AN INVESTIGATION INTO OPERATIONAL RISK MITIGATION IN UK RETAIL BANKS

A Thesis submitted in partial fulfilment of

the requirement for the degree of

Doctor of Business Administration

by

Keith Blacker

Henley Management College / Brunel University

October 2001

ABSTRACT

This research studies a growing area of interest in financial services, namely operational risk management. The use of the term operational risk has grown in importance in financial services over the last ten years for a number of reasons, not least of which is the catastrophic failure of Barings bank in 1995. The failure of Baring's management to manage its operational risk exposures was one of the main factors behind the collapse. This study is focused on the UK retail banking industry and looks specifically at how these banks mitigate their operational risk exposures.

The first problem with operational risk is finding an agreed and accepted definition within the financial services community. It is typically described as the potential for loss arising from inadequate or failed internal processes, people and systems or external events. It is thus an umbrella term covering a number of risk categories such as legal risks, people risks, information technology risks, compliance risks and so on.

The Basle Committee on Banking Supervision, a Committee of banking supervisory authorities established by the central-bank Governors of the Group of Ten countries in 1975, published in January 2001 a draft capital accord which requires, inter alia, banks to set aside capital to cover their operational risk exposures. This accord resulted from a number of discussion documents issued by Basle, which focused increasing attention on the need for adequate management of operational risks. There is, and continues to be, mounting pressure on bank management to ensure that operational risk exposures are being mitigated effectively. This provided the impetus for the research, which is the first independently sponsored study of how UK retail banks have established their operational risk management frameworks, which in turn provide the basis for mitigating their operational risk exposures.

The research is inter-disciplinary exploring the main players in operational risk management: Internal Audit, the Risk Management Unit and Operational Management themselves. Since the process of mitigating an operational risk involves making a decision, theoretical propositions in this area established the foundations from which the fieldwork could be undertaken. The design for the study uses multiple case studies to answer the research questions and establish 'core practice' in operational risk mitigation. Interviews were held with practitioners from the main players in operational risk management cited above. Four leading UK retail banks were selected as representatives of the industry.

The research supports the conclusions of Basle and others that the responsibility for operational risk management, and therefore mitigation, rests with operational managers. The analysis illustrates, however, that they do not do this in isolation but are assisted by other 'experts'. A model of operational risk mitigation is proposed illustrating the complexity of the decision making process which is directly related to the nature and the scale of the operational risk identified. An operational risk mitigation checklist is suggested to help operational managers determine the feasibility of the proposed mitigation tactic together with a high-level review document for auditing the Operational Risk function. The thesis concludes by identifying some of the possibilities for research in this new and developing field.

TABLE OF CONTENTS

ABSTRACT ..... *ii*
TABLE OF CONTENTS ..... *iii*
LIST OF FIGURES ..... *vii*
LIST OF TABLES ..... *viii*
DEDICATION ..... *ix*
ACKNOWLEDGEMENTS ..... *x*

1. INTRODUCTION 1

1.1 BACKGROUND TO THE RESEARCH 1
1.1.1 Basle Committee on Banking Supervision *1*
1.1.2 A Framework for Risk Management *2*
1.1.3 Definition of Operational Risk *4*
1.1.4 Operational Risk Management in UK Retail Banks *6*
1.2 FRAMEWORK OF THE RESEARCH 8
1.2.1 Lack of Prior Research *8*
1.2.2 Focus of the Research *9*
1.2.3 The Research Questions *10*
1.3 RESEARCH DESIGN 11
1.3.1 Case study Methodology *11*
1.3.2 An Overview of the Research Design *12*
1.4 SCOPE OF THE RESEARCH 14
1.5 POSITIONING OF THE RESEARCHER 15
1.5.1 The Researcher's Objectives *15*
1.5.2 The Researcher's Bias *15*
1.5.3 Choice of Topic *17*
1.6 CONTRIBUTION TO KNOWLEDGE 18
1.7 STRUCTURE OF THE THESIS 20

2. LITERATURE REVIEW 21

2.1 INTRODUCTION 21
2.1.1 Disciplines covered by the Literature Review *21*
2.1.2 Focus on the Management of Risk *22*
2.1.3 Sources of Literature *25*
2.1.4 The Role of Theory *25*
2.2 BANKING 26
2.2.1 Industry Structure in UK Retail Banking *26*
2.2.2 Competition *30*
2.2.3 Distribution and Service *33*
2.2.4 The Regulatory Environment *36*
2.2.5 Information Technology *40*
2.2.6 Other Issues for Retail Bank Management *41*
2.2.7 Risk Management in the Current Environment *43*
2.2.8 Implications for Operational Risk Management *46*
2.2.8 Summary *47*
2.3 AUDITING 48
2.3.1 Internal Auditing *48*

2.3.2 External Auditing *51*
2.3.3 Internal Control *53*
2.3.4 Internal Control in Banking *59*
2.3.5 Audit Techniques and Risk *61*
2.3.6 Fraud *65*
2.3.7 Corporate Governance *67*
2.3.8 Implications for Operational Risk Management *68*
2.3.9 Summary *69*
2.4 RISK MANAGEMENT 70
2.4.1 The Concept of Risk and Risk Management *70*
2.4.2 Risk Management Framework *74*
2.4.3 Risk Perceptions and Decision Making *78*
2.4.4 Focus on Operational Risk *82*
2.4.4.1 Reviewing the definition of Operational Risk 82
2.4.4.2 The Increasing Importance of Operational Risk Management 86
2.4.4.3 Operational Risk and Internal Control 89
2.4.4.4 Operational Risk Mitigation 90
2.4.4.5 The Quantification of Operational Risk 92
2.4.4.6 Regulatory Issues 94
2.4.4.7 Operational Risk Management Roles 96
2.4.5 Summary *97*
2.5 MANAGEMENT AND ORGANISATIONS 99
2.5.1 Theories of Management and Organisations *99*
2.5.2 The Organisation and its Environment *103*
2.5.3 Decision Making in the Organisation *104*
2.5.4 Barriers to Decision Making *109*
2.5.5 Implications for Operational Risk Management *110*
2.5.6 Summary *111*
2.6 SUMMARY OF THE LITERATURE REVIEW 112
3. METHODOLOGY 116
3.1 METHODOLOGY – IN OUTLINE 118
3.2 RESEARCH METHODS IN PERSPECTIVE 121
3.2.1 Metaphysics and Research Paradigms *121*
3.2.2 Qualitative Methods *125*
3.2.3 Quantitative Methods *127*
3.2.4 Case Study Methods *129*
3.2.5 Case Study Methods in Business Research *132*
3.2.6 Strengths and Weaknesses of Case Studies *134*
3.3 RESEARCH DESIGN FOR THIS STUDY 136
3.3.1 Research Design *136*
3.3.2 Preliminary Research Model *140*
3.3.3 Critical Incident Techniques *144*
3.3.4 Quality of the Research Design *145*
3.4 SELECTION OF CASES FOR STUDY 147
3.4.1 Sampling *147*
3.4.2 Study Population *149*
3.4.3 Unit of Analysis *150*
3.4.4 Organisational Secrecy *150*
3.5 LIMITATIONS OF THE RESEARCH DESIGN 151

4. CASE STUDIES 154
4.1 CASES STUDIED 154
4.1.1 Selection Criteria *154*
4.1.2 Managers Interviewed *155*
4.2 CASE STUDY METHODS 157
4.2.1 Data Collection *157*
4.2.2 Case Study Protocol *160*
4.2.3 Pilot Case Study *160*
4.2.4 Data Analysis *161*
4.2.5 Drawing Conclusions *164*
4.3 CASE SUMMARIES 166
4.3.1 Common Themes *166*
4.3.2 Major Differences between the Banks *168*
5. STUDY FINDINGS 171
5.1 INTRODUCTION 171
5.2 OPERATIONAL RISK MANAGEMENT 172
5.2.1 Defining Operational Risk *172*
5.2.2 Operational Risk Management in the Organisation *175*
5.2.3 The Role of the Operational Risk Management Function *178*
5.2.4 Operational Risk Management Techniques *183*
5.2.5 Operational Risk Identification *187*
5.2.5.1 Responsibility 188
5.2.5.2 Process 189
5.2.5.3 Data 191
5.2.6 Operational Risk Appraisal *192*
5.2.6.1 Responsibility 193
5.2.6.2 Process 195
5.2.6.3 Data 197
5.3 OPERATIONAL RISK MITIGATION 198
5.3.1 Responsibility for Operational Risk Mitigation *198*
5.3.2 Operational Risk Mitigation – exploring the tactics used *200*
5.3.3 Operational Risk Mitigation – deciding what to do *205*
5.3.4 Operational Risk Mitigation – the problems faced by management *208*
5.3.5 Operational Risk Mitigation – critical incidents *210*
5.4 OPERATIONAL RISK – QUANTIFICATION AND TRAINING 215
5.4.1 Quantification *216*
5.4.2 Training *218*
5.5 SUMMARY OF FINDINGS 220
6. ANALYSIS AND IMPLICATIONS FOR MANAGEMENT 223
6.1 INTRODUCTION 223
6.2 ORGANISATIONAL IMPLICATIONS 223
6.2.1 Implications for the Board *223*
6.2.2 Risk Management Committee *225*
6.2.3 The Operational Risk Manager *227*
6.2.4 Integrated Risk Management *228*
6.3 IMPLICATIONS FOR OPERATIONAL MANAGEMENT 231
6.3.1 Operational Risk Management *231*

6.3.2 Operational Risk Mitigation *233*
6.3.3 Training *234*
6.4 IMPLICATIONS FOR THE OPERATIONAL RISK FUNCTION 235
6.4.1 Risk-mapping framework *235*
6.4.2 The role of the operational risk function *237*
6.4.3 Quantification *238*
6.5 IMPLICATIONS FOR INTERNAL AUDIT 240
6.5.1 The role of Internal Audit *240*
6.5.2 Risk-based auditing *242*
6.6 CONCLUSIONS ABOUT THE RESEARCH PROBLEM 243
6.7 SUMMARY 249

7. SUMMARY 251

7.1 SUMMARY OF THE RESEARCH 251
7.2 LIMITATIONS OF THE RESEARCH 255
7.3 SUGGESTIONS FOR FURTHER RESEARCH 256

APPENDICES 259

APPENDIX A PENSIONS MIS-SELLING IN THE UK – A CASE STUDY 259
APPENDIX B CASE STUDY PROTOCOL 262
APPENDIX C EXAMPLE OF OPERATIONAL RISK ASSESSMENT FORM 278
APPENDIX D CRITICAL INCIDENTS 280
APPENDIX E HIGH LEVEL REVIEW DOCUMENT FOR AUDITING THE OPERATIONAL RISK FUNCTION 283
APPENDIX F CHECKLIST FOR MITIGATING OPERATIONAL RISKS 285

BIBLIOGRAPHY 288

LIST OF FIGURES

Figure 1 Simple Risk Management model....3
Figure 2 A priori operational risk mitigation model....13
Figure 3 The boundaries and academic disciplines of the study....22
Figure 4 Forces driving change in financial services....27
Figure 5 Distribution Channel Strategies....33
Figure 6 Internal Control Framework....57
Figure 7 Key Elements of an integrated risk management and internal auditing model....62
Figure 8 Internal Audit micro risk assessment....64
Figure 9 Risk Management Model....75
Figure 10 Risk Management Framework highlighting possible mitigation strategies....76
Figure 11 Risk perception formulation model....78
Figure 12 The process/risk/control equation....85
Figure 13 Relationship between core elements of operations management....102
Figure 14 Organisational culture and managers decision-making ability....110
Figure 15 Structure of section 3 showing sectional links....117
Figure 16 Preliminary Risk Mitigation Model....141
Figure 17 Sequential flow of Research Findings....171
Figure 18 Integrated Operational Risk Management....230
Figure 19 Proposed Operational Risk Management model....245

LIST OF TABLES

Table 1 Distribution/network hierarchy in Financial Services 35
Table 2 Comparison of Basle 1988 Accord and Proposed New Accord 38
Table 3 Broad Elements of the Internal Control Structure 58
Table 4 Reinventing Risk Management 71
Table 5 The Research Process 123
Table 6 Interpretive Paradigms 124
Table 7 Breakdown by research intent/methodology among listed cases in Operations Management Journal . 134
Table 8 Strengths and Weaknesses of Case Studies 135
Table 9 Relevant Situations for Different Research Strategies 136
Table 10 Research Design: Phase/Date/Process/Documentation 140
Table 11 Case Study Tactics for Four Design Tests 146
Table 12 Limitations of the Research Design 152
Table 13 Table of managers interviewed 157
Table 14 Issues in assessing the quality of the research conclusions 165
Table 15 Major differences between the banks 169
Table 16 Definitions of Operational Risk 173
Table 17 The Operational Risk Management Functions in the Organisation 176
Table 18 Role of the Corporate Operational Risk functions 180
Table 19 Operational Risk Management techniques 184
Table 20 Risk Mapping Frameworks - data output 185
Table 21 Operational Risk Identification: data analysis 188
Table 22 Operational Risk Appraisal: data analysis 193
Table 23 Operational Risk Mitigation responsibility: data analysis 199
Table 24 Operational Risk Mitigation tactics: data analysis 202
Table 25 Operational Risk Mitigation selection procedures and follow-up: data analysis 206
Table 26 Operational Risk Mitigation barriers: data analysis 209
Table 27 Operational Risk Quantification: data analysis 216
Table 28 Operational Risk Training: data analysis 218
Table 29 Phases of the risk management models compared 246

DEDICATION

To

Nicola and Paul

"Success comes in cans"

I love you both

ACKNOWLEDGEMENTS

Many people have helped me during the last four years of researching operational risk. For some it may just have been a five-minute conversation about a particular point of concern whilst others have been providing advice and encouragement throughout. I am grateful to them all.

I have been especially fortunate with my two supervisors who together have provided me with constant support throughout. Acting out the roles of friend, critic, mentor or coach (to name but a few) is no easy task when one is busy with a multitude of other work pressures. Pat McConnell has been a constant source of inspiration with his help, encouragement and attention to detail.....and all of this done across cyberspace. Roger Mills has guided me through the process, kept me focused in the right areas and offered support whenever I have asked for it. I am grateful to you both.

Having been in operational management myself, I know first-hand how busy and demanding the job can be. Managers are busy people. I am grateful to all those in the banks I have worked with who found the time to meet with me. An extra word of thanks goes to those who acted as the main contact and organised all the diary arrangements. Without your help this study would never have been completed.

Finally, I would like to thank my wife, Sue, for the unequivocal support she has shown whilst I have been undertaking this research. I could never have gone through this process without your love, patience and understanding.

1. INTRODUCTION

This section provides background to the research and introduces the research questions. Case studies provide the methodological framework for this study and an overview of the research design is given together with some information about the author and his background. The section concludes with a discussion of the contribution to knowledge and the structure of the thesis.

1.1 Background to the Research

1.1.1 Basle Committee on Banking Supervision

"In an effort to encourage better risk management practices, the Committee is keenly interested in efforts by Institutions to better mitigate and manage operational risk".

