primary risk type.

Based on the outcome of the empirical research, it was concluded that a structured approach to operational risk management should address all primary risk types, as there is a continuous interaction between them during an enterprise-wide risk management process. Although this does not form part of the scope of this study, it should be an important consideration during the establishment of a structured approach to an operational risk management process.

6.2.2. A Formal Definition of Operational Risk

According to the literature study, there are various definitions of operational risk. It is important, however, for a bank to adopt a formal definition in order to demarcate the key areas that should be managed as part of operational risk. The research revealed that most banks are in a process of developing a definition of operational risk. It was found that a general accepted definition does not exist in
the banking industry, although the Basel Committee is presently in a process of developing and finalising such a definition. It was also found that some banks are waiting for this definition to be finalised before attempting to formalise their operational risk management processes. This is delaying the formalising of the operational risk management processes of these banks.

The fact remains, however, that for banks to succeed in managing operational risk, they must adopt a formal definition that enables them to demarcate the key areas to be managed. In this regard banks could adopt the following definition, formulated in chapter 2:

**Operational risk is the exposure of a bank to potential losses, resulting from shortcomings and/or failures in the execution of operations. These losses may be caused by the internal failures or shortcomings of people, processes and systems as well as the inability of people, processes and systems to cope with the adverse effects of external events.**

An important aspect about the above-mentioned definition is that it comprises people, processes, systems and external events, which demarcate the key areas of operational risk. These will be discussed as part of a structured approach to operational risk in the ensuing sections.

6.2.3. **The Primary Operational Risk Factors**

From the literature study it is evident that there is a general agreement that operational risk comprises the following underlying risk factors:

- People.
- Processes.
- Systems.
- External events.

This viewpoint is confirmed by the empirical research. It can be thus concluded that these risk factors should form an inherent part of a structured approach to operational risk in a banking environment. The factors demarcate the key areas of exposure which should be managed during an operational risk management process.

It is furthermore evident that the aforementioned underlying risk factors of operational risk comprise a variety of sub-factors. Table 6.1 contains examples of these sub-factors.

**Table 6.1: Sub-factors of the Main Underlying Risk Factors of Operational Risk**

<table>
<thead>
<tr>
<th>People</th>
<th>Processes</th>
<th>Systems</th>
<th>External Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incompetence</td>
<td>Errors in procedures</td>
<td>System infiltration</td>
<td>Acts of God</td>
</tr>
<tr>
<td>Negligence</td>
<td>Errors in execution</td>
<td>System failures</td>
<td>External criminal activities</td>
</tr>
<tr>
<td>Human error</td>
<td>Documentation errors</td>
<td>Fraud</td>
<td>Domestic political upheaval</td>
</tr>
<tr>
<td>Low morale</td>
<td>Product complexity</td>
<td>Programming errors</td>
<td>Regulatory and compliance</td>
</tr>
<tr>
<td>High staff turnover</td>
<td>Security risk</td>
<td>Information risk</td>
<td>Legal actions</td>
</tr>
<tr>
<td>Fraudulent activities</td>
<td></td>
<td>Telecommunication risk</td>
<td>Deterioration of reputation</td>
</tr>
<tr>
<td>Lack of training</td>
<td></td>
<td>Obsolescence of systems</td>
<td>Strikes</td>
</tr>
</tbody>
</table>

From the literature study and the empirical research it is evident that there are more sub-factors than those mentioned in table 6.1. At the time of the survey, however, they were viewed as the most important. Although the literature study
showed that the above list is not exhaustive, it is also evident that the importance of sub-factors will depend on a bank’s business exposures. For example, a bank that operates in a politically unstable country will be more exposed to political upheaval than those banks that operate in politically stable countries.

As the sub-factors are often subject to change, it is important that they are identified at an early stage in order to be effectively managed and controlled. The dynamic nature of these sub-factors, however, makes it difficult to include them by specific name in a framework for operational risk. Each bank should rather specify its own sub-risks for inclusion in its framework. It remains important, however, that these sub-risks are considered during an operational risk management process.

6.2.4. The Operational Risk Management Process

The literature study identified the elements of an operational risk management process as risk identification risk evaluation, risk control and risk financing. The empirical research confirmed this. A formal process will ensure the efficient management of operational risk as it will dictate all action steps to be followed and will identify persons or departments responsible for the different steps. It will also ensure a proactive attitude towards the continuous management of operational risk.

6.2.4.1. Risk Identification

Although risk identification can be regarded as the first step of the operational risk management process, it is an ongoing process that must ensure the timeous and continuous identification of new or changing risk exposures.
Various methods that could be used to identify these exposures were identified. According to the findings of the empirical research, the following are the most applicable for risk identification:

- Workshops;
- Brainstorming sessions; and
- Process mapping.

Although these methods were rated to be the most important at the time of the survey, other methods may prove to become more important in the future as the risk factors change.

6.2.4.2. Risk Evaluation

The literature study indicated that once operational risk exposure is identified, it should be evaluated. During this process, the exposure is assessed in terms of likelihood of operational failure and the severity of such a potential loss. Qualitative methods are applied to determine the likelihood of an operational event occurring, while quantitative methods are applied to measure or predict the potential severity of a possible loss-event. The empirical research proved that the qualitative methods to measure operational risk are more readily being implemented by banks compared to the quantitative methods. The proposals of the New Basel Accord of 2001, however, will force banks to implement quantitative methods to measure operational risk, as it will be required to determine the capital charge for operational risk.

According to the empirical research, the current most widely used qualitative methods to measure operational risk are historical data, self-risk assessments and risk mapping/process flows. The method recommended by respondents is self-
risk assessment. This method, however, lacks the ability to quantify operational risk, but it allows the risk factors to be graded into categories of high, medium and low exposures. This categorisation may provide management with an indication of the main focus areas to be managed.

The most widely used quantitative method is the risk indicator method which provides predictive information to facilitate decision-making and enable preventative actions. Other methods such as causal modeling, escalation triggers and loss-event databases are currently not as widely used to quantify operational risk. According to the research, however, the loss-event database is becoming a popular method and is indicated to be the preferred method that banks should apply to quantify operational risk. The following reasons may be assigned to this phenomenon:

- This method is one of a few, if not the only method that provides both financial and quantitative measures of operational risk.
- The collected information can be classified into focus areas (risk factors) and can subsequently be managed by the relevant managers.
- Losses are tracked and trends can be determined to indicate focus areas that must be managed.
- The data can be used as a tool to determine a capital charge for operational risk which is aligned with the latest proposals of the New Basel Accord of 2001.
- The data can also be used as input for other methods, such as causal modeling and eventually the determining of the value-at-operational risk.
From the above-mentioned it is evident that risk evaluation performs an important function in a structured approach to operational risk management in a banking environment.

6.2.4.3. **Operational Risk Control**

After evaluating and measuring operational risk, the next important management step is control. The literature study indicated that control activities should be aimed at reducing or eliminating the possible adverse occurrences of an event or, after it had occurred, minimising the loss to the bank. The control measures that were identified with regard to operational risk are policies, internal controls and reporting.

*Policies* are directives that are supported by procedures and should be used for guidance during the management of operational risk. They should also be communicated to management and staff throughout the organisation to illustrate the bank’s approach to operational risk management. The empirical research indicates that policies are regarded as the most important control measure of operational risk.

*Internal controls* were identified as the second control measure of operational risk. According to the literature study, there are a variety of internal controls that could be implemented to control operational risk. The research indicates that internal controls are important control measures of operational risk which should form part of the operational risk management process.

*Reporting* is another control measure of operational risk and is seen as the process that is aimed at providing accurate and timely information on risk exposures to risk and functional managers. Risk reporting focuses on risk
management information that meets the objectives and needs of different target audiences. The research findings also indicate that risk reporting is already an important control measure of operational risk. Risk reporting is becoming even more important as risk management is being emphasised by, for example, the latest corporate governance initiatives.

It is evident, therefore, that policies, internal controls and reporting are fundamental control measures of operational risk and should form an integral part of the operational risk management of banks.

6.2.4.4. Risk Financing

According to the literature study, risk financing entails reviewing the financial implications of the adverse affects of a risk and determining the financial implications of minimising the risk itself. There are three options available to attain the above-mentioned, namely:

- Risk transfers to third parties.
- Risk retention by means of establishing funds for the financing of losses and/or use of insurance.
- Risk retention without making special provision for losses.

The research indicates that the first two financing techniques are currently the most widely used by banks. As banks improve their risk control, however, they should be able to reduce their operational risk exposures and be in a better position to apply all three methods, depending on the nature of their risks. An effective and efficient operational risk management process should ensure improved controls that could subsequently reduce the risk exposure and the cost of financing the risk.
In order to ensure implementation of the most effective risk financing technique, it is imperative that the element of risk financing be included as an integral part of a structured approach to operational risk.

6.2.5. Operational Risk Management Structures

According to the literature study, a formal organisational structure forms the basis for an effective risk management environment. It allocates responsibilities for the execution of risk management activities at all management levels and provides structured reporting lines. If correctly designed, it will ensure the active involvement of top management, for example, the chief executive officer (CEO) and members of the board of directors in the operational risk management process. The research indicates that it is important to have a separate organisational structure for operational risk management. This is to ensure the coordinated management of operational risk at all management and operating levels.

A formal organisational structure for operational risk management could *inter alia* have the following benefits for a bank:

- Involvement of all personnel, including top management, in the risk management process.
- Specific allocation of responsibilities for managing operational risk.
- Improved control of operational risk in accordance with the bank’s risk appetite which will allow it to make calculated decisions on, for example, the financing of operational risk.
• Reducing the involvement of internal audit in the management of operational risk and assigning it to specialist risk managers.

• Specifying reporting lines between those members involved in operational risk.

• Serving as a basis for a structured approach to operational risk management throughout the organisation.

It is evident that a formal structure for operational risk management will be to the advantage of a bank and should form an integral part of a structured approach to operational risk management in a banking environment.

6.2.6. Capital Adequacy Requirements

Capital adequacy requirements aim to ensure that a bank has sufficient capital available to serve as a buffer against losses. The New Basel Accord of 2001 is focusing on introducing a capital charge for operational risk. The research indicates that relatively few banks are involved in determining a capital charge for their operational risk. This is mainly due to the fact that they are still in the process of establishing their operational risk management structures rather than determining a capital charge for operational risk.

It is, however, imperative that all banks seriously consider the implications thereof and start preparing to adhere to the proposed regulatory requirements related to operational risk. An obvious starting point for banks is to establish a structured operational risk management approach that also includes the consideration of capital adequacy for operational risk.
6.3. **Framework for Operational Risk Management**

Based on the components of operational risk listed in this chapter, a framework for a structured approach to operational risk could be developed. A framework example is depicted in figure 6.1.

The framework comprises the relevant operational risk management components required for a structured approach by a bank. Firstly, it includes the primary risk types of a bank of which operational risk forms part. It also shows that in terms of enterprise-wide risk management, there is an interrelationship between these risk types. Secondly, it provides a formal definition of operational risk that is essential to demarcate the area of the risk that should be managed.

The main underlying operational risk factors, namely people, processes, systems and external events, form the third part of the model. These risk factors indicate the main operational risk exposures of a bank and consist of sub-factors. The four main risk factors could be regarded as the pillars of operational risk. The next crucial concept of a structured approach to operational risk management is the management process. The elements of an operational risk management process are risk identification, risk evaluation, risk control and risk financing. These elements should be applied on an ongoing basis. This ensures the continuous identification and evaluation of the risks as well as the application of risk mitigating and risk financing techniques.