This quote from the Operational Risk Supporting Document to the New Basle[1] Capital Accord (Basle 2001) encapsulates the aim (encourage better risk management practices) and focus (operational risk mitigation) of this research study. The Basle Committee on banking Supervision published its first Capital Accord document in 1988 (Basle 2001) and it is now in force in over 100 countries. In the last 13 years much has changed in the banking world. Barings[2] and other major frauds (see McKechnie and Howell 1998 for

[1] The Basle Committee on Banking Supervision is a Committee of banking supervisory authorities which was established by the central-bank Governors of the Group of Ten countries in 1975. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom and the United States. It usually meets at the Bank for International Settlements in Basle.

[2] Whilst the recent demise of Barings sent shock waves through the banking system, it is not the first time the bank has had financial problems. In 1890 Barings was found to be in difficulties resulting from swollen commitments and temporary illiquid resources, particularly in South American securities. A guarantee of

examples) highlight the dangers of not managing risk effectively. Examples of diversification in UK retail banking (Brown 1992) illustrate the extent to which banks are moving into new business areas, in this case insurance, thus creating additional risks. In the UK environment, director's obligations vis-à-vis effective risk management have manifested themselves in other regulatory pronouncements (ICAEW 1999), which also affect banks.

Basle's proposals recognise the changing climate and are aimed at ensuring that all banks maintain sufficient regulatory capital to cover the underlying risks they face, no matter what the source.

1.1.2 A Framework for Risk Management

In 1916 Henry Fayol's work "Administration industrielle et générale[3]" established six organisational groupings for the activities of a company:

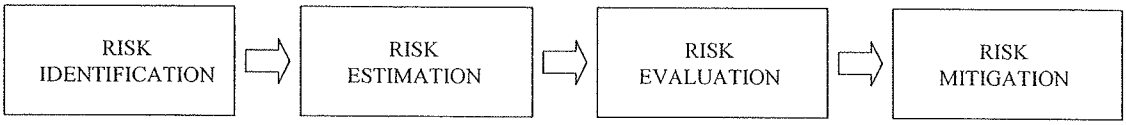
1. Technical (engineering, production, manufacture, adaptation)
2. Commercial (buying, selling, exchange)
3. Financial (search for and optimum use of capital)
4. Security (protection of assets and personnel)
5. Accounting (stocktaking, balance sheets, costs, statistics)
6. Managerial (planning, organising, commanding, coordination, controlling)

Barings' contingent liabilities was shared in by a large number of banks, and, although grave disturbance resulted, the crisis was overcome without panic or serious interruption to the conduct of general banking business (Crick and Wadsworth 1936 p. 38)

[3] The first English translation appeared in 1929 with a revised edition appearing some 20 years later (see Fayol 1949)

The Security function he discussed had, as its objective, "to safeguard property and persons against theft, fire and flood, to ward off strikes and felonies and broadly all social disturbances liable to endanger the progress and even the life of the business" (Fayol 1949 p.4). Subsequent writers, who have placed Fayol's work within today's body of management theory (for example Gray 1984), see a major component of security as being risk management, which involves "exposure identification, risk evaluation, risk control and risk financing" (Gray 1984). This establishes a framework for the management of risk within an organisation and other authors (Acs 1985, White 1995, Sadgrove 1996, Shackleton 1997, Harris-Jones 1998) have identified the same basic principles, which may be summarised in a simple model as shown in Figure 1.

Figure 1 Simple Risk Management model



Source: Various

White (1995) defines the first three terms as:

> Risk Identification - perceiving hazards, identifying failures, recognising adverse consequences;
>
> Risk Estimation - estimating risk probabilities, describing the risk, quantifying the risk;
>
> Risk Evaluation - estimating the impact of the risk, judging acceptability of the risk, comparing risks against benefits.

Risk Mitigation is then the action taken once the identification, estimation and evaluation processes have taken place. The principal objective of risk mitigation is to adjust the level

of risk faced by the business until it is acceptable in terms of the risk/reward criteria adopted by the Board (Harris-Jones 1997).

Risk management encompasses all facets of risk within a business. A review of the literature found many different types of business risks[4] and a growing interest being taken by the established consultancy firms in the generic area of risk management[5]. A recent survey report suggests that companies are losing millions of pounds a year because they fail to manage risk correctly (PriceWaterhouseCoopers 1998).

1.1.3 Definition of Operational Risk

There is no agreed definition of operational risk (Basle 1998a, Blacker 1998). This may seem somewhat paradoxical given that the common features of operational risk have existed in companies for many years. Banks have tended to produce their own definitions and a number have taken the Basle (1998a) definition as the start point and produced variations on this theme. Basle (2001) have recently adopted the definition proposed by the British Banking Association and PriceWaterhouseCoopers (BBA 1999a) thus:

"The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or external events" – Basle (2001)

---

[4] The term business risk includes all risks faced by an organisation including financial risk, market risk, credit risk, operational risk, legal risk, reputational risk and project risk. This is not an exhaustive list since different definitions of these types of risks exist. The first issue faced by an organisation who wishes to manage its total business risk exposure is to decide what types of risk are included vis-à-vis its own business environment

[5] Andersen Consulting have produced their own Business Risk Model™ (ICAEW 1998)

It is interesting to note that this definition of operational risk uses the word risk within it. This presupposes that the reader has an understanding of the concept of risk in the first place which some would argue is unhelpful when defining a term.

The definition illustrates that the focus is on a loss resulting from a breakdown (failure) in the internal controls (systems/processes) that should be *designed to mitigate the risks in the first place* (my italics). This breakdown can occur for a variety of reasons, including, as quoted, people or management failure, non-compliance with regulations, and so on. Equally, a breakdown can occur because there is no control (or controls) in place to reduce the possibility of the risk occurring. The definition also recognises the effect that external events can have in giving rise to operational risk. External events might include systemic risk (an external loss affecting multiple institutions simultaneously with broad consequences), exposure to other industry participants (for example, custodians or exchanges), physical or natural disasters, or a change in regulation/law/accounting /tax beyond the institution's control (BBA 1999a).

This definition also focuses exclusively on the negative or downside aspects of risk. Positive risk, whilst probably an oxymoron from a language point of view, is not considered an appropriate concept in the context of operational risk although the author considers that under certain circumstances the decision taken to mitigate an operational risk may bring benefits, for example, outsourcing. This is a view shared by Basle (2001).

1.1.4 Operational Risk Management in UK Retail Banks

"The real value of what is emerging with operational risk management is the recognition that it is not wrong to have an operational risk exposure, as long as you understand it and can say it's not cost effective to the business to introduce controls"

The above quote, made by one of the risk managers interviewed in this study, encapsulates the essence of operational risk management. This study focuses on operational risk management in UK retail banks, with particular emphasis on the mitigation phase. The UK retail banking industry was chosen for five reasons:

1. There is growing pressure on the regulators of UK banks to ensure that they inspect the adequacy of Banks' risk management frameworks and internal control mechanisms (Basle 2001, Basle 1998c, IOSCO 1998) to counteract (inter alia) operational risk exposures;
2. The corollary to the latter point is the growing pressure on the senior management of UK retail banks to ensure it has established adequate risk management frameworks and internal control mechanisms to counteract (inter alia) operational risk exposures;
3. UK retail banks are likely to have common operational risk problems since they have a common set of products and systems within which operational risk may occur;
4. The opportunity for risk related problems is greater in retail banks, compared to say investment banks, because of the numbers of people and systems involved;
5. The author's knowledge of the dynamics of the financial services industry.

Operational risk was chosen since a number of authors have confirmed the view of Thompson and Frost (1997) that the "management of operational risk is still in its

infancy" (Gandy 1997, Parsley 1996 and Hoffman and Johnson 1996). Much of the academic literature concerning the management of banking risks has focused on market risk and credit risk with operational risk being ignored (Tschoegl 2000). This makes it an interesting and fruitful area for research since it relates to a practical and current problem facing management.

Risk Mitigation was selected in order to focus the research into one area which could be seen as one of the most important daily challenges facing management, i.e. how best to reduce the operational risk exposures identified through the risk management model. Risk identification, evaluation and estimation are all important phases of risk management, but unless conscious risk mitigation strategies are deployed it may all be to no avail. The effect of not having effective risk mitigation strategies can be catastrophic as was highlighted at Barings[6]. In financial terms, the Baring's case, however, has been overshadowed by the $3.265 billion bailout of the Long-Term Capital Management (LTCM) hedge fund in 1998. The failure of LTCM was the result of the ultimate but ill-judged application of "one of the most innovative piece of mathematics over the last 30 years, coupled to a genius for marketing, at the expense of operational risk management" (Smallman 2000). Appendix A provides an example of a brief case study on a well-publicised operational risk incident which affected UK retail banks: the pensions mis-selling scandal. This incident is useful to examine because it is in the public domain, has a significant financial impact and provides a perfect opportunity to examine the mitigating actions that have taken place to prevent a re-occurrence.

[6] For a perpetrator's view of the fraud see Leeson (1996)

1.2 Framework of the Research

1.2.1 Lack of Prior Research

Citing Merton (1995), McConnell (1996) noted that "risk management of financial institutions and the role of capital is a rich and topical subject from the perspectives of both academics and practitioners". Tufano (1996) avers that "academics know very little about corporate risk management practices" because of the limitations of obtaining hard empirical data.

Risk may be viewed as the unwanted future event which, on a small scale, can happen on a daily basis but which, when they hit the headlines, can lead to firms losing significant sums of money. As was witnessed by the events at Barings, the consequences of inadequate risk management can even lead to the collapse of a whole company. The fact that inadequate operational risk management and, in particular, inadequate operational risk mitigation can lead to an impact on the bottom-line further highlights the importance of research into the area of risk.

A review of the literature found only one journal paper which deals with risk mitigation strategies in Financial Institutions (Oldfield and Santamero 1997) and this was focused on asset portfolios with only a passing reference to operational risk. In the paper, operational risk is defined as "the problems associated with accurately processing, settling, and taking or making delivery on trades in exchange for cash. It also arises in record keeping, computing correct payment amounts, processing system failures, and complying with

various regulations". This variety of activities suggests that there is no one best way to mitigate operational risk and there is unlikely to be any consensus about the most appropriate way forward.

1.2.2 Focus of the Research

The origins of the term retail bank can be traced back to 1983 when the Bank of England (1983) created a new "retail banks group" for statistical reporting purposes. The key to being in this category was the provision of extensive retail services. Further insight was given by the Bank of England (1991) when retail banks were a "group which broadly comprises banks which have extensive branch networks in the United Kingdom and participate in the UK Clearing System". All such banks are supervised by the Bank of England and any new 'person' entering into this category (for example, a demutualising building society) would have to be authorised by the Bank of England to carry on such business[7]. For the purposes of the research, a UK retail Bank has five characteristics. It is a retail bank when it: (1) is under the jurisdiction of the Bank of England; (2) is regulated by the Financial Services Authority; (3) has a large customer base; (4) is a member of the clearing system, and; (5) has a significant network of branches/ATMs.

It is clear from the above, that the research has not been expanded into the unified European banking market but contained within the UK. European retail banks have been excluded because of the practical issues of gaining access and, more importantly, the loss of control caused by having a number of different regulators involved. This does not, of course, preclude expanding the research into these markets at a later date.

The research examined four UK retail banks and, using well-established case study methodologies, explored the operational risk mitigation process from the perspective of a variety of stakeholders in the organisation. The research was concerned to establish whether one stakeholder may mitigate an operational risk differently from another and focused on modelling the processes involved.

1.2.3 The Research Questions

When managers have to decide on how best to mitigate risks, they will normally have multiple risk mitigation strategies available to them. Horrigan (1967), for example, identified 6 ways of controlling risk situations[8]:

1. Risk avoidance
2. Risk assumption
3. Risk reduction
4. Risk transfer
5. Hedging (or neutralisation)
6. Combination

Managers themselves, will also have their own risk taking behaviour patterns (Hendrickx and Vlek 1990). In addition to these factors, they must also take due cognisance of the nature of the risk being mitigated, the risk appetite of the business in which they work, the time available to effect the mitigation action, and the cost of the potential risk mitigation solutions. This provides an interesting 'cocktail of ingredients' from which a

---

[7] This is a requirement of the Banking Act 1987 Part 1 Section 3 (1)
[8] This paper discusses risk in any organisation and is not focused on financial services

risk mitigation decision must be taken, even if that decision is to do nothing and thus accept the risk.

In an attempt to understand better the processes used (rather than the psychological factors at work) the main research question was:

How do UK retail banks mitigate their operational risk exposures?

A number of secondary questions were developed. They concern the areas of mitigation responsibility, the establishment of mitigation tactics, the communication of risk management decisions, regulatory expectations or risk mitigation models and the barriers to mitigating operational risk.

It was hoped that answers to these questions would give an indication as to how seriously UK retail banks are taking the proposals on operational risk emanating from the leading World Banking Supervisory body, the Basle Committee. It would also establish whether operational risk mitigation can be modelled as a basis for extending the risk management model.

1.3 Research Design

1.3.1 Case study Methodology

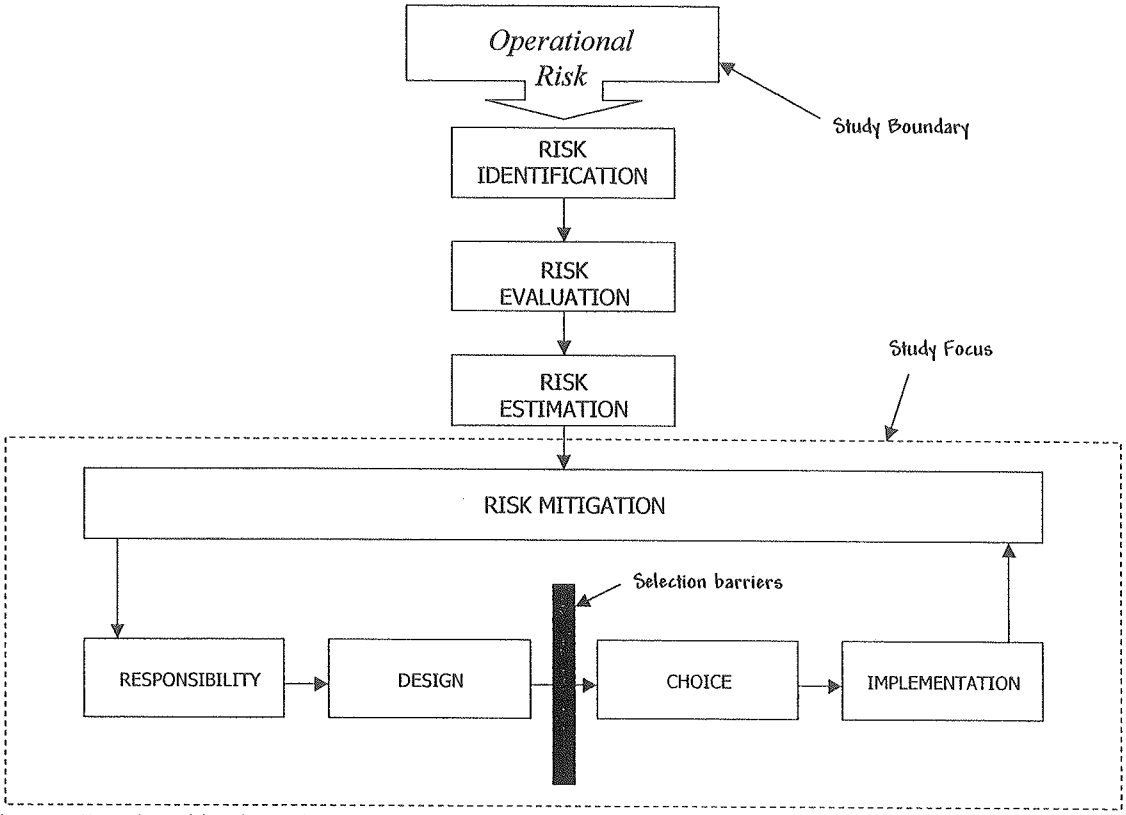
Quantitative survey research is still the favoured methodological paradigm, although other methods have begun to erode the prominence of this methodology (Fontana and

Frey 1998 p. 51). This change of emphasis towards the use of qualitative methods, and the inherent strengths that they bring, is beginning to be more widely accepted and the "metaphysical polemics" (Kirk and Miller 1986 p.15) concerning epistemological techniques are mellowing in their intensity. Case study methodologies are now well-developed and articulated in the literature and are highly appropriate when; the research questions are "how" and "why"; where the focus is on contemporary events; the research is exploratory or descriptive (Yin 1994). The data was collected using multiple exploratory case studies, which are favoured for hypothesis generation (Yin 1994, McCutcheon and Meredith 1993, Bonoma 1985). Multiple case studies also enabled the author to compare management practices and identify 'core practice' in operational risk mitigation.