The framework also includes a separate operational risk management structure, reporting lines, the allocation of responsibilities and the involvement of all personnel and top management.
Figure 6.1: Framework of a Structured Approach to Operational Risk Management in a Banking Environment

Continuous Interaction

Credit Risk  Market Risk  Liquidity Risk  Interest-rate Risk

Operational Risk Factors

Systems

Risk Evaluation
Qualitative & Quantitative risk measurement

Risk Control
Policies
Internal controls
Reporting

Continuous Process
Finally, the framework depicts the importance of capital adequacy for operational risk. The latest tendency of regulators to implement a capital charge for operational risk necessitates the inclusion of this concept to ensure a proactive approach by banks to comply with regulatory requirements regarding operational risk.

6.4. Conclusion

All the important components of operational risk management that were identified and included in a framework are:

- The primary risk types of a bank.
- The definition of operational risk based on its primary sub-factors, namely people, processes, systems and external events.
- The elements of an operational risk management process, namely, risk identification, risk evaluation, risk control and risk financing.
- The organisational risk structure and capital adequacy.

The next and final chapter of this study provides an overall summary of findings based on the literature study and empirical research as well as the final conclusions and recommendations.
CHAPTER 7

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

7.1. Introduction

The purpose of the research is to develop a structured approach to the management of operational risk in a banking environment. In order to attain this purpose, the various components of operational risk management were determined by means of a comprehensive literature study and empirical research, where after a framework for such an approach was developed. The study was approached in three phases, namely:

- Phase 1 – A literature study.
- Phase 2 – Empirical research.
- Phase 3 – Development of a framework for a structured approach to operational risk management based on phases 1 and 2.

This chapter, firstly, provides a summary of the literature study and empirical research; secondly, the conclusions are summarised; and finally, recommendations are made on further research to enhance operational risk management in a banking environment.

7.2. Summary of the Study

Operational risk is recognised as a primary risk type in a banking environment along with the other vital risk types such as credit, market, liquidity and interest-rate risks. It does, however, still require some development as a primary risk type as it was found that many undefined risks are currently classified as part of
operational risk. In addition, only a few banks have formal operational risk management structures and processes in place. This impedes the effective management of operational risk as specific responsibility areas as well as processes and procedures are not clearly defined. This points to a “wide” approach to operational risk that may lead to the neglecting of certain crucial aspects and consequent losses to a bank. There is also currently no consensus on a single definition for operational risk. This has led to dissimilar and unrelated risks often being combined for the convenience of management and control. This has also resulted in the combination of risks under a composite name, more descriptive of the product or service than of the underlying risk. The literature study, therefore, firstly focused on the terms: risk, risk management and the risk management process; and then the classification of risks was explored in order to identify all the operational risk factors. The knowledge about the risk factors was used as the basis for the compilation of a definition for operational risk management, namely:

**Operational risk is the exposure of a bank to potential losses, resulting from shortcomings and/or failures in the execution of its operations. These losses may be caused by the internal failures or shortcomings of people, processes and systems as well as the inability of people, processes and systems to cope with the adverse effects of external events.**

The operational risk factors that comprise the essence of the definition are people, processes, systems and external events.

**People**, as an underlying risk factor of operational risk, could include a variety of sub-risks that should be addressed during an operational risk management process. The following sub-risks are the most common:
• Incompetence.
• Negligence.
• Human error.
• Low morale.
• High staff turnover.
• Fraudulent/criminal activities by employees.
• Lack of training.

Banks should proactively identify the sources of people risk in order to manage it as an integral part of the risk management process.

_Systems_ often have implications of complexity and uncertainty as banks develop and adapt to changing circumstances. The following are system exposures that should be managed:

• System infiltration.
• System failures.
• Fraud (Hacking).
• Programming errors.
• Information risk.
• Telecommunication risk.
• Obsolescence of systems.

_Processes_ are regarded as an integral part of operational risk and include the following sub-factors that should be managed:

• Errors in procedures/methodologies.
• Execution errors.
• Documentation errors.
• Product complexity.
• Security risks.

*External events* are usually beyond the direct control and influence of a bank. The following are examples of external events:

• Acts of God.
• External criminal activities.
• Domestic political upheaval.
• Regulatory and compliance.
• Legal actions.
• Business environment changes.
• Deterioration of a bank’s reputation as perceived by the market.
• Strikes.
• Money laundering.

The sub-risks pertaining to the underlying main risk factors do not constitute an exhaustive list of all possible sub-risks due to the fact that they will differ from one bank to another, depending on a bank’s unique situation and risk exposures.

The operational risk management process consists of the following four elements:

• Risk identification that includes risk awareness.
• Risk evaluation that includes risk assessment and risk measuring.
- Risk control that includes issues such as risk reporting, monitoring and risk policies and procedures.
- Risk financing that includes the cost of risk.

The following methods are used to identify operational risk exposures:

- Workshops.
- Brainstorming sessions.
- Questionnaires.
- Process mapping/process flows.
- Comparisons with other organisations.
- Discussions with peers.

Risk evaluation requires an estimate of the probability of an operational loss and the potential size of the loss. The two most used methods to measure operational risk are qualitative in nature. These methods are:

- **Self-risk assessments.** This method assesses the operational risk the organisation is exposed to by means of internal knowledge and experience of the assessors. The identified exposures are then scored in red, yellow and green indicators that indicate the exposures' importance and are then addressed by management.
- **Risk maps/process flows.** This method is a tool for identifying, categorising and analysing operational risks. These activities are performed by means of analysing business processes to identify all the inherent risks and subsequently define the appropriate control measures.
The quantitative methods to measure operational risk were found to be difficult to implement, especially in the case of identifying unexpected risks. However, various methods are used of which the following are the most extensively used:

- **Causal modeling.** This method models the cause/effect data and analyses the relationship between them. It improves the understanding of operational risk and provides a means for performing stress testing and simulations.

- **Risk indicators.** These are quantitative measures of current or historical data. They report on what has happened, focusing on the results and not on the underlying risk factors of operational risk.

- **Escalation triggers.** These may be used to communicate potential problems to management. The starting point for escalation trigger points is a set of risk indicators with set goals or limits. When they reach the goal or limit, these indicators are highlighted and given to the predetermined appropriate business unit to manage.

- **Loss-event database.** This method captures and accumulates individual loss events across business and risk types. It provides both financial and quantitative measures of operational risk.

Although there are various approaches and methodologies to evaluate and measure operational risk, the limitations of each should be taken into account when applied. Therefore, no risk manager should rely on a single aggregate measure as a basis for understanding the full extent of a firm’s exposure to operational risk.

Risk control entails any activity that is aimed at preventing losses, minimising the consequences of losses and dealing with the adverse event in advance or as it occurs.
A bank could consider the following alternatives with regard to the control of risks:

- Put controls in place to limit the possibility of the risk arising;
- Accept the costs of the risk as part of the cost of the business;
- Transfer the risk using insurance or other mechanisms; and
- Avoid the business altogether if the cost is too high.

Operational risk policies and procedures should clearly communicate the risk management organisational structure and should specify the roles and responsibilities of different personnel with respect to risk management. Such policies should also identify the bank’s exposures and should serve as directives on how to manage these exposures in the context of the bank’s strategic plan.

Risk financing entails reviewing the costs and benefits to a bank relating to the actions involved to prevent or minimise the operational risks. Risk-financing mechanisms can be categorised into two broad strategies, namely:

- Pre-loss financing through insurance and retention funding; and
- Post-loss financing by means of cash resources.

Risk transfer and risk retention decisions play a major role in a risk financing programme. When considering such a programme it is important to ensure the use of the right coverage vehicle and to make sure exposures remain limited. It is critical for a successful risk management programme to find the correct ratio between reducing the insurance costs through highly visible and creative alternative risk financing practice and minimising losses through sound control and prevention measures.
The banking world has undergone a series of important changes since the original Basel Accord of 1988 on capital adequacy. Banks have increased their interest in operational losses in order to reduce the large losses, improve general risk awareness and generally contribute to well-run, profitable institutions. The Basel Committee has also renewed their focus on the risk profile of banks, hence the focus on capital charges for operational risk. The New Basel Accord of 2001 also focuses on operational risk and intends to impose a capital charge for operational risk with effect from 2005.

The research methodology used for the gathering and analysis of empirical data includes a theoretical background on research methods and the statistical techniques available to analyse the data. A questionnaire was used to gather the data from local and foreign banks. It comprised open- and close-ended questions. The Likert-type ordinal measuring scale was used to measure the response.

The questionnaire was subjected to a pretest that confirmed its validity and reliability for the purposes of the research.

The returned questionnaires were also subjected to statistical analysis. This included a nonparametric analysis consisting of the analysis of descriptive and inferential data to determine the central tendency of respondents as well as the significant differences of the responses at a 95% confidence level.

The statistical analysis of the results was divided into three parts, namely:

- The analysis of the demographic data to gather information on the respondents.
• The grouping of the questions with a similar underlying construct to simplify the statistical analysis.

• The statistical analysis of the data from the completed questionnaires according to the above-mentioned statistical methodology.

Finally, the literature study and the empirical information were used to develop a framework for a structured approach to operational risk management in a banking environment. This framework may be used by banks to enhance their own operational risk management processes.

7.3. Conclusions

The main conclusions are grouped under the eight identified items, mentioned in chapter 5, namely:

• **Risk Types.** The primary risk types of banks are credit, market, liquidity, interest-rate and operational risks. Although other risks like legal, reputation and country risk are regarded as secondary risk types, they should also form part of a management process.

• **Operational Risk Factors and Definition.** Although most banks differ in their approaches to operational risk management, the primary risk factors were identified and agreed to by the majority of the banks as people, processes, systems and external events. These factors could be used to form the basis of a formal definition of operational risk, which should help to more clearly demarcate the area to be covered by a formal operational risk management process.
There are many sub-factors for each primary operational risk factor. It will be impossible to compile a standardised list of these sub-factors as they would depend on the unique circumstances of a specific bank. It is very important, however, that these sub-factors be identified and managed accordingly to minimise or limit the risk exposures to a bank.

- **Operational Risk Management Process.** A formal operational risk management process could be regarded as a prerequisite for the effective management of operational risk exposures. The elements of such a process are risk identification, risk evaluation, risk control and risk financing. This process is also regarded as ongoing in order to ensure the timely identification of operational risk exposures that should be subjected to risk evaluation to measure and assess them. After evaluating the risk it should be controlled to minimise or eliminate its impact in accordance with the risk appetite of the bank and, finally, it should be subjected to risk financing techniques if necessary.

- **Identification of Risk.** The identification of risk is the first step of a risk management process. It consists of the continuous monitoring of risk exposures to identify potential risk factors that have to be managed.

The current most widely recognised methods to identify operational risks are workshops, brainstorming sessions and process mapping/process flows.
• **Measurement of Operational Risk.** There are two basic approaches to measure operational risk, namely, quantitative and qualitative approaches. Although the measuring of operational risk is still in its early stages of development, banks do recognise its importance. The self-risk assessment method is the most important qualitative method to measure operational risk, while the loss-event database method is the method banks use the most to quantify operational risk.

The importance of measuring operational risk is emphasised by the proposed minimum regulatory capital requirement for operational risk. In order to determine a realistic capital allocation for operational risk, the quantifying of operational risk is a prerequisite and should be the centre of management's focus.