1.3.2 An Overview of the Research Design

The research methodology used in this study involved developing an *a priori* model of the risk mitigation process, based on the literature review, and exploring adherence to the model. The *a priori* model was an extension of the risk management model in the risk mitigation phase. The extension was based on an appropriate decision making model, derived from the literature (Simon 1977, Nutt 1984), since the act of mitigation involves making a decision about how to lessen the impact or reduce the probability of the risk. The model is shown in Figure 2.

Figure 2 A priori operational risk mitigation model



Source: Developed by the author

Data was collected using primarily open-ended interviews, together with papers and documents concerning the bank and its approach to operational risk management. Data triangulation was employed wherever possible, chiefly through the use of critical incident techniques, where secondary data is normally available.

The literature review carried out prior to the detailed fieldwork identified two main players who assist operational management mitigate operational risk, vis, risk managers and internal auditors. These two groups together with the operational managers themselves were the units of analysis for the study. The research was carried out between February 1999 and December 2000.

1.4 Scope of the Research

The "boundary" (Miles and Huberman 1994 p.25) for this study was operational risk management, whilst the "focus" (Miles and Huberman 1994 p.25) was one phase of operational risk management, namely operational risk mitigation.

The author recognises that there are other risks within banks, for example market risk and credit risk, but they have not been examined in this study, although the critical reader may note that there are occasions when the boundaries between these risk types are not clear cut (for examples see BBA 1999a p.34). The fact that the research questions are aimed at exploring the risk mitigation phase did not preclude an examination of the other phases of risk management. They were included in the study but not discussed in any great detail, except for where there was some link to risk mitigation.

There is one particular area of operational risk that has attracted a significant amount of attention over the last few years, operational risk measurement. This is concerned with the estimation and evaluation phases and is an attempt to quantify operational risk exposures. The author has jointly made a contribution to the debate on quantification (McConnell and Blacker 1999) and discussed it in very broad terms at the interviews to establish whether quantification and mitigation were in any way linked. The generic area of operational risk quantification is, however, outside the scope of this study.

The emphasis on UK retail banks did not preclude the author from examining operational risk management in other banking operations. This was done to broaden the author's knowledge base and literature review as there is little to be found in the current literature

about operational risk management in the context of UK retail banks. Other banking operations are, however, excluded from the study, except where it is appropriate to draw upon certain specific experiences, which the author considers are relevant to the argument being made.

1.5 Positioning of the Researcher

1.5.1 The Researcher's Objectives

From the outset, the author was interested in completing a piece of research that would be of interest and use to practitioners. Thus, the development of a theoretical model of the risk mitigation process was considered an important output. Models that are generated from academic research should have "pragmatic validity" according to Worren et al (1997). By this they mean they should be "useful and user friendly".

Managing operational risks is, or at least should be, of interest to every manager, whether they work in financial services or otherwise. The cost of operational risk management failures in all industry sectors can be measured not only in monetary terms but also sadly in terms of people's lives (see Smallman 2000 for examples). The author was also attempting to raise the profile of operational risk management, and therefore mitigation, as a result of this research project.

1.5.2 The Researcher's Bias

With a first degree in Maths completed in 1974, followed by qualification as a Chartered Accountant in 1977, the author embarked on a career within the audit profession, initially

in external audit and then in 1979 a move to the internal audit function of HFC Bank. This was followed by two further moves within the internal audit functions of financial services organisations, the latter being as Head of the Internal Audit department of TSB Insurance. The author enjoyed working in this environment where the focus of the work was upon improving control procedures and was always very keen on, and actively marketed, the role of Internal Audit. Perhaps the greatest benefit that internal auditors have is the opportunity to review the systems, procedures, risk and controls of all functions within a business. In 1987, the author's goal of moving from Internal Audit was realised and a move to the newly created Business Development Unit of TSB Insurance took place. It was at this point that the author, reflecting on his academic career to date, decided to undertake a part-time MBA. The combination of the academic teachings and the practical experience of managing business development projects within TSB Insurance provided further exposure to the management disciplines required to operate at senior level. The MBA was completed in 1990. One of the projects that the author was involved in was the establishment of a joint venture bancassurance operation (based in Milan) with an Italian savings bank and a major French insurance company. This project came to fruition at the end of 1990 and the author was invited to move to Milan on a secondment basis to help set up the operation. The initial period of assignment was for 3 years but this was subsequently extended to six years. The author was one of the original team of four who established the business. As Head of Planning and Personnel and then subsequently Operations Director, the author had day-to-day responsibility for IT, Personnel, Planning and Budgeting, Management Reporting and Office Services. It was a challenging and rewarding experience to see a new business grow and develop into a

successful operation for all three partners[9]. In 1996 the author returned to the UK and began working in a project management role in the Risk Management/Internal Audit unit of the newly formed Lloyds TSB. As the author entered into this research project in 1997, he was biased in his view of the role of Internal Audit in the management of operational risk and he was keen to establish where the internal audit profession was heading in this area[10]. The project management role in Lloyds TSB was not a permanent position, however, and the author decided in early 1998 to move into freelance consulting, which he continues to do today.

The author recognises the bias in his approach but considers that his broad range of experience outside the audit profession offers the opportunity to take a more balanced, pragmatic and constructive view of both the subject area and the developing profession of risk management.

1.5.3 Choice of Topic

The research topic selected was chosen for three main reasons: (1) it fitted well with the author's academic background, career to date and future aspirations; (2) the literature review revealed that it was an area where little academic research had been carried out; (3) it was an area of growing interest to practitioners, regulators and senior managers in banks. The author knew from the outset that this would be an interesting area to explore because of the interest being taken by Internal Audit in risk management (McNamee and

[9] The author has written and published at Cranfield a case study based on his experiences of this international, joint venture, start up operation

[10] The author had continued to maintain links with the Institute of Internal Auditors and was awarded a Fellowship of the Institute in 1999 for his contribution to the profession

Selim 1998) and the fact that some Internal Auditors had combined their internal audit activities with operational risk management (Cunnington 1999). Operational risk was beginning to appear in the everyday vocabulary of internal auditors, risk managers and operations managers. The selection of this as an area of research was intuitively appealing and challenging to the author.

1.6 Contribution to Knowledge

Operational risk is an area that is under researched and is of growing importance to financial institutions because of regulatory requirements. The study examines an uncharted area with a practical orientation towards managing operational risk on a day-to-day basis. Whilst the focus of the study has been in the UK, it has international implications because the Basle committee is an international organisation responsible for bank regulation.

There is mounting pressure from Basle, both on the regulators of UK banks and senior management within the banks, to mitigate operational risk exposures effectively. Basle are also mandating banks to 'bolster market discipline through enhanced disclosure' (see Basle 2001). This will require, inter alia, disclosure of the bank's risk assessment methods, an area which the study has examined in some detail in relation to operational risk. The development of a theoretical framework for operational risk mitigation actions will provide an important contribution to how UK retail banks are tackling this problem and help identify what is current 'core practice'. The development of a practical checklist

or 'road map' of how to approach operational risk mitigation will provide an important contribution to those 'managers'[11] who are seeking to improve their understanding of the process. Finally, the development of a high-level review document for auditing the emerging operational risk functions will help to provide comfort that such functions are doing their job effectively.

As recognised by Basle (2001), studying how banks mitigate operational risk will be an important contribution to helping banks reduce the exposure, frequency or severity of an operational risk incident. Reducing fraud, errors and inefficient operations through effective operational risk mitigation will have a positive effect on an organisation's cash flows and help to improve a 'risk awareness culture' in the business, which should ultimately lead to an increase in shareholder value[12]. Additionally, this study will provide a contribution to the understanding of management in major financial institutions, particularly from a Board perspective, where the pressure to demonstrate effective corporate governance continues unabated. This is particularly so in the UK environment with the recent emphasis being placed on risk management by Turnbull (ICAEW 1999).

Given the lack of research in the area of operational risk, it is hoped that the study will contribute to the construction of a cumulative knowledgebase vis-à-vis operational risk management, operational risk mitigation and the processes and tactics used to mitigate

[11] Managers means principally operational management but equally applies to risk managers and internal auditors

[12] Shareholder Value Analysis is a valuation approach which considers in broad terms that the value of a business to a shareholder can be determined by discounting its future cash flows using an appropriate cost of capital (Mills 1998)

operational risk. The research is very much at the exploratory stage of theory development. Methodologically, the study contributes to the growing repository of case study research programs in another area of business, risk management.

1.7 Structure of the Thesis

The thesis has been structured in the following way:

- Chapter 2 provides a comprehensive review of the related literature and discusses why operational risk is important and why the particular *a priori* model was chosen;
- Chapter 3 argues for the methodological position adopted and provides the research design;
- Chapter 4 focuses on the cases studied and describes how case study methods have been applied to the study;
- Chapter 5 provides the study findings emerging from the detailed data analysis work and provides alternative explanations;
- Chapter 6 discusses the implications for management, focusing particularly on operational risk management;
- Chapter 7 summaries the research and identifies the limitations and suggested areas for further research.

2. LITERATURE REVIEW

This section covers the literature review and aims to build a theoretical foundation upon which the research is based. 'Relevant literature' is reviewed and issues related to the topic being studied are identified. The section begins with introductory comments concerning the areas of knowledge being reviewed. Each area is then examined in more detail.

2.1 Introduction

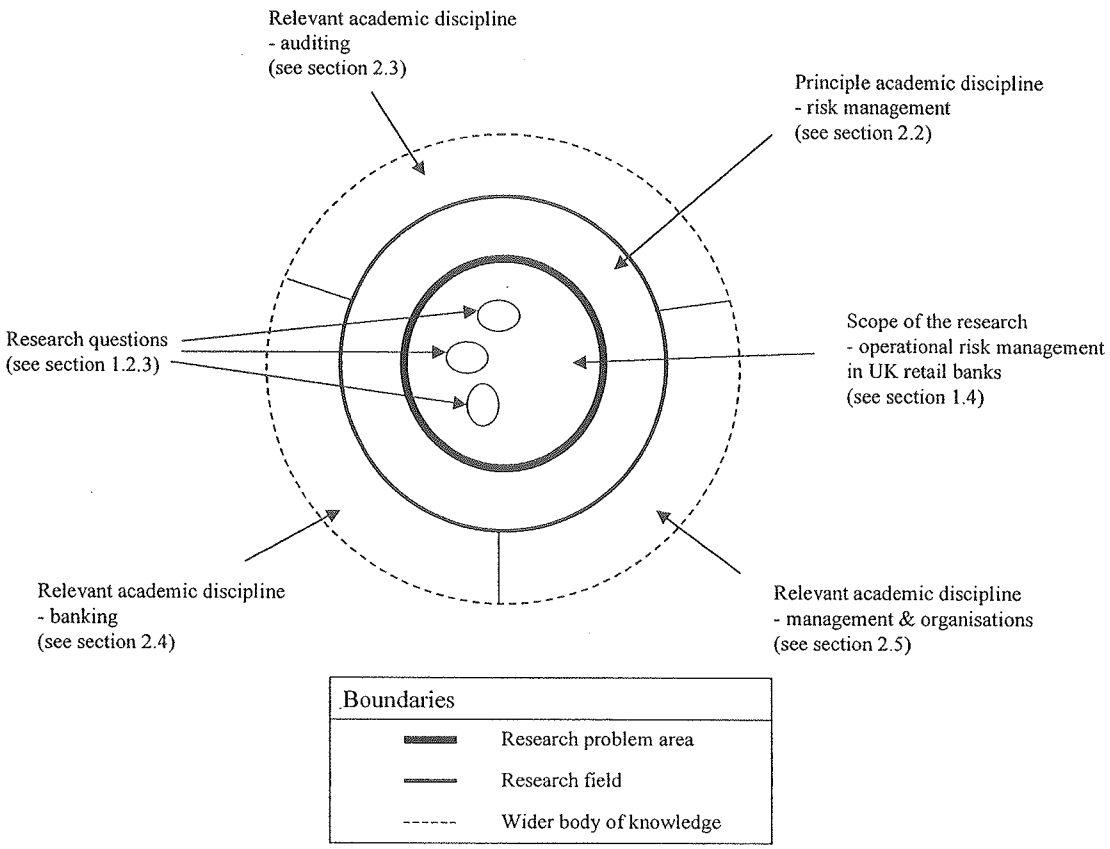
2.1.1 Disciplines covered by the Literature Review

The research is based on four academic disciplines:

1. Risk Management – the immediate discipline where the literature review has been focused and, in particular, the regulatory environment has been examined;
2. Auditing – the role of internal auditing in the internal control framework where operational risk is managed;
3. Banking – the current issues facing UK retail banks and how they may impact upon the management of operational risk;
4. Management and Organisations – the decision-making environment and the organisational arrangements for operational risk mitigation.

Figure 3 illustrates diagrammatically how the research questions link to the wider body of knowledge. The outer layer represent the wider body of knowledge and this and the other layers may be 'peeled back' to arrive at the 'core' of the research problem, i.e. the research questions.

Figure 3 The boundaries and academic disciplines of the study



Source: Developed by the author

2.1.2 Focus on the Management of Risk

Since the core discipline underpinning this research is risk management, a few introductory words that reflect on its history and identify its theoretical positioning, are considered appropriate to place the research into context.

Bernstein (1996) discusses how a 'mere 350 years' separate today's risk assessment and hedging techniques from decisions guided by superstition, blind faith and instinct. The notion of risk management by instinct can be seen throughout the history of civilisation.

For example, early man feared attack from animals so mitigated this risk by living in a cave; the Romans feared insurgence so mitigated this risk by maintaining a big well-trained army; and the merchant navy feared their ships would sink because of overloading so mitigated this risk by introducing the plimsoll line. Risk management is, therefore, nothing new and more recent times have seen increasing sophistication in the development of risk management techniques.

Lavington (1925) developed an approach to the theory of business risks based on the economic viewpoint of "satisfying material wants" and the inherent problems, or business risks, in attempting to achieve this. His theory was built on two conditions which affected production within an organisation: the *intractability* of the natural resources at the organisation's disposal; the *incalculability* of the results of the operations by which these resources are adapted by the organisation to produce goods and services for society. He concluded that business risks consist in the probability of occurrence of all losses, and only those losses, which arise from incalculability. He, therefore, placed the emphasis of risk management within the operations of the organisation where the goods and services are produced.