• **Operational Risk Control.** The primary control measures that should be developed and implemented by banks are policies, internal controls and risk reporting. The aim of these control measures should be to reduce, control or contain the risks.

• **Operational Risk Structure.** A separate organisational risk structure for operational risk should be established to ensure a coordinated and structured management approach. Clear allocation of operational risk responsibilities is essential to ensure the appropriate involvement of key role players in the operational risk management process. These role players would include the CEO, board of directors, business managers and internal audit.
A direct reporting line between risk managers and the CEO is important in terms of establishing the bank's risk appetite, making risk financing decisions and ensuring the general involvement of the CEO in the operational risk management process.

The involvement of the board of directors is imperative in the strategic management of operational risk. This will also address the requirements of corporate governance relating to risk management.

The role of internal audit in risk management should be independent of the daily management functions. Internal audit should provide management with the reports regarding the effectiveness of operational risk.

Lastly, it is imperative that business managers be actively involved in operational risk management. This will ensure the awareness of the operational risk exposures that should be addressed in a bank.

**Financing of Operational Risk.** The primary risk financing techniques were identified as risk transfers and risk retention (funded and unfunded).

Risk transfers proved to be a popular risk financing technique. As a bank's risk control measures improve, however, the bank should be prepared to retain a larger percentage of the risk by either making financial provision for it (for example, captives) or accepting the risk without any financial provision. It is crucial,
however, for management to ensure the most cost-effective risk financing technique is applied to mitigate or minimise the effect or potential effect of operational risk exposures.

As regulators prepare to impose a capital charge for operational risk, it is imperative for banks to be actively involved in the process of assessing capital for operational risk. This will allow banks to determine a realistic minimum capital requirement for operational risk which should ensure that economic capital is kept to a minimum to avoid a negative effect on the profit margins.

Furthermore, a positive and proactive approach towards the Basel proposals should ensure that banks are prepared for the implementation of a capital charge for operational risk in 2005.

7.4. Recommendations

To conclude this study, the writer proposes the following recommendations to enhance the establishment of a structured approach to operational risk management in a banking environment:

- The framework for a structured approach should be used by banks to enhance the development of their own operational risk processes. Although individual banks will identify their own operational risk management processes, the framework comprises the major components of operational risk that should be addressed during the development of such a process.
- It is imperative that banks should adopt a formal definition of operational risk, preferably one that is aligned with a definition
that is acceptable to the banking industry. This will add value to a bank’s approach to operational risk as it may then compare its operational risk to that of the industry and adjust it if necessary.

- Banks should establish formal operational risk management structures. Such structures will ensure the physical establishment of operational risk management in banks and the enhancement of formal risk management processes. It will also ensure the correct allocation of responsibilities to personnel involved in managing operational risk as well as their formal reporting lines.

- As the concept of operational risk management is not yet fully established in most banks, it is important to develop and implement a formal training programme for operational risk management. This will enhance the awareness of operational risk in the bank and stimulate the interest in its management.

- All banks should actively participate in the current negotiations with regulators concerning capital adequacy for operational risk. In neglecting to do so, banks may be unprepared to adhere to the regulatory requirements for operational risk.

- All banks should investigate and implement a formal quantitative method to measure operational risk. This will ensure that all operational risks will be addressed in the form of control measures and/or risk financing techniques. Formal measurement should add value when determining a realistic capital charge for operational risk.

During the study, certain concepts which could have an effect on an operational risk management process were identified. As it was not part of the scope of this study, it was not pursued in detail. It could, however, affect the management process pertaining to operational risk and should be taken into account. The
following recommendations relating to these concepts, therefore, may be worthwhile:

- The first aspect that was found to be lagging is that of capital adequacy for operational risk. The assessment of operational risk to determine a capital charge is a contentious issue in the international banking industry. Many questions are still to be researched and answered before it can be implemented by the year 2005. One such a question is the quantification of operational risk.

- Another issue, which affects operational risk management as well as the management of the other risk types, is corporate governance. According to the King 2 Report of 2001, corporate governance, for instance, affects the responsibilities of banks for risk management which should be addressed. Thus, another possible field to be investigated for further research is the influence of the initiatives of corporate governance on the process of risk management in a banking environment.

- Finally, it is also apparent that risks should not be managed in silos. There are many interactions that should take place between areas/departments during the management of primary risk types. With the latest developments of operational risk and its management, it is necessary to determine the interaction of operational risk with the other risk types in an enterprise-wide risk management framework. This is also recommended as a topic to be investigated for further research.

This research by no means provides a final solution to a structured approach to operational risk management in a banking environment. The intention is to enhance the progress of the development of operational risk as a primary risk
type alongside others such as credit, market, liquidity and interest-rate risks. Furthermore, this study aims to stimulate further creative thinking and research to increase the value-adding capabilities which a structured approach to operational risk management may provide to the banking industry as well as other corporate industries.
REFERENCES


Foster, B. 1998. Interview with Mike Clemens, the CEO of the Commerce Exchange Bank. The Journal of Lending and Credit Risk Management, 80(6), February:13.


Rachlin, C. 1998. Operational Risk in Retail Banking: Promoting and Embedding Risk Awareness across Diverse Banking Groups in


ANNEXURE A

June 2001

Dear Respondent

SURVEY ON OPERATIONAL RISK MANAGEMENT

Thank you for taking the time to complete this questionnaire as part of empirical research on operational risk management conducted by the Department of Business Management, Sub-Department Risk Management of the University of South Africa.

The aims of the survey are as follows:

- To determine the status quo regarding operational risk management in the banking industry; and
- To determine the views and opinions of experts/specialists on how certain issues relating to operational risk management in the banking environment should be approached.

The answers to the questionnaire will remain anonymous. It will take about 15 to 20 minutes to complete.

After completing the questionnaire please E-mail it to the following E-mail address, or return it in the provided self-addressed, prepaid envelope:

jackiye@netactive.co.za

If you would like a copy of the results, please indicate accordingly and they will be forwarded to you by 30 September 2001.

Your response by 31 July 2001 will be appreciated.

Kind regards

MR JACKIE YOUNG
UNIVERSITY OF SOUTH AFRICA
ANNEXURE B
QUESTIONNAIRE ON OPERATIONAL RISK MANAGEMENT

This questionnaire consists of three sections. Section 1 concerns demographic information. Section 2 aims to determine the current approach to operational risk management adopted by your bank. Section 3 aims to determine what your bank’s approach towards operational risk management should be, based on your views, experience and knowledge.

Please indicate your appropriate choice by marking the relevant box with a cross (X) or specify your answer under "other".

Section 1: Demographic Information

1. Indicate the type of bank that you are representing
   1.1. Retail
   1.2. Commercial
   1.3. Investment
   1.4. Merchant
   1.5. All the above
   1.6. Other:

2. Indicate your specific portfolio
   2.1. Risk Manager
   2.2. Line Manager
   2.3. Internal Auditor
   2.4. Operational Risk Manager
   2.5. Other (Specify)

3. Indicate your number of years of practical banking experience
   3.1. 0 - 2 years
   3.2. 3 - 4 years
   3.3. 5 - 7 years
   3.4. 8 - 10 years
   3.5. 11 - 12 years
   3.6. 13 - 15 years
   3.7. More than 16 years

4. Does your bank regard itself as a foreign bank to the Republic of South Africa?
   4.1. Yes
   4.2. No

5. If you would like a copy of the results, please indicate your address/E-mail address below

Sections 2 & 3
Please answer the following questions by indicating your answer with a cross (X) in the applicable box according to the following scale or specify your answer under "other":

Scale:
1 = Not at all
2 = To a lesser degree
3 = To a fair degree
4 = To a high degree
5 = Totally
6 = Unsure
Section 2: Your bank's current approach towards operational risk management.

1. To what degree would you rate the following as primary risk types within your organisation?

<table>
<thead>
<tr>
<th>1.1. Credit risk</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2. Market risk</td>
<td></td>
</tr>
<tr>
<td>1.3. Liquidity risk</td>
<td></td>
</tr>
<tr>
<td>1.4. Interest rate risk</td>
<td></td>
</tr>
<tr>
<td>1.5. Country risk</td>
<td></td>
</tr>
<tr>
<td>1.6. Reputation risk</td>
<td></td>
</tr>
<tr>
<td>1.7. Legal risk</td>
<td></td>
</tr>
<tr>
<td>1.8. Operational risk</td>
<td></td>
</tr>
<tr>
<td>1.9. Other:</td>
<td></td>
</tr>
</tbody>
</table>

2. To what degree has your organisation implemented the following as primary factors of operational risk?

<table>
<thead>
<tr>
<th>2.1. People</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2. Processes</td>
<td></td>
</tr>
<tr>
<td>2.3. Systems</td>
<td></td>
</tr>
<tr>
<td>2.4. External factors (e.g. natural disasters, fraud, political pressures etc.)</td>
<td></td>
</tr>
<tr>
<td>2.5. Other:</td>
<td></td>
</tr>
</tbody>
</table>

3. To what degree has your organisation recognised the following people exposures as an important part of operational risk?

<table>
<thead>
<tr>
<th>3.1. Incompetence</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2. Negligence</td>
<td></td>
</tr>
<tr>
<td>3.3. Human error</td>
<td></td>
</tr>
<tr>
<td>3.4. Low morale</td>
<td></td>
</tr>
<tr>
<td>3.5. High staff turnover</td>
<td></td>
</tr>
<tr>
<td>3.6. Fraudulent/criminal activities by employees</td>
<td></td>
</tr>
<tr>
<td>3.7. Lack of training</td>
<td></td>
</tr>
<tr>
<td>3.8. Other:</td>
<td></td>
</tr>
</tbody>
</table>

4. To what degree has your organisation recognised the following process exposures as an important part of operational risk?

<table>
<thead>
<tr>
<th>4.1. Errors in procedures/methodologies</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2. Execution errors</td>
<td></td>
</tr>
<tr>
<td>4.3. Documentation errors</td>
<td></td>
</tr>
<tr>
<td>4.4. Product complexity</td>
<td></td>
</tr>
<tr>
<td>4.5. Security risks</td>
<td></td>
</tr>
<tr>
<td>4.6. Other:</td>
<td></td>
</tr>
</tbody>
</table>

5. To what degree has your organisation recognised the following system exposures as an important part of operational risk?

<table>
<thead>
<tr>
<th>5.1. System infiltration</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2. System failures</td>
<td></td>
</tr>
<tr>
<td>5.3. Fraud (e.g. hackers)</td>
<td></td>
</tr>
<tr>
<td>5.4. Programming errors</td>
<td></td>
</tr>
<tr>
<td>5.5. Information risk</td>
<td></td>
</tr>
<tr>
<td>5.6. Telecommunication risk</td>
<td></td>
</tr>
<tr>
<td>5.7. Obsolescence of systems</td>
<td></td>
</tr>
<tr>
<td>5.8. Other:</td>
<td></td>
</tr>
</tbody>
</table>
6. To what degree has your organisation recognised the following external exposures as an important part of operational risk?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1. Acts of God</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2. External criminal activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3. Domestic political upheaval</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4. Regulatory and compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5. Legal actions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.6. Business environment changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.7. Deterioration of a bank’s reputation as perceived by the market</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.8. Strikes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.9. Money laundering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.10. Other:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

7. To what degree does your organisation recognise the importance implementing a formal risk management process?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

8. To what degree has your organisation adopted a specific definition for operational risk?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