More recently McConnell (1996) in his review of the Market Risk Management function of International Banks noted how the (risk management) function performs a similar role to the 'traditional control functions in the 'technostructure[13]' part of the firms

[13] The functions in the 'technostructure' operate at all levels of the organisation by analysing activities of workers in the operational core, planning and carrying out studies of managerial tasks and planning and developing control systems for senior management (Mintzberg 1979)

organisation' and that one of their primary roles is that of 'problem identification and formulation'.

Risk management is also concerned with influences outside the firm, in particular, the environmental conditions within which the firm must operate. Hatch (1997) noted how rapidly changing environments require organisational flexibility giving rise to the term *organic organisations*, because like other living things, they adapt flexibly to changing circumstances. At the opposite end of the spectrum are *mechanistic organisations* which Hatch (1997) points out exist in stable environments where the need is for specialisation of the tasks and jobs undertaken, thus creating a high-performance and disciplined (or mechanistic) system.

The decision as to when to use either the mechanistic or organic form of organisation is an example of contingency theory, i.e. the most effective way to organise is contingent upon two conditions, namely, the complexity of and change in the environment. Risk theory and the framework within which risk management takes place is rooted in contingency theory since the process of risk identification (the first phase in the risk management process) takes place within a two dimensional framework within the business environment in which the firm operates: the likelihood of the risk against its possible impact. Risk mitigation, the phase that follows, must take due cognisance of the probability and impact as part of the 'information' from which a decision will have to be made.

2.1.3 Sources of Literature

In order to provide a broad ranging view of the disciplines, literature has been selected from both academic and practitioner sources. The emphasis has been on academic material but the reader should note that both the areas of internal auditing and operational risk management have a large number of practitioner's references. This reflects the lack of academic emphasis that has been placed in these areas as described by Boyle (1993) for internal auditing and Tschoegl (2000 p 103) for operational risk management.

2.1.4 The Role of Theory

The development of theory is valuable for researchers because it can serve as a basis for accumulating and refining knowledge in the domain of interest (Eiermann et 1995). Since one of the objectives of this research is to present a theoretical vision of operational risk mitigation, a few words on what a theory is, are presented in this section.

Bacharach (1989) describes the purpose of a theory as "to organise (parsimoniously) and to communicate (clearly)". Epistemologically, a theory enables the components of a complex phenomenon to be brought together in one understandable whole (Weber 1998). The terms grand theory, middle range theory and substantive theory (Weber 1998) are used to describe the scale of what is being proposed, although exactly what constitutes a good theory has been the subject of debate (see Sutton and Shaw 1995, Weick 1995 and Di Maggio 1995). According to Sutton and Shaw (1995) this has arisen because of a "lack of direction and a disorganisation of the body of knowledge" in the area of theory development.

Weick (1995) describes the process of theory building as being iterative where one is continually 'speculating and abstracting' through the process using the data that has been collected. The resulting theory should be a coherent narrative composed of assumptions, abstract reasoning, and speculation which describes and explains an observed or experienced phenomenon's constructs (terms which may be applied or even defined on the basis of the observables), their interrelationships, and their boundaries (Weber 1998). The operational risk mitigation theory developed in this study is based on this definition. The theoretical framework proposed is then used to develop a model of the process.

2.2 Banking

2.2.1 Industry Structure in UK Retail Banking

A recent report by PriceWaterhouseCoopers and the Economist Intelligence Unit (PriceWaterhouseCoopers 1999) identified four 'forces' that are driving retail banks[14] to change the way they operate:

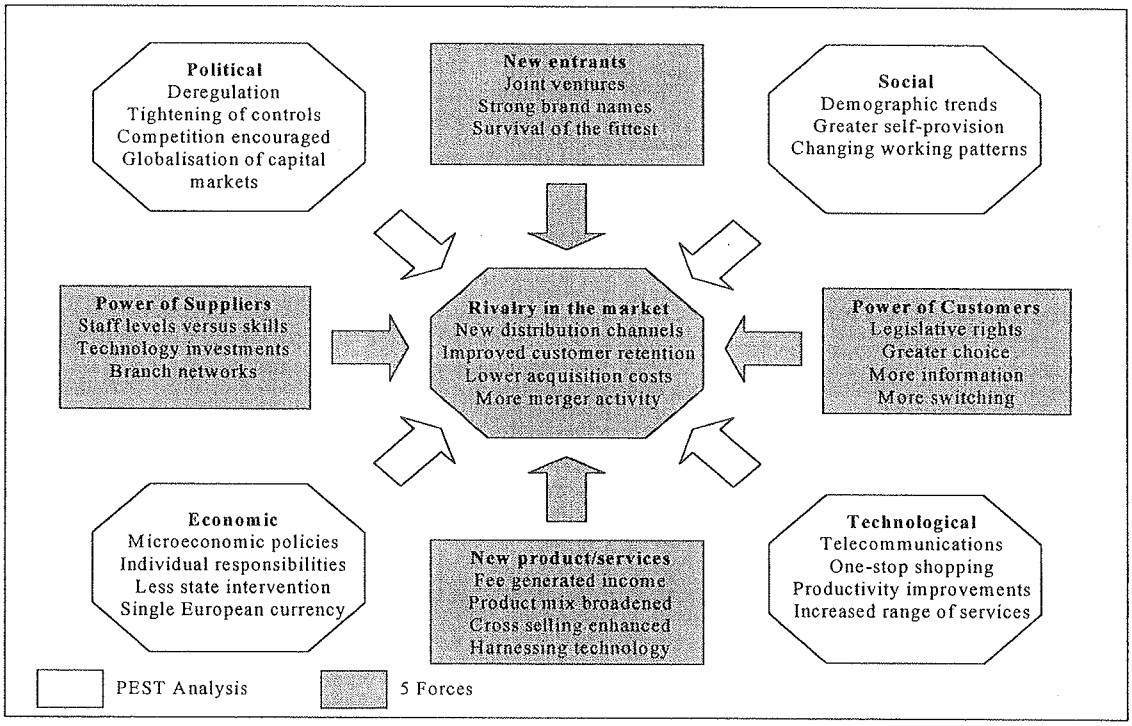
1. Consumer demands – consumers are demanding fast, convenient, 'glitch-free' service from branches and non-premise distribution channels;
2. Technology developments – many large consumer banks are building sophisticated information management capabilities that will help them enhance their customer management capabilities;
3. Competition – new customer acquisition strategies are intensifying whilst revenue generation is growing more complex, more difficult and more costly;

[14] This study was undertaken in North America, the UK, continental Europe and the Asia-Pacific region

4. E-commerce – 'Internet banking' and, in particular, the timing of when to enter the market is set to dominate the way 'business to customer' transactions are undertaken.

Underlying these forces, Nellis (1998) looks at the drivers behind change in the UK financial services industry at the macro level, i.e. developments in the wider business environment commonly known as a PEST (political, economic, social and technological) analysis, and the micro level, i.e. based on the five forces model of Porter (1985). His analysis is represented diagrammatically in Figure 4.

Figure 4 Forces driving change in financial services



Source: Adapted from Nellis (1998)

There are many examples to support the development of these forces and a number of writers have elucidated some of the themes in the diagram. For example, Hickson and Turner (1996) looking at the most efficient method for regulating banks (political analysis) argue for even greater regulation because 'bank regulation, especially capital requirements, induces bank stability' whilst other methods of regulation, such as deposit insurance, 'induces instability'. They present evidence to support the view that the deregulation process over the last 20 years has led to a more unstable banking system. Lowe and Kuusisto (1999) suggest that banks in facing these structural changes should not lose sight of one of their most valuable intangible assets, namely, their institutional stature. Their study is based on a comparison of Finnish and UK retail banks and they argue that whilst customers are not very happy with the services that banks deliver, they still trust their banks as a safe and secure place to keep their money. Kaminsky (1989) discusses the concept of 'Integrated Consumer Banking' as the way to counter the threat from other organisations that have been so successful in taking away customers. Fundamental to the development of the concept is a recognition that value comes from developing long-term customer relationships rather than just selling more products. Heffernan (1996) notes how competitive pressures are forcing banks to reduce their operating costs, particularly in the area of branch operations because branches are expensive to maintain and can contain a large number of non-revenue generating personnel.

This is not to say that UK retail banks have been standing still whilst these threats have been around. The success of bancassurance during the last 15 years (see Brown 1992 for a

history of the TSB experience with bancassurance) bears witness to banks fighting back and a quick perusal of the Report and Accounts of any of the main UK retail banking operations will highlight the increasing importance that life insurance profits have on the bottom line.

The number of players in the UK retail banking market has changed over the last few years as a result of Building Societies de-mutualising (e.g. Abbey National, Northern Rock, Woolwich, Halifax and Bradford and Bingley) and mergers/takeovers (e.g. Lloyds merger with TSB in 1996 and more recently in 1999 the Royal Bank of Scotland takeover of National Westminster bank). In addition, the European banking industry is seeing changes resulting from the Single Market Programme which has set in motion a 'rationalisation process' which will have a dampening affect on their traditional business margins (Nellis et al 2000). How well prepared UK retail banks are to face these challenges is still unclear. Evidence from Nellis et al (2000) suggests that change will be most pronounced in countries where there is:

1. A relatively large number of small-sized banks, indicating that there are prospects for exploiting economies of scale;
2. A low level of domestic concentration, suggesting that there are important market power connotations associated with increasing market share;
3. An increasing role for institutional investors as the key facilitators of bank disintermediation and asset securitisation.

As a result of the above analysis, they go on to point out that the most likely strategic response will be based on European 'regionalisation' of banks rather than a development

of 'pan-Europeanisation'. If this analysis is to be believed then the strategic implications for UK retail banks are that they should concentrate on their home markets.

2.2.2 Competition

The previous section illustrated the structural changes that are occurring in the banking industry. Many of these changes will affect the competitive climate in which banks will have to operate. In the UK, competitors to the retail banks come from many sources, building societies, insurance companies, supermarkets, high street stores to name but four. Diversification has occurred on a vast scale in the last 15 to 20 years and nowhere has competition been more intense than between banks and building societies (McGoldrick and Greenland 1992). The traditional boundaries of operation between the two have become blurred to the point that the average consumer may well wonder what the difference is between a bank and a building society. Embracing the concepts of retail marketing, and with it a better understanding of customer needs, is seen as a critical success factor by McGoldrick and Greenland (1992) in their empirical study of the attributes and dimensions upon which building society and bank customers tend to base their choices. They go on to discuss this in the framework of the marketing mix utilised by financial services retailers: product range, pricing, promotion, personal selling, service, environment and location, concluding that a careful repositioning is 'required' if banks and building societies are to avoid a 'lemming-like rush' towards being all things to all people.

Strategic positioning is a theme picked up by Zineldin (1996) in his review of Swedish commercial[15] banks. He identified a number of barriers that banks can construct in order to protect themselves against competitive actions:

- Creating customer satisfaction by delivering product/services for the benefit of both personal and corporate customers;
- Using proprietary technology in an equipment-based product/service (e.g. home or private banking);
- Recruiting, developing and retaining the most talented staff in order to be able to deal with and treat customers with trust, respect and the highest ethical standards;
- Using superior technology and products/services as the means for building broader and deeper relationships and recognising the importance of continuity of customers.

Positioning is an attempt to 'distinguish the bank from its competitors' in order to be the most preferred for a certain market segment. Differentiation in this way is a point developed by Lowe and Kuusisto (1999) who urge banks to focus their marketing strategies on exploiting on of their most 'neglected assets', vis, the institutional stature or their privileged trustworthy position with customers. Retail banks in the UK are, however, coming increasingly under fire from the Press (see Sunday Times 2001a, 2001b, 2001c, 2001d for examples) and the Government, on their privileged position status. The Cruickshank (1999) report commissioned by the Chancellor of the Exchequer was highly critical of certain areas of retail banking competition. For example, the following

[15] Commercial is not defined but such banks compete with savings banks in all types of bank's operations and activities

comments were made with respect to the supply of banking services to personal customers:

- The supply of current accounts is highly concentrated and holds the key to competition to suppliers in many other product areas;
- Consumers perceive significant barriers to switching current accounts;
- Few consumers are aware of the terms and conditions of the products they hold, pointing to significant information problems;
- Consumers have inadequate representation and redress.

These comments along with the general thrust of the report towards increased regulation will only serve to further the competitive climate in which retail banks will operate.

One particular source of competition is coming from the development of Internet banking operations. This new distribution channel is forcing the 'old economy' retail banks to re-assess their strategies as a defensive measure against new entrants, which in the case of Egg[16], has made a 'significant entry' (Jayawardhena and Foley 2000). The growth in Internet banking could also provide opportunities to improve customer management. PriceWaterhouseCoopers (1999) consider how 'click-tracking' promises to help a bank 'monitor, analyse and respond to the customer's online activity almost as soon as it occurs'.

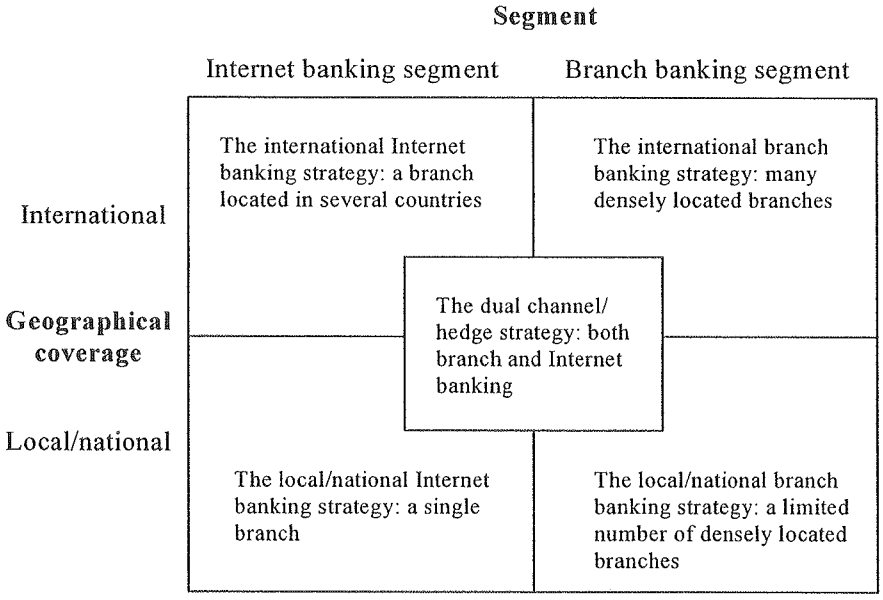
So who will be the winners and losers in this competitive environment? Nellis (1998) identifies a number of winning characteristics including a willingness to experiment, a

recognition that customer data should drive strategic planning and a management able to cope with uncertainty and new challenges. The losers, on the other hand, will be those organisations that are unable to 'escape from the past' and which continue to 'play by the old rules'.

2.2.3 Distribution and Service

Mols (1998) discusses the possible distribution strategies available to banks with the growth in Internet banking capabilities. These are split by geographical coverage and banking segment as shown in Figure 5.

Figure 5 Distribution Channel Strategies



Source: Mols (1998)

Mols (1998) argues that this segmentation will force retail banks to decide which segments to target and which geographical area to aim at. A problem which is being addressed by other industries where the Internet is developing as a distribution channel.

[16] Egg is the brand name for the banking services offered by the UK life insurer Prudential

Delivering products and services via the Internet does not imply that there will be a complete demise in other distribution mechanisms. The delivery system in a bank is seen as a mix of 'human resources, locations and equipment'[17] (Zineldin 1996). Equipment, in particular, has enabled retail banks to offer their customers quick and efficient service twenty-four hours a day. Devlin (1995) argues that the opportunities offered by technological advancements mean that the 'cashless society' will not be long in arriving, if the customer wants it. The growing use of call centres is discussed by Betts et al (2000) who find that whilst they can offer customers improved service, it is difficult to do this consistently because of the difficulties of resourcing short-term peaks in demand.

Location refers to the branch network offered by the retail banks. Greenland (1995) discusses the demise of the bank branch channel but notes how the role of the branch has been re-orientated to more of a 'retail and selling role' and as a consequence, the 'spatial arrangements' of branches has been a focus of activity together with the hierarchical organisational arrangements. He sees the distribution/network hierarchy being based on seven levels as depicted in Table 1.

[17] Equipment includes Automated Teller Machines, Point of Sale Terminals and telephone banking

Table 1 Distribution/network hierarchy in Financial Services

Level	Type	Facilities provided
1	Remote ATM/ deposit box	ATMs/deposit boxes detached from the branch but usually serviced by a local parent or community branch
2	Nominal or automated branch	Predominantly 'remote' self-service outlet/kiosk projecting the corporate image: ATMs, advanced touch screen banking machines, telephone links with community branches and maybe one or two sales assistants
3	Sub-branch	Small retail unit: ATMs, cash counter, maybe an interview facility, limited service offering and perhaps limited opening hours. They frequently have no managerial presence but are visited by a 'nomadic' sales advisor from a parent/community branch
4	Parent branch Corporate branch	Retail/personal branch, typical town/suburban outlet, a more complete range of personal banking services in a retail oriented design Outlet offering facilities for corporate/business customers only, i.e. no tills/retail area. They frequently comprise management suites with parking areas operating from business park developments that have lower rents
5	Community branch	Financial supermarket: banking hall is broken into specific product areas, full service range including personal as well as business corporate services, tele-enquiry/tele-service/telesales support facility for lower level branches and frequently processing and administration assistance too. They tend to be large expensive city centre branches
6	Regional HQ	Administration/control centres fro the regional network
7	National HQ	Administrative and management centres determining and implementing a national network policy via the regional headquarters

Source: Greenland 1995

This provides an interesting analysis of how distribution may be linked to service/product offerings and offers the opportunity to review customer segments against these levels to determine appropriate strategies for direct targeting of customers.

Underpinning both location and equipment are human resources as part of the delivery system. The last few years in UK retail banking has been characterised by mergers with one of the principal driving factors being the need to reduce costs. In a service organisation such as a bank, reducing costs tends to be focused on reducing headcount

and staff numbers have seen a significant reduction over the last few years (Greenland 1995).

As has been previously noted, the services offered by banks have broadened with the development of Allfinanz or bancassurance operations (Brown 1992). Internet banking provides a whole range of services (see Jayawardhena and Foley 2000 for examples) for customers and removes the face-to-face contact that has always been the hallmark of retail banking. Take up of Internet banking has, however, been slow (Jayawardhena and Foley 2000) suggesting that customers will continue to use the traditional branch channel for a little while yet. Research in this area (McGoldrick and Greenland 1992, Zineldin 1996) suggests that customers still see banks as 'trustworthy' organisations particularly where they provide a 'reliable, reassuring and responsive' service (Zineldin 1996).

2.2.4 The Regulatory Environment

The history of banking regulation in the UK can be traced back to 1857 when it became possible for 'banking co-partnerships to shed their cumbersome constitutions and acquire the benefits of incorporation as either limited or unlimited companies' (Crick and Wadsworth 1958, p 31). Following the introduction of limited liability, the banking system became more prone to instability through bank runs, and government monitoring was thus introduced (Hickson and Turner 1996). The degree of government monitoring became crucial to improving the stability of the banking sector and continuing bank failures in the 1920s and 1930s are generally accepted as the cause for further extensive bank regulations being introduced across many countries (Hickson and Turner 1996). By

this time, minimum capital ratios were being adopted in the US (Comptroller of the Currency 1997) and this momentum continued around the globe with a hotchpotch of different regulatory requirements being used. Despite this, banks continued to have problems and it was not until the early 1980s, as concern about international[18] bank's financial health mounted and complaints of unfair competition increased, that the Basle Committee on Banking Supervision started considering proposals to set capital standards for these banks (Santos 2000). In 1988, when the Basle Accord came into being, it was seen as a breakthrough in regulation. For the first time, regulators from a number of countries had set a truly global standard for capital adequacy in relation to banking operations.

The initial Accord explicitly covered only credit risk. It required international banks from the G10 countries to hold minimum total capital equal to 8% of risk-adjusted[19] assets, with at least half of this met by Tier 1 capital (equity capital and disclosed reserves). Tier 2 capital (other hybrid debt/capital instruments) could also be used in the calculation. In 1996 an amendment to the accord introduced a Tier 3 capital to cover market risk exposures, and as noted by Santos (2000), the main novelty of the amendment was that it 'allowed banks to use their own internal models to determine the required capital charge for market risk'. The Value-at-risk (see section 2.4.4.5) concept had now entered into the regulatory regime.

---

[18] International means banks operating in the three major time zones – Europe: centred on London, North America: centred on New York and Asia: centred on Tokyo (McConnell 1996)

[19] The calculation for risk adjusting assets involves taking both on and off balance sheet items and assigning them to risk category which would weight them (by factors of 0%, 20%, 50% and 100%) according to the perceived riskiness of the asset

The reader will note the focus on risk that the Basle accord introduced was geared towards credit risk and market risk. Operational risk was not specifically mentioned but interest in this area probably grew as a result of the banking collapses, which derived from operational risk failures (e.g. Barings). Additionally, the Basle Accord had one serious drawback in that it adopted a 'one size fits all' approach (Santos 2000). To address these issues, the Basle Committee have recently published a new capital accord (Basle 2001), which is meant to take into account the shortcomings of the previous one. This new accord is designed to be more flexible and risk sensitive as highlighted in Table 2.

Table 2 Comparison of Basle 1988 Accord and Proposed New Accord

1988 Accord	Proposed New Accord
Focus on a single measure	More emphasis on banks own internal methodologies, supervisory review, and market discipline
One size fits all	Flexibility, menu of approaches, incentives for better risk management
Broad brush structure	More risk sensitivity

Source: Basle (2001)

The structure of the new accord is based on three 'mutually reinforcing pillars'. Together these are seen as contributing to 'safety and soundness in the financial system'. The pillars cover:

- Pillar 1: minimum capital requirement – this is still set at 8% of risk-weighted assets, but a revised credit risk measurement is proposed, a measure for operational risk is included whilst market risk remains unchanged.

- Pillar 2: supervisory review process – requires supervisors to ensure that each bank has sound internal processes in place to assess the adequacy of its capital based on a thorough evaluation of its risks.
- Pillar 3: market discipline – aims to bolster market discipline through enhanced disclosure by banks including the way a bank calculates its capital adequacy and its risk assessment methods.

The scene has, therefore, been set for banks to move their risk management and measurement techniques into the 21st century and for the first time operational risk will feature directly in the assessment of capital adequacy together with the review undertaken by the supervisors. In the US the Comptroller of the Currency (1997) has pointed out that whilst measuring capital is one thing, it is important not to lose sight of the 'function of capital' itself. Capital is 'only one, albeit important, indicator of an institution's overall health, as well as being only one, albeit important, tool in the overall supervisory arsenal'. Supervisors are likely to be playing a more active role in future in monitoring a bank's capital adequacy and risk management arrangements.

As if this regulatory pressure was not enough, in the UK environment, the Cruickshank (1999) report is providing retail banks with further problems to manage. The report was commissioned by the Government and looked at competition in the UK retail banking market. Three main areas were examined: money transmission; services to personal customers; services to small and medium sized businesses. In each of these areas the review was keen to establish if competition was effective. In all three areas the response

was 'No', principally because the current market structure (with the 'big four' controlling most of the market) creates artificially high barriers to entry and thus stifles competition. Cruickshank (1999) goes on to propose a new policy framework consisting of four main elements:

1. Increasing transparency in banking supervision – recommendations on disclosure of information including support for the Basle (2001) proposals on publishing more information about risk exposures and risk strategies;
2. Getting institutional incentives right – recommendations on how the three main bodies in banking regulation and supervision should organise themselves to work better together and provide a more effective regulatory framework;
3. Delivering effective competition scrutiny – recommendations on how banks and other financial institutions should be exposed to the full rigours of the competition laws;
4. Eliminating regulatory distortions – recommendations to shift some self-regulatory initiatives to the Government.

The regulation and competitive pressures on UK retail banks are, therefore, set to increase on a number of fronts. This provides further impetus and support for this research project with its emphasis on understanding how UK retail banks are mitigating the operational risks that confront them.

2.2.5 Information Technology

The rapid change in technology in wholesale and retail banking will have a major impact on the competitive structure of banking systems, especially retail banking (Heffernan

1996 p 328). Retail banks use information technology extensively in carrying out their day-to-day operations, most notable in the areas of electronic cash dispenser networks and more recently in the areas of home and telephone banking systems (Devlin 1995). The development of the Internet and with it e-commerce has removed one of the main barriers to entry in retail banking, i.e. the cost of setting up a branch network (Nellis et al 2000). Internet only banks, such as 'Smile' attest to the use to which information technology may be put in developing a banking operation.

Information technology is also becoming important in the generic area of risk management for banking operations. McConnell (1996), in his review of information technology for market risk management, highlighted how 'some banks, especially in the US, have risk management support systems already in place whereas others (in Europe) have barely started the development process'. In the context of information technology developments in the area of operational risk, the author was unable to find any research that had studied this area. A number of UK based companies[20] are known to have developed software to support operational risk management and an examination of the practitioner's literature (e.g. Risk Professional) regularly carries advertisements for such products.

2.2.6 Other Issues for Retail Bank Management

Over the last few years, a number of research projects in the UK banking sector have examined the effectiveness of different management processes. Specific examples include:

- Asif and Sargeant (2000) developed a model of internal communications based on two UK clearing banks and found that the process may be represented as an ongoing activity where a variety of different variables will determine the outcome of any communication effort undertaken;
- Caruana and Calleya (1998) examined the internal marketing processes in a retail bank and how they influenced commitment amongst branch managers. The research confirmed that a significant relationship existed between the two and that this in turn had an important effect on the success of relationship building with customers;
- Reid et al (1998) looked at the value of information in the decision making process and specifically at the role of a corporate library in that process. Managers from six UK retail banks were selected and the results found that, irrespective of its source, information is a valuable commodity and does add considerable value to the decision making process.
- Wilson (1997) looked at the norms, values and behaviours that make up the corporate culture of the branch team in a major UK bank and assessed how this impacted upon service delivery and corporate identity. The results found that there was no obvious link between culture and service and that the management of corporate behaviour was far more difficult and complex than the management of the visual identity element of corporate identity.

These studies indicate the importance of communications, internal marketing, information used in decision making and branch culture in the UK banking sector. They

[20] Two such companies are known personally to the author

highlight the complexity of issues that bank management face and two of the themes, communications (Asif and Sergeant 2000) and information used in decision-making (Reid et al 1998) have been identified as important areas in the management of risk (see Royal Society 1992 and Blacker 2000). The future success of retail banks would appear to rest on a number of factors with no single strategic model being appropriate. The strategic choices that banks make, will drive their future positioning in the market and ultimately their ability to create and maximise shareholder value.

2.2.7 Risk Management in the Current Environment

According to Cade (1997 p.211) responsibility for risk management in a bank lies ultimately with the Board and management. He goes on to point out how the board's objectives must govern the way risk management is organised in the bank and suggests a list of 'attributes and disciplines' (Cade 1997 p.216) which can help in the organisation of risk management. These include:

- A commonly accepted definition of 'risk' and risk types leading to a practical risk map for the bank;
- Clear risk management responsibilities (downwards) and accountabilities (upwards), to avoid confusion, duplication of effort, and things falling between the stools;
- Transparency, a comprehensive management information, monitoring and reporting system, in which material exposures, gains and losses are fully disclosed, analysed and communicated to those who need to know, and stored for future reference;

- Professional, specialised staff, expertise in developing, hedging and controlling the different types of risk encountered in a banking business.

In order to co-ordinate all these activities Cade (1997 p 219) sees the creation of a top level risk management committee which oversees all the risk management activities and acts as the main conduit to the Board. The term 'risk management' in a bank, however, covers a multitude of risks, some of which are more amorphous than others (Santamero 1997). In America, the Office of the Comptroller of the Currency identifies and defines nine categories of risk for banking supervision purposes (Comptroller of the Currency 1998c): credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic and reputation which it uses to profile a bank's exposures. These nine categories are used in assessing a banks exposure in other areas, for example, technology risks are found to contain exposures in transaction, strategic, reputation and compliance (Comptroller of the Currency 1998a and 1998b).

Basle (2001) proposes that only market, credit and operational risks will be used for regulatory purposes and specifically excludes strategic and reputational (although it fails to define what they are). A further regulatory view (Quick 2000) avoids the words operational risks directly and uses the term 'other risks' to mean 'business risks, including operational risks, which are unrelated to financial markets or credit'. Pyle (1997) suggests that four categories are sufficient: market, credit, operational and performance whilst Cade (1997 p19) analyses risks in six different categories: solvency, liquidity, credit, interest rate, price and operating.

Taking the specific example of another risk type, vis, environmental risk, Santamero (1997) identifies this as a separate category, which requires 'substantial time and resources' devoted to its management. A view supported by Thompson (1998) who devotes a whole paper to defining environmental risk in the context of bank lending and then goes on to assess the relative environmental exposures of the UK's major clearing banks concluding that banks vary in their exposure and suggesting that further work needs to be done 'to establish suitable ways of measuring such risks'.

One way of improving the management of risks would be to learn from previous bank failures to ensure that they cannot be repeated. Heffernan (1996 p 292) analyses failures over the last 20 years and identifies a number of 'common lessons' that should be learnt by bank management. These include (1) weak asset management, as reflected in the loan book, is a common reason why banks get into difficulty, (2) inexperience with new products, (3) general management deficiency was a 'contributory factor' aggravated by inappropriate promotion criteria, (4) fraud and dishonesty. A final, interesting hypothesis raised by Heffernan (1996 p 296) is the notable clustering of cases of failure (in a country) around a few years rather than an even spread over time. The presence of clusters, she argues, may suggest that the state of the macro economy is a contributory factor in bank failures.

It may be concluded that risk management in the current banking environment is a complicated area with no clear consensus emerging about the best way to analyse the risks faced by a bank. As a first step, banks need to be clear about the risk categorisation

that they use. A clear definition of these risk categories will help to ensure that they cover all the risks of running their business and ultimately satisfy both the regulators and the other stakeholders who have an interest in seeing an effective risk management system in place.