9. To what degree has your organisation recognised the following as important elements of an operational risk management process?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1. Risk identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2. Risk evaluation/measurement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.3. Risk control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.4. Risk financing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.5. Other:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

10. To what degree does your organisation recognise the importance of aligning an operational risk management process with its strategy and objectives?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

11. To what degree is an operational risk management process recognised as an important and integral part of your organisation's overall management process?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

12. To what degree has your organisation recognised the following methods as the most appropriate to identify various risk types?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1. Workshops</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.2. Brainstorming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.3. Questionnaires</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.4. Process mapping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.5. Comparisons with other organisations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.6. Discussions with peers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.7. Other:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

13. To what degree has your organisation recognised the importance of and implemented the following qualitative methods to measure operational risk?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1. Historical data to forecast the likelihood of a potential loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.2. Self-risk assessments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.3. Risk maps/process flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.4. Other:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

14. To what degree has your organisation recognised the importance of and implemented the following quantitative methods to measure operational risk?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1. Causal modeling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.2. Risk indicators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.3. Escalation triggers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.4. Loss-event database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.5. Other:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>
15. To what degree has your organisation recognised the implementation of risk identification as an important ongoing process?  

16. To what degree has your organisation recognised the importance of and implemented the following control measures of operational risk?  
16.1. Policy and procedures  
16.2. Internal controls  
16.3. Risk reporting  
16.4 Other:  

17. To what degree has your organisation established a separate operational risk management structure?  

18. To what degree has a risk manager a direct reporting line to the CEO of your organisation?  

19. To what degree does your organisation involve internal audit to manage operational risk?  

20. To what degree has your organisation involved business managers in an operational risk management process?  

21. To what degree does your organisation regard operational risk management as a function and responsibility of the board of directors?  

22. To what degree has your organisation recognised the importance of and implemented the following risk financing techniques?  
22.1. Risk transfers (to third parties - insurance companies)  
22.2. Risk retention (funded)  
22.3. Risk retention (unfunded)  
22.4. Other:  

23. To what degree has your organisation been involved in determining a regulatory capital allocation for operational risk?  

24. To what degree has your organisation recognised and evaluated the following Basel approaches to assess capital for operational risk?  
24.1. Basic Indicator Approach  
24.2. Standardised Approach  
24.3. Internal Measurement Approach  
24.4 Other:  

25. To what degree does your organisation regard the allocation of a regulatory capital allocation for operational risk, proposed by the Basel Committee, as essential?
Section 3: What should your bank's approach be towards operational risk management.

26. In your opinion to what degree should your bank manage the following as primary risk types within a banking environment?  
<table>
<thead>
<tr>
<th>26.1. Credit risk</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.2. Market risk</td>
<td></td>
</tr>
<tr>
<td>26.3. Liquidity risk</td>
<td></td>
</tr>
<tr>
<td>26.4. Interest rate risk</td>
<td></td>
</tr>
<tr>
<td>26.5. Country risk</td>
<td></td>
</tr>
<tr>
<td>26.6. Reputation risk</td>
<td></td>
</tr>
<tr>
<td>26.7. Legal risk</td>
<td></td>
</tr>
<tr>
<td>26.8. Operational risk</td>
<td></td>
</tr>
<tr>
<td>26.9. Other:</td>
<td></td>
</tr>
</tbody>
</table>

27. In your opinion to what degree should your bank regard the following as primary factors of operational risk management?  
<table>
<thead>
<tr>
<th>27.1. People</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.2. Processes</td>
<td></td>
</tr>
<tr>
<td>27.3. Systems</td>
<td></td>
</tr>
<tr>
<td>27.4. External factors (e.g. natural disasters, fraud, political pressures etc.)</td>
<td></td>
</tr>
<tr>
<td>27.5. Other:</td>
<td></td>
</tr>
</tbody>
</table>

28. In your opinion to what degree should your bank manage the following people exposures as part of operational risk?  
<table>
<thead>
<tr>
<th>28.1. Incompetence</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.2. Negligence</td>
<td></td>
</tr>
<tr>
<td>28.3. Human error</td>
<td></td>
</tr>
<tr>
<td>28.4. Low morale</td>
<td></td>
</tr>
<tr>
<td>28.5. High staff turnover</td>
<td></td>
</tr>
<tr>
<td>28.6. Fraudulent/criminal activities by employees</td>
<td></td>
</tr>
<tr>
<td>28.7. Lack of training</td>
<td></td>
</tr>
<tr>
<td>28.8. Other:</td>
<td></td>
</tr>
</tbody>
</table>

29. In your opinion to what degree should your bank manage the following process exposures as part of operational risk?  
<table>
<thead>
<tr>
<th>29.1. Errors in procedures/methodologies</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.2. Execution errors</td>
<td></td>
</tr>
<tr>
<td>29.3. Documentation errors</td>
<td></td>
</tr>
<tr>
<td>29.4. Product complexity</td>
<td></td>
</tr>
<tr>
<td>29.5. Security risks</td>
<td></td>
</tr>
<tr>
<td>29.6. Other:</td>
<td></td>
</tr>
</tbody>
</table>

30. In your opinion to what degree should your bank manage the following system exposures as part of operational risk?  
<table>
<thead>
<tr>
<th>30.1. System infiltration</th>
<th>1 2 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.2. System failures</td>
<td></td>
</tr>
<tr>
<td>30.3. Fraud (e.g. hackers)</td>
<td></td>
</tr>
<tr>
<td>30.4. Programming errors</td>
<td></td>
</tr>
<tr>
<td>30.5. Information risk</td>
<td></td>
</tr>
<tr>
<td>30.6. Telecommunication risk</td>
<td></td>
</tr>
<tr>
<td>30.7. Obsolescence of systems</td>
<td></td>
</tr>
<tr>
<td>30.8. Other:</td>
<td></td>
</tr>
</tbody>
</table>
31. In your opinion to what degree should your bank manage the following external exposures as part of operational risk?