2.2.8 Implications for Operational Risk Management

There are a number of implications for operational risk management emerging from this brief review of the issues facing UK retail banks. The industry structure is changing and with change comes risk. Regulation, in particular, is a key driver behind changes at the macro level and retail banks will have to ensure that they are ready to face the challenges being imposed by the new regulatory regime, with its increased emphasis on the management of operational risk. The drivers of a changing operational risk environment are also coming from competition and new technologies. New entrants into the market, particularly supermarkets and high street shops already have their customer bases through which they can offer products. Retail banks will have to respond to these threats by taking more risks to secure their business and avoid customers leaving them in droves. An example of this would be increasing deposit account interest rates in order to compete, but this increase is likely to have a direct impact on profitability if it fails to retain and attract customers. New technology, particularly Internet technology, brings new risks and retail banks will need to ensure that their developments in this area are managed with the potential risks in mind. There is evidence to suggest that fraud and security risks have not been adequately managed in some of the online banks (The Independent, 2/8/2000).

Branches are being closed and operations transferred to more centralised units. This transfer of operational risk needs to be managed effectively, particularly bearing in mind the customer and the reputational risks faced when a small branch closes. Customers are becoming more demanding and the marketing mix is changing with a much broader range of products being offered and supported by the bank. All of these have implications for operational risk as the banks react and change the way they do business. One specific example, which has been previously cited, is the movement of retail banks into the insurance market. This has brought increased operational risk with new processes and internal control frameworks being either developed or acquired, but more importantly, it may increase the tension between the 'bankers' and the 'insurers' and their understanding of each other's business[21].

2.2.8 Summary

This section has provided an overview of the current challenges being faced by UK retail banks and illustrated how many of these challenges will impact upon their operational risk profile. A review of the macro level industry structure was followed by an examination of several key areas, with a specific focus on the regulatory regime, which is one of the main drivers for this study. A discussion on risk management in the current banking environment confirmed a number of complexities and issues that will need to be managed. The section concluded with a review of the implications for operational risk management.

---

[21] There is a salutary lesson to be learned from Barings here. One of the causes of failure was the fact that senior management did not understand the trading operation they acquired in 1984 with the purchase of stockbrokers Henderson Crothwaite. There was a 'constant clash of cultures' and Peter Baring is reputed to have said, "It's not terribly difficult to make money in the securities business" (McConnell 1998)

2.3 Auditing

2.3.1 Internal Auditing

Internal Auditing is defined as:

"An independent and objective assurance and consulting activity that is guided by a philosophy of adding value to improve the operations of the organisation. It assists an organisation in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organisation's risk management, control and governance processes" (IIA 1999a)

Crucial to the success of an Internal Audit department is the independence of the function from operational management, which is usually achieved through the reporting line. This enables it to provide the 'objective assurance' alluded to in the definition. The definition also identifies the focus of Internal Audit activities as being in the areas of risk management, control and governance, with control being seen as the essential function of internal audit (Spraakman 1997). The resulting scope of activities is guided by five 'control objectives' for the internal audit function (IIA 1998b):

1. Reviewing the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information;
2. Reviewing the systems established to ensure compliance with those policies, plans, procedures, laws, regulations and contracts which could have a significant impact on operations and reports, and should determine whether the organisation is in compliance;
3. Reviewing the means of safeguarding assets and, as appropriate, verifying the existence of such assets;
4. Appraising the economy and efficiency with which resources are employed;

5. Reviewing operations or programmes to ascertain whether results are consistent with established objectives and goals and whether the operations are being carried out as planned.

Boyle (1993) notes that whilst the Internal Audit function has gained favourable accolades in the practitioner journals, the topic has generated minimal interest among academic researchers. Additionally, he points out that whilst an extensive amount of research has been carried out in the external audit field, there is a distinct scarcity of research monographs in the internal auditing field. Vinten (1996 sec 2, 3 and 4) provides a comprehensive review of the internal audit literature over the last fifty years and concludes that most internal audit research has concentrated on reporting of data and descriptive studies of companies. Boyle (1993) claims that lack of theory for the use of internal audit as an organisational control, is the main reason why little research has been done in the area. Theoretical propositions for Internal Audit have been proposed by a number of authors:

1. San Miguel and Govindarajan (1984) discuss the inter-relationship between the divisional controller and the internal audit function. Their research suggests that a contingent relationship exists between the divisional controller's independence from the Division and the duties and responsibilities assigned to the Internal Audit function;
2. Boyle (1993) proposes a theoretical framework identifying four roles/relationships:
    a. contribution to organisational compliance, efficiency and effectiveness;

b. development of future managers;

c. participation in the external audit examination;

d. contribution to organisational legitimacy.

3. Adams (1994) proposes an agency theory framework for internal auditing. Agency theory postulates that the firm consists of a group of contracts between the principals (the owners of the economic resources of the firm) and the agents (the managers who use the economic resources) (Jensen and Meckling 1976). It also assumes that principals and agents will act rationally and behave in the best interests of the firm. Adams (1994) argues that one way that the agents can ensure that the principals don't make adverse judgements against them, is to 'demand monitoring services' such as internal audit, to confirm that they are behaving as the principals would wish;
4. McNamee (1995) discusses a number of models that help explain why Internal Audit exists and where internal auditors can best add value. For example, a four phase interaction model is proposed, looking at the focus, processes, role and impact of Internal Audit and how it ought to function;
5. Spraakman (1997) proposes a transaction cost economics theory for internal auditing. Transaction cost economics is a variation of agency theory and 'conceptualises intra-organisation production as a series of activities linked by transactions' (Spraakman 1997). Through the work they undertake, Internal Audit are seen as providing superior information to managers about the cost economics of the transactions, and hence their role is crucial to the organisation.

Evidence from the practitioner literature supports some of the propositions being made, for example, Allott (1996) discusses using internal audit as a training ground thus supporting Boyle's (1993) 'development of future managers'.

Specific reference to the role of Internal Audit in banks is mentioned by Cade (1997) who lists five activities: (1) inspecting the books in all locations of the bank (including branches); (2) monitoring the operation of risk controls; (3) participating in the design of new risk controls; (4) managing all aspects of fraudulent activity; (5) acting as a point of contact with industry peers and the police on intelligence matters. The role of Internal Audit in operational risk management is discussed by Blacker (1998) and the importance of Internal Audit in operational risk management was identified by the BBA (1997) who found that 80% of banks in their survey used Internal Audit reports to determine their response to risk.

2.3.2 External Auditing

External auditing has a different emphasis to internal auditing. In the UK, the external audit is a legal requirement carried out by a suitable qualified person in order to give an opinion on the truth and fairness of the Annual Report and Accounts of an organisation. Gray and Manson (1989) p 9 define an audit thus:

> 'An audit is an investigation, or a search for evidence, to enable an opinion to be formed on the reliability of financial and other information by a person or persons independent of the preparer and persons likely to gain directly from the use of the information, and the issue of a report on that information with the intention of increasing its credibility and therefore its usefulness'.

The auditor's opinion is intended to assist the shareholders to 'take decisions by reason of the information it gives on the quality of the statements, accounts, conduct, performance

or achievement of the persons or organisations involved' (Flint 1998 p 45). It is much more concerned with the accounting systems and financial controls rather than the complete internal control system although the external auditors work will involve making a judgement on the robustness of the internal control systems from which the Annual Report and Accounts are derived.

Whilst internal auditors are accountable to management, external auditors are accountable to shareholders. Nevertheless there is scope for both parties to work together and a study by Felix et al (1999) in America found that the relationship between the two parties can be categorised in one of four ways:

1. Co-existence – both parties pursue separate missions;
2. Co-ordination – both parties plan independently but share information on risk analysis;
3. Integration – both parties share risk models and audit plans;
4. Partnering – both parties have a shared mission and work together in a joint and integrated way.

The results of their work found that 60% of internal auditors characterised their relationship as one of co-ordination.

The external audit process and the use of an appropriate risk analysis is described in Grobstein and Craig (1984). They see the approach as being split into three phases: initial planning, program development and program execution. The initial planning process involves an overall view of the client's current business and financial situation as a pre-

cursor for developing an overall audit plan (Grobstein and Craig 1984). Peters (1991) identifies how, in this process, external auditors identify potential risks (to the audit) as a 'first step' in developing an audit plan, in part to mitigate those risks

2.3.3 Internal Control

Fayol (1949) identified control as one of the five functions of management, the others being planning, organising, commanding, co-ordinating. By control he meant 'verifying whether everything occurs in conformity with the plan adopted, the instructions issued and principles established'. The IIA (1998b) define control as 'any action taken by management to enhance the likelihood that established objectives and goals will be achieved'. They go on to say that control is the result of proper planning, organising and directing by management and that there are three types of controls:

1. Preventive – to deter undesirable events from occurring;
2. Detective – to detect and correct undesirable events which have occurred;
3. Directive – to cause or encourage a desirable event to occur.

Internal control came into general use to distinguish controls within an organisation from those existing externally to the organisation (IIA 1998b). Since internal auditors work within an organisation and are responsible for evaluating management's response to all controls, the distinction between internal and external control[22] is not necessary. Equally, from the organisation's viewpoint, internal control is considered synonymous with control within the organisation.

[22] For a detailed review of the relative strengths and shortcomings of internal and external control mechanisms see Walsh and Seward (1990)

An internal control system has been defined (Turnbull 1999) as 'the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives;
- help ensure the quality of internal and external reporting;
- help ensure compliance with applicable laws and regulations and also with internal policies with respect to the conduct of the business.

This definition introduces the concept of risk and how the internal control system responds to or manages the risks that the business faces. As such it provides a link between the maintenance of an internal control system and the management of risk.

The development of control theory is traced by Giglioni and Bedeian (1974) who conclude that the executive in an organisation has plenty of guidance to turn to in 'performing their control function'. Specifically, executives can use:

- A knowledge of the control concept;
- A knowledge of the process required to control;
- A knowledge of the characteristics of the control systems;
- A knowledge of the problems likely to occur when controlling and, therefore, a knowledge of what to guard against;
- A number of control models;
- A framework or principles for effective control;
- A set of control techniques.

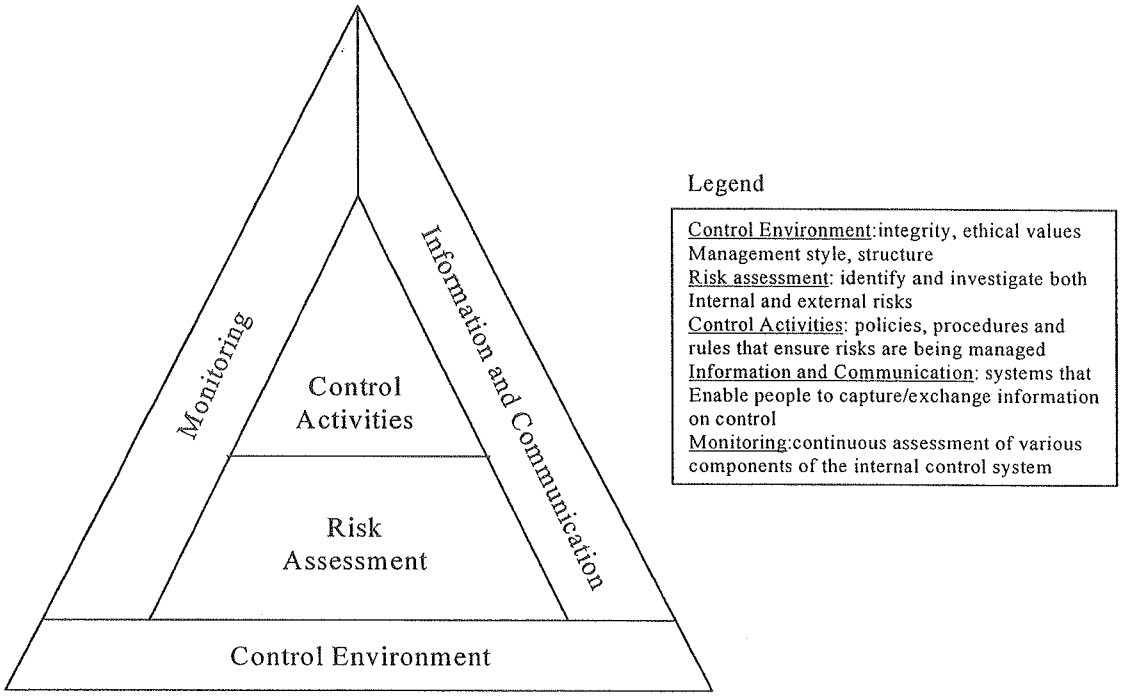
The design and analysis of internal control systems to help managers is discussed by Bailey et al (1981) who use complexity theory to illustrate how certain regulatory control requirements can impose theoretically unacceptable costs of analysis on the accounting and auditing professions with respect to internal control requirements. This suggest that a framework for developing internal control mechanisms would be useful to guide managers on how to design an appropriate system. Ouchi (1980) provides a framework at the organisational level and identifies three mechanisms known as markets, bureaucracies and clans each of which place different emphasis on both social and informational requirements required to drive the control environment of the business. Merchant (1982) addresses the organisational control problem from a different perspective by asking the question how can good control be achieved? Good control should mean that an informed person could be reasonably confident that no major unpleasant surprises will occur. His analysis concludes that good control can be achieved by avoiding some behavioural problems (to do with personnel) and/or by implementing one or more types of control to protect against remaining problems. The options available to protect against these remaining options are (Merchant 1982):

1. Problem avoidance controls attempt to disallow no opportunities for 'improper behaviour', for example, automation of a procedure avoids human intervention and provides enhanced reliability;
2. Specific action controls attempt to ensure that individuals perform (or do not perform) certain actions that are known to be desirable (or undesirable), for example, segregation of duties helps to ensure that one person cannot perform an improper act;

3. Control of results attempts to ensure employees are responsible for certain prescribed results, for example, performance measurement systems which provide rewards help to ensure objectives are achieved;
4. Control of personnel attempts to place reliance on staff to do what is best for the organisation, for example, sound communication systems help to ensure a consistent message is given and shared beliefs in organisational goals is created.

One internal control framework used in practice, is that which emerged from the Treadway Commission (COSO 1992) which has become commonly known as the COSO framework. This identifies an internal control structure consisting of five inter-related elements as shown in Figure 6 below.

Figure 6 Internal Control Framework



Source: Adapted from COSO (1992)

The COSO framework has been studied by a number of authors: Crawford (2000) describes how it is used in practice; Rezaee (1995) looks at the implications for internal auditors: Mills (1997) illustrates the link with shareholder value. Its emphasis on risk assessment and control activities being central to a sound internal control system provide further evidence of the link between risks and the role that 'controls' have to play in managing risks. This is a point endorsed by Preston (1993) whose in depth study of the relationship between risk management and organisational control concludes that a system of effective risk management can 'redirect the emphasis of control towards prevention rather than cure' and thus impact directly on the performance of the organisation.

The COSO (1992) framework is noted as being generic and illustrates internal control at the macro level. At the micro level, an organisation needs to establish its own internal control structure, which reflects the 'emphasis with which the entity's owners, Board of directors, and management place on controls' (Colbert and Alderman 1995). The types of issues that need to be addressed are discussed by Colbert and Alderman (1995) and are shown in Table 3. It is likely that management will place different emphasis on different aspects of this structure, reflecting the 'risks faced by the company' (Turnbull 1999).

Table 3 Broad Elements of the Internal Control Structure

Area	Examples of elements of internal control
Methods of assigning authority and responsibility	• Delegation of authority • Assignment of responsibility • Documentation of authorisation • Policies on conflicts of interest and acceptable business practices
Management's control methods	• Planning and reporting systems • Investigation and communication of variances from planned performance policies to develop and modify systems and control procedures • Investigation and communication of violation of laws and regulations
External influences	• Laws, rules, and regulations of regulatory bodies review and follow-up by external parties
Organisational structure	• Management functions • Reporting relationships • Data processing organisation
Management's philosophy and operating style	• Management's attitude and actions toward reporting • Management's approach to taking and monitoring business risks • Management's emphasis on compliance with laws and regulations • Management's emphasis on meeting financial and operating goals
Personnel policies	• Policies regarding hiring, training, evaluating, promoting and compensating employees
Audit Committee	• Role in communication between board of directors and internal/external auditors • Role in communication with auditors from regulatory agencies • Role In overseeing accounting and financial reporting
Internal Audit function	• Authority of internal auditors • Reporting relationship • Qualifications of staff • Resources

Source: Colbert and Alderman (1995)

It can be noted in the table that Internal Audit themselves are seen as an important part of the internal control system, a point emphasised by Turnbull (1999) who states that 'the Board of a company that does not have an internal audit function should assess the need for such a function annually'.

2.3.4 Internal Control in Banking

Basle (1998b) discusses a framework for internal control systems in banking organisations. Reaction to this regulatory pronouncement was mixed according to Talmor (1998) who quotes a number of practitioners who are concerned that the proposals do not address the potential for a 'more efficient allocation of capital' although it was recognised that it could help to set a 'common benchmark across the industry'. Basle (1998b) point to the significant losses incurred by several banking organisations and how they could probably have been avoided if the banks had maintained effective internal control systems. Five types of control breakdowns typically seen in 'problem bank cases' are identified:

1. Lack of adequate management oversight and accountability, and failure to develop a strong control culture within the bank;
2. Inadequate recognition and assessment of the risk of certain banking activities, whether on- or off-balance sheet;
3. The absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance;

4. Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems;
5. Inadequate or ineffective audit programs and monitoring activities.

The framework provides a response to these breakdowns and identifies thirteen principles, which should be followed for assessing the robustness of the internal control system including a specific requirement to recognise and assess all risks facing the bank (Basle 1998b, principle 4). The role of Internal Audit is mentioned, and indeed is criticised, for failing to be 'effective' in many banking organisations.

The previous section illustrated that the role of Internal Audit was focused on the internal control environment. Given the statement of Basle (1997) that 'operational risk is principally addressed through a firm's internal control framework', then it should be clear that Internal Audit has an important part to play in the effective management of operational risk. They would have a prime responsibility to independently provide assurance to the Board that operational risk exposures are being properly addressed.

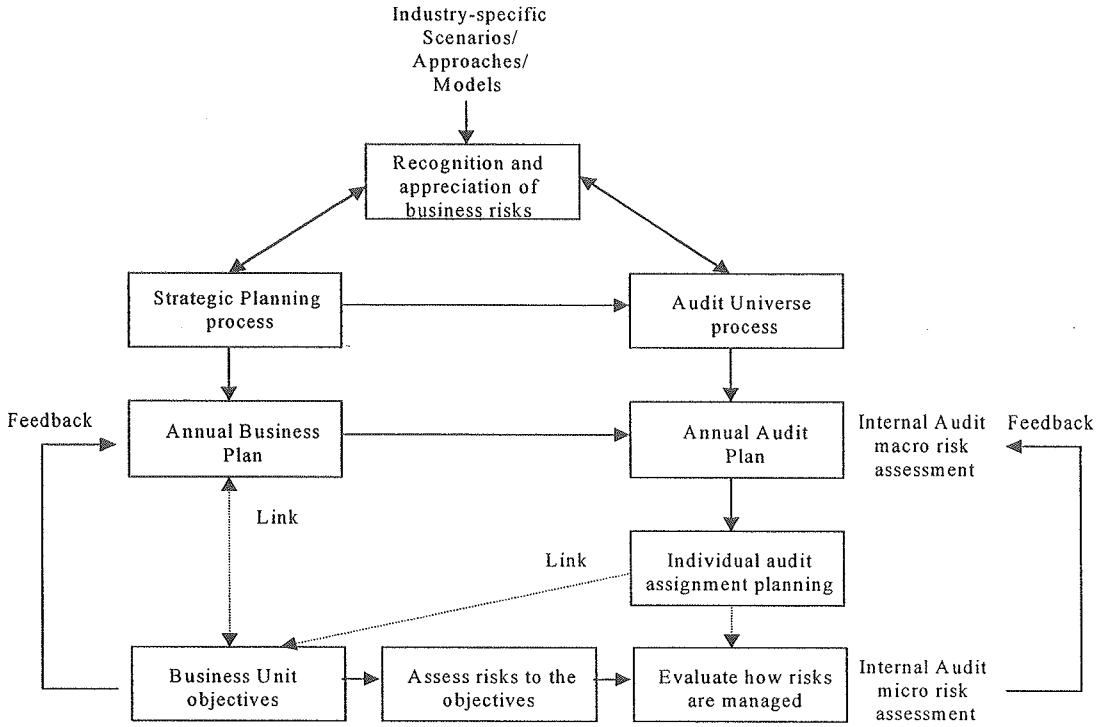
Internal control within banking is also discussed by Kinsella (1995a) whose analysis of the UK banking system, is driven by the need to understand the 'cultural differences between the banker and the auditor' and the impetus of many banks to invest in developing new 'risk management methodologies, procedures and controls' (p 4). Walsh (1995) examines a particular area of interest in the internal control environment of banks, namely, computerised systems and urges banks to think carefully about trying to 'gain a short-term competitive advantage through information technology' at the expense of the

'internal control standards' (Walsh 1995 p 20). Kinsella (1995b) sees three main issues that banks need to address when looking at internal control. The first relates to capital adequacy and internal controls, which are 'in many ways a front line defence for shareholder's equity and depositor's funds' (Kinsella 1995b p 102). The second is the behavioural dimension of controls, which have increased tension in them in areas such as derivatives trading where 'the line between trading and gambling is a narrow one' (Kinsella 1995b p 103). The third issue is whether the present overall control systems impair operational efficiency because of the 'onerous and costly body of compliance requirements' that have been established in a bank (Kinsella 1995b p 105). This latter point is particularly interesting because it highlights the potential for too much control in relation to the possible risk involved.

2.3.5 Audit Techniques and Risk

Internal Audit has a vested interest in managing risks through its review of the adequacy of the control procedures designed to mitigate those risks. McNamee (1997) and Paul (1994) illustrate this with a move towards risk-based auditing techniques in the banking sector. In evaluating internal controls Internal Auditors need to have an understanding of risks (including operational risks). As McNamee (1997) points out "instead of looking at the business process in a system of internal control, the internal auditor views the business process in an environment of risk". McNamee and Selim's (1998) research into this area identified a descriptive model of how integrated risk management and internal auditing are linked. This is shown in Figure 7.

Figure 7 Key Elements of an integrated risk management and internal auditing model



Source: Adapted from McNamee and Selim (1998)

The two elements of this diagram which describe a risk-based auditing approach, are:

- Internal Audit macro risk assessment (high level planning)– a review of the organisational goals in order to focus audit effort in the high risk areas;
- Internal Audit micro risk assessment (audit assignment planning) – a review of the business unit objectives, in order to focus audit work on how effectively management is dealing with the significant risks it faces in achieving its objectives.

A detailed examination of how the macro risk assessment is applied is given by Ziegenfuss (1995) who examines twelve internal audit risk assessment techniques and concludes that practitioners, irrespective of the risk assessment technique used, would be

well-advised to perform an *ex post* review to ensure that the assessment reflects the actual risks faced by the organisation. This could be done by reference to the actual losses incurred and/or major audit findings. Two further authors describe models that may be used in risk-audit planning: Hemaida (1997) uses a multifactor evaluation process to identify risk factors, rank the relevant auditable activities in terms of their riskiness and produce a composite score of for each audit area; Colbert and Alderman (1995) use a simple model of audit risk to help plan the audit:

$$AR = IR \times CR \times DR$$

where AR = Audit risk,

IR = Inherent risk – the risk, before internal controls, that there is an error in the population,

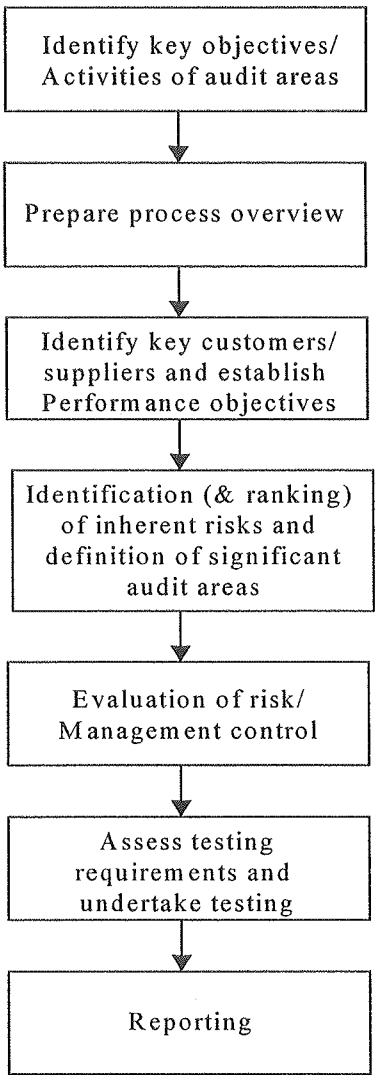
CR = Control risk – the risk that errors, when present, will not be prevented or detected by internal controls,

DR = Detection risk – the risk that audit evidence will fail to detect errors that do exist.

Each of these components is measured by the likelihood and probability of an error occurring (Friedlob and Scheifer 1999).

The steps in the internal audit micro risk assessment are discussed by Paul (1994) and are divided into a number of phases as shown in Figure 8.

Figure 8 Internal Audit micro risk assessment



Source: Adapted from Paul (1994)

Paul (1994) goes on to say that by selecting risk as the key audit driver, the internal auditor is 'encouraged to develop a fuller understanding of the commercial objectives and environment of the area under review' and in doing so, is able to 'demonstrate more easily the value that we (Internal Audit) can add to the business'.

2.3.6 Fraud

Kinsella (1995b p 101) points out that banks are perhaps uniquely vulnerable to the impact of fraud and the subversion of controls. The large scales losses that banks have suffered bear witness to this, perhaps the most famous being that of Barings which resulted in the complete collapse of the bank[23]. Cade (1997 p 197) discusses certain types of frauds which banks are particularly vulnerable to, including card[24] fraud, phantom cash withdrawals and money laundering. Money laundering, or the attempt by criminals to 'legitimise' the proceeds of crime by placing it into 'legitimate accounts' is one area of concern for all banks where they work together to combat this type of fraud.

Fraud is a risk that every organisation faces (ECIIA 1999) and Dowd (1998 p195) specifically describes fraud as an operational risk that a bank has to face. The ECIIA (1999) position paper on fraud highlights the role that Internal Audit has to play in fraud prevention and detection, highlighting that whilst Internal Audit can conduct fraud investigations but only if they have proper 'expertise and authority'. Fraud detection can be by pure chance, through the internal control system or what has become known as whistleblowing (Vinten 1995). Whistleblowing is defined as:

> 'the unauthorised disclosure if information that an employee reasonably believes evidences the contravention of any law, rule or regulation, code of practice, or professional statement, or that involves mismanagement, corruption, abuse of authority, or danger too public or worker health and safety' (Vinten 1995)

Whistleblowing may be used as an effective control device and a number of organisations now offer a confidential service to companies through which members of staff can

---

[23] For a detailed analysis of the Barings case see McConnell (1998)

[24] The term card embraces credit and debit cards, charge cards and all similar plastic instruments

telephone a hotline to disclose information they feel will help their organisation improve its control ethics (Crook 2000) and expose fraudulent activities.

Frauds against banks and the methods used to bring the perpetrators to justice are discussed by Nicholson (2000 p 49). He points out the complexities that can be involved with bank frauds and the administrative steps that need to be taken. Walden (2000 p 391) discusses a new type of fraud that is hitting banks that of 'crime in cyberspace' and illustrates, in particular, the jurisdictional issues that can arise because of difficulties in establishing where the event took place and having governments with harmonised computer crime laws (Walden 2000 p 400). All of these points illustrate the need to ensure that adequate control procedures are in place to guard against the threat of fraud risk and the impact that it may have on the bank both in financial and reputational terms.

Theoretical propositions concerning the effectiveness of countermeasures taken to prevent fraud acts include general deterrence theory (Straub and Welke 1998). This theory posits that individuals with an instrumental intent to commit antisocial acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts. This is seen as a particularly important deterrent in crimes involving computers where more active and visible policing is thought to lower potential abuse because the chances of getting caught and punished are perceived to be high (Straub and Welke 1998).

2.3.7 Corporate Governance

Corporate Governance has become much more prevalent in the UK over the last ten years (IIA 1999c). The debate on corporate governance began with the publication of the Cadbury report (Cadbury report 1992), which discussed the standards of financial reporting and accountability resulting from scandals such as Polly Peck, BCCI and Maxwell (IIA 1999c). Turnbull (1999) is the latest document to issue guidance on corporate governance and makes a specific reference to the board's role in internal control and risk management and the need to establish adequate monitoring procedures over the proper functioning of internal controls, which may include an internal audit function.

The UK is not alone in establishing guidance on matters of corporate governance. For example the Organisation for Economic Co-operation and Development has published certain principles of good corporate governance (OECD 1999) that are much broader in nature than Turnbull and discuss the rights of shareholders, the role of stakeholders, the responsibilities of the Board and disclosure and transparency of information.

Academic research in the area of corporate governance is beginning to develop and Burton (2000) provides an interesting theoretical analysis of the 'relative uniformity of Anglo-Saxon corporate governance codes' which, he says, are at odds with 'the basic tenet of contingency theory that for best performance require structural form to be tailored to the company's circumstances'. He points out that the argument that compliance with corporate governance codes will improve company performance is done without

significant evidence to support this position and that Boards which operate with a 'heavy emphasis on monitoring management' are normally associated with inferior performance. The implication of this research, if it were to be true, would suggest the balance between risk and the level of management control is indeed a fine one.

2.3.8 Implications for Operational Risk Management

The evidence from this review of the literature indicates that Internal Audit has an important role to play in the management of operational risks. Internal Auditors are interested in internal control where most operational risks are to be found (Basle 1997). The focus of their work should be around evaluating the mitigating actions taken by management to reduce the impact and/or probability of an operational risk materialising. Additionally, since they are, or at least should be, independent of management they will also be responsible for appraising the work of the risk units that exist within the bank.

The question arises as to what happens when Internal Audit is also given responsibility for operational risk management? There is evidence in the practitioner's literature (Cunnington 1999) to support this stance and Shackleton (1997) provides a brief case study on how the Internal Audit department of Rolls Royce plc[25] identifies and reports on risk. She points out that through discussion, the Board of Rolls-Royce identified the major risks facing the company and then requested the Internal Audit department to examine each of these risks and report on:

[25] Rolls Royce plc designs, manufactures and supports aero engines, gas turbines and power generation and transmission equipment.

- The scale of the risk
- The awareness within the organisation
- The means by which the risk was addressed
- Any weaknesses in the means of addressing the risk
- To what extent such weaknesses were tolerable or had to be remedied.