- Acts of God
- External criminal activities
- Domestic political upheaval
- Regulatory and compliance
- Legal actions
- Business environment changes
- Deterioration of a bank’s reputation as perceived by the market
- Strikes
- Money laundering
- Other:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

32. In your opinion to what degree should your bank implement a formal risk management process?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

33. In your opinion to what degree should your bank adopt a formal definition of operational risk?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

34. In your opinion to what degree should your bank regard the implementation of the following elements of an operational risk management process as important?

- Risk identification
- Risk evaluation/measurement
- Risk control
- Risk financing
- Other:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

35. In your opinion to what degree should your bank’s operational risk management process be aligned with its strategy and objectives?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

36. In your opinion to what degree should your bank’s operational risk management process be regarded as an important and integral part of its overall management process?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

37. In your opinion to what degree should your bank recognise the importance of the following methods to identify various risk types?

- Workshops
- Brainstorming
- Questionnaires
- Process mapping
- Comparisons with other organisations
- Discussions with peers
- Other:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

38. In your opinion to what degree should your bank recognise and implement the following qualitative methods to measure operational risk?

- Historical data to forecast the likelihood of a potential loss
- Self-risk assessments
- Risk maps/process flows
- Other:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>
39. In your opinion to what degree should your bank recognise and implement the following quantitative methods to measure operational risk? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.1. Causal modeling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39.2. Risk indicators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39.3. Escalation triggers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39.4. Loss-event database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39.5. Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

40. In your opinion to what degree should your bank recognise the importance and manage operational risk as an ongoing process? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

41. In your opinion to what degree should your bank recognise and implement the following control measures of operational risk? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.1. Policy and procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41.2. Internal controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41.3. Risk reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41.4 Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

42. In your opinion to what degree should your bank establish a separate operational risk management structure? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

43. In your opinion to what degree should your bank’s risk manager have a direct reporting line to the CEO? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

44. In your opinion to what degree should internal audit be involved and responsible for operational risk management of your bank? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

45. In your opinion to what degree should business managers be involved in an operational risk management process? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

46. In your opinion to what degree should the function of operational risk management be regarded as a function and responsibility of the Board of Directors? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

47. In your opinion to what degree should your bank recognise the importance and implementation of the following risk financing techniques? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.1. Risk-transfers (to third parties - insurance companies)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47.2. Risk retention (funded)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47.3. Risk retention (unfunded)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47.4. Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

48. In your opinion to what degree should your bank be involved in determining a regulatory capital allocation for operational risk? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

49. In your opinion to what degree should your bank recognise and implement the following Basel approaches to assess capital for operational risk? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.1. Basic Indicator Approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49.2. Standardised Approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49.3. Internal Measurement Approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49.4. Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

50. In your opinion to what degree should your bank recognise the importance of and necessity to implement a minimum capital requirement for operational risk? 

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

THANK YOU
ANNEXURE C

OPERATIONAL RISK MANAGEMENT - DIAGNOSTIC QUESTIONNAIRE

As a respondent of the survey on operational risk management, it will be appreciated if you could also answer the following diagnostic questions relating to the questionnaire by marking the appropriate block with a cross (X), or by commenting in the space provided:

1. How many minutes did you take to complete the questionnaire (undivided attention)?
   1.1. 0 to 10 minutes
   1.2. 10 to 15 minutes
   1.3. 15 to 20 minutes
   1.4. 20 to 40 minutes
   1.5. More than 40 minutes

2. To what degree did the questionnaire, as a whole, interest you to respond and motivate you to complete it?
   2.1. To no degree
   2.2. To a lesser degree
   2.3. To a fair degree
   2.4. To a high degree
   2.5. Totally

3. To what degree was the language understandable?
   3.1. To no degree
   3.2. To a lesser degree
   3.3. To a fair degree
   3.4. To a high degree
   3.5. Totally

4. How would you describe the questions as applicable to operational risk management?
   4.1. Not applicable
   4.2. Applicable
   4.3. Totally applicable

5. Please list the question numbers which you regard as not applicable

6. Are the instructions to complete the questionnaire clear?
   6.1. Yes
   6.2. No

7. If your answer is no, please indicate where you experienced problems and what changes you would recommend

8. In your opinion to what degree do the questions follow a logic sequence?
   8.1. To no degree
   8.2. To a lesser degree
   8.3. To a fair degree
   8.4. To a high degree
   8.5. Totally
9. In your opinion to what degree is the scale applicable to the questions?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1. To no degree</td>
<td></td>
</tr>
<tr>
<td>9.2. To a lesser degree</td>
<td></td>
</tr>
<tr>
<td>9.3. To a fair degree</td>
<td></td>
</tr>
<tr>
<td>9.4. To a high degree</td>
<td></td>
</tr>
<tr>
<td>9.5. Totally</td>
<td></td>
</tr>
</tbody>
</table>

10. In your opinion to what degree did you understand the aim of the questionnaire?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1. To no degree</td>
<td></td>
</tr>
<tr>
<td>10.2. To a lesser degree</td>
<td></td>
</tr>
<tr>
<td>10.3. To a fair degree</td>
<td></td>
</tr>
<tr>
<td>10.4. To a high degree</td>
<td></td>
</tr>
<tr>
<td>10.5. Totally</td>
<td></td>
</tr>
</tbody>
</table>

11. In your opinion was the questionnaire too long?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1. Yes</td>
<td></td>
</tr>
<tr>
<td>11.2. No</td>
<td></td>
</tr>
</tbody>
</table>

12. Did you experience any problems when you completed the questionnaire electronically?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1. Yes</td>
<td></td>
</tr>
<tr>
<td>12.2. No</td>
<td></td>
</tr>
</tbody>
</table>

13. If yes, please name these problems

THANK YOU