Organisations that have this dual Internal Audit responsibility may have adopted this approach for a whole variety of reasons, but from the banking perspective Basle (2001) will be looking towards an audit function that, inter alia, ensures the 'integrity of the overall risk management process'.

2.3.9 Summary

This section has provided an analysis of the internal audit function and illustrated how risk management has provided the impetus for a new paradigm to emerge in the way that internal audit work is conducted. Following an examination of the role of Internal and External Audit, a detailed description of internal control and control theory was given. A link between Internal Audit and the internal control environment was established and an overview of the risk-based approach to internal auditing was presented. Fraud and corporate governance, two areas of interest to Internal Audit, which also have an impact on operational risk management, were then briefly examined. The section concluded with a review of the implications for operational risk management.

2.4 Risk Management

2.4.1 The Concept of Risk and Risk Management

"I have observed that progressive managers no longer want to deal with information of a historical nature – other than to look at the past for its heritage value. Today, the emphasis is on what I call occurrence management, which concentrates on identifying a potential problem and taking action before it happens"

This quote by Rodgers (1986 p 122) appears to capture the essence of what proactive, as opposed to reactive risk management (Smallman 1996) is all about: identifying a potential problem (risk) and taking action (mitigation) before it happens. This is a view shared by Toft and Reynolds (1997) who describe the activity of risk management as being the embodiment of the old adage 'an ounce of prevention is better than a pound of cure'.

It is likely that most people's understanding of the word risk would similarly trigger the thought of something that could go wrong. A point emphasised by the Oxford English dictionary definition of risk, which is:

"the possibility of incurring misfortune or loss".

This negative definition of risk, however, ignores the expected benefits or rewards that can accrue from taking risks (Sadgrove 1996) and management has plenty of opportunities to take 'speculative' (Harris-Jones 1998) risks in areas such as the Treasury function, where the decision to invest can subsequently yield losses as well as gains. Equally, a failed business acquisition, a missed opportunity to enhance performance or the failure to move into a new business area are as much a risk as the possibility of a control failure (Martin 1998).

The concept of risk is normally associated with insurance (Williams 1996), a point which has been emphasised in the past by describing the risk manager's role in the organisation as being involved with the 'technical aspects of insurance' (Horrigan 1967). In organisational terms, risk and how it is managed have now taken on a much broader dimension and the assessment of risk in the development of corporate strategy should now go hand in hand (Froot et al 1994, Ealy 1993). This change in the risk management paradigm is illustrated by Williams (1996) who describes it as 'reinventing risk management' as per Table 4.

Table 4 Reinventing Risk Management

Old Paradigm	New Paradigm
Risk management only applied to pure risk	Risk management applied to pure and speculative business risks
Functional approach, limited to the risk management department	Process approach transcending functions and division
Insurance perspective	Business perspective
Risk manager	Risk process manager or risk champion
Senior management support	Senior management support and involvement
Insurance jargon understood by a few	Common risk language understood from the boardroom to the boiler room

Source: Adapted from Williams (1996)

The table identifies how risk management has broadened to cover all aspects of the business as well as illustrating how senior management understanding and involvement is essential in establishing the risk management 'culture'.

According to Beck (1992) risk is now a dominant feature of society. The business of estimating and assessing risk is complex and controversial and has become an industry

with many competing specialists (Krebs and Kacelnik 1997). A general concept of risk is defined by the Royal Society (1992 p 4) as 'the chance, in quantitative terms, of a defined hazard occurring'. It, therefore, combines a probabilistic measure of the occurrence of an event with a measure of the consequence of that event.

The concept of risk management is described as 'hazard identification, risk analysis, risk criteria and risk acceptability'(Royal Society 1992 p 5). According to Young (1999), the discipline of risk management is well advanced in sectors outside of financial services. He identifies a number of different 'experiences' of risk management that are drawn from these other sectors:

- The fundamental risk assessment processes are subjective and value laden and risk cannot, therefore, be precisely defined and unambiguously measured in objective terms;
- The actions of people cannot be predicted with certainty[26] and individual action, in particular, cannot be pre-specified and reduced to a simple numerical representation;
- In the case of extreme events, data is likely to be in short supply. This makes it extremely difficult to obtain a realistic, quantitative appraisal given the high level of uncertainty;
- Systems theory predicts that an open system can have an infinite number of ways of failing. It is not, therefore, possible to undertake a risk analysis of an organisation and specify an exhaustive set of failure modes;

- For a dynamic organisation operating in a dynamic global economy the past is not necessarily a good predictor of the future.

These experiences illustrate the complexity of risk management and some of the difficulties associated with quantifying risk exposures.

The growing interest in risk and risk management is evidenced by the increasing attention being shown by the quality newspapers about the subject. The Financial Times ran a ten part series on 'Mastering Risk' (Financial Times 2000) drawing on the collective experience of practitioners and academics alike and providing a 'comprehensive overview of the important concepts of risk management' (Part 1 p 2). Given this increasing interest in risk management, it begs the question why should organisations manage risk? Toft and Reynolds (1997) argue that 'good management is risk management' because it is not an 'activity which is separate from those which take place in mainstream management but the raison d'être for all management'. Kaen (2000) provides six reasons why he believes firms should manage risk:

1. Risk management can be used to align the interests of management with those of the owners of the company;
2. Risk management can be used to lower the firm's expected tax payments;
3. Risk management can reduce the costs of financial distress and bankruptcy;
4. Risk management can be used to encourage and protect firm specific investments;
5. Risk management can be used to assist firms in developing financial plans and funding programs;

---

[26] See Mars (1996) for a discussion on human failures and the implications for risk management

6. Risk management can be used to stabilise cash dividends.

A number of these issues are to do with managing cash flows, for example, the stabilisation of cash dividend payments, and both managing cash and managing risk are seen as essential for survival and creating value (Groth 1992). Froot et al (1994) go as far as to say that a risk management program should have 'a single overarching goal: to ensure that a company has the cash available to make value-enhancing investments'. It would appear that good risk management should lead to enhanced cash flows, which in turn should lead to improved performance (creation of shareholder value).

2.4.2 Risk Management Framework

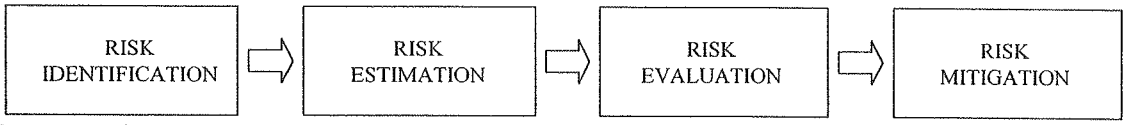
In considering how to manage risks, MacCrimmon and Wehrung (1986) provide a framework based on three components and focusing on the negative connotation of risk: the magnitude of loss, the chance of loss and the exposure to loss. The components of loss are described by Engemann and Miller (1992) as being a *threat* (a disaster that can lead to a loss of resources), which leads to an *event* (a loss of resource for a definite time period). MacCrimmon and Wehrung (1986) argue that to manage risk, you need to reduce one, or maybe all three, components. This could involve building complex models based on previous risk exposures within the organisation, assuming you are able to capture the data (Miccolis 1996) although it is likely that the initial risk assessments will be done very much on a judgmental basis.

A number of authors (Acs 1985, White 1995, Sadgrove 1996, Shackleton 1997, Harris-Jones 1998) summarise the principal approach[27] to risk management as having the following four phases:

1. Risk Identification - perceiving hazards, identifying failures, recognising adverse consequences;
2. Risk Estimation - estimating risk probabilities, describing the risk, quantifying the risk;
3. Risk Evaluation - estimating the impact of the risk, judging acceptability of the risk, comparing risks against benefits;
4. Risk Mitigation - deciding on an appropriate course of action such as acceptance, reduction, insurance and so on.

This system can then be applied equally to all types of risk exposure within a company and is summarised in the model shown in Figure 9.

Figure 9 Risk Management Model



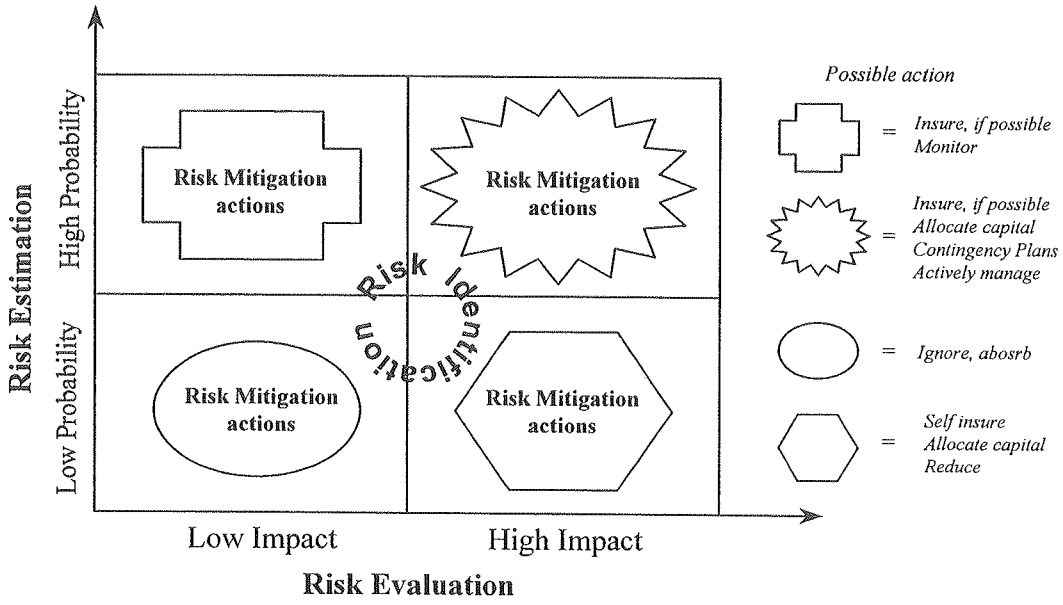
Source: Various

The model involves a systematic approach to risk identification, estimation, evaluation and mitigation. Figure 10 builds upon the work of Sadgrove (1996) and Shackleton (1997) and illustrates how risks can be categorised into one of four quadrants, depending on how the probability (risk estimation) and impact (risk evaluation) of the risk are

[27] The terminology may differ between the authors but as Acs (1985) noted there is considerable agreement about the components of the model even if the labels are different

assessed. There may also be scope for assigning different quadrants with different mitigation strategies as shown in figure 10:

Figure 10 Risk Management Framework highlighting possible mitigation strategies



Source: Developed by the author

This generic framework can be found and applied in a number of different industry sectors, for example:

- German and Robinson (1998) discuss how operational risk management for the North Atlantic pipeline involves, inter alia, continuous detection and tracking of icebergs (risk identification is an ongoing process) where the intervention (risk mitigation action) will either be 'modest' or 'aggressive' depending upon the assessment (risk evaluation/estimation) of the threat (the size/position of the iceberg);
- Kurland (1993) illustrates the 'defence-in-depth' (risk mitigation) design philosophy used in risk management in the nuclear industry;

- NHS (1999) illustrates how the risk management process can be used to assess the health care risk management context: clinical risk, organisational risk and financial risk

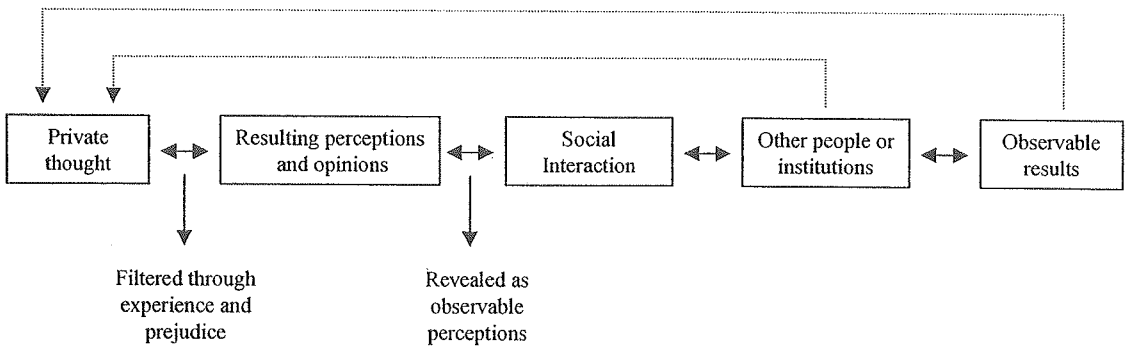
In addition, a whole body of literature has been developed on frameworks for managing project risks (Chapman and Ward 1996) with research focused in a variety of different areas of project risk: Benjamin et al (1995) examine a risk classification methodology for information technology projects; Raz and Michael (2001) look at the tools used in managing project risks; Lansdowne (1999) illustrates a system for prioritising project risks and tracking the progress of risk mitigation actions.

The reader will note that these frameworks are built around 'proactive' risk management, i.e. trying to prevent something happening rather than dealing with something that has happened (reactive risk management). Other methods for proactively managing risks are discussed by Hillson (1997) who develops a technique for benchmarking risk management in the organisation with suggestions on how it can be improved depending upon the current benchmarked level. Simons (1999) develops a risk exposure calculator to help gauge a company's 'likelihood of being surprised by errors or breakdowns' and suggests a number of control levers that can be applied to help mitigate the risks. For reactive risk management, Augustine (1995) provides a personal account of how organisations should handle crisis using a six stage process with the overriding message, 'resolve your organisation's crises promptly, they won't improve with age'.

2.4.3 Risk Perceptions and Decision Making

Teuber (1990) argues that our attitudes toward risk vary according to what has happened to us, what we expect, what we feel, what we know, and what we care about. In other words our perceptions of risk are selective and change as our social and business life changes. Klein (1996) notes that one of the reasons why a risk analysis may not be carried out in a project is because there is a 'perception that the risks are not sufficiently great or poorly understood to justify analysis and/or a perception that the risks will in any case be borne by other parties'. Much of the research into risk perception has focused on the public's viewpoint, rather than that of the managers (Gregory and Lichtenstein 1994), although managers are, of course, part of the public (Smallman 1996). The interplay of the variables that influence how people formulate their perceptions of risk has been studied by Ritchie and Marshall (1994) and their model is shown in Figure 11.

Figure 11 Risk perception formulation model



Source: Ritchie and Marshall (1994)

Wildavsky and Dake (1990) explain five theories of risk perception as follows:

1. Knowledge theory: the (often) implicit notion that people perceive technologies (and other things) to be dangerous because they know them to be dangerous;
2. Personality theory: some individuals love risk taking so they may take many risks, while others are risk averse and seek to avoid as many risks as they can;
3. Economic theory: the rich are more willing to take risks stemming from technology because they benefit more and are somehow shielded from adverse consequences;
4. Political theory: people view the controversies over risk as struggles over interests, such as holding office or party advantage;
5. Cultural theory: adherents of hierarchy perceive acts of social deviance to be dangerous because such behaviour may disrupt their preferred (superior/subordinate) form of social relations (and vice versa).

They conclude that people perceive a variety of risks in a manner that supports their way of life and suggest that risk communication programs might profitably be used to 'focus on the underlying causes of risk perception rather than only on the facts regarding possible harms'. This point on risk communication is picked up by a number of authors (Powell 1996, Kurland 1992, Royal Society 1992, Cox and Tait 1991). Powell (1996) discusses why risk communication, or the science of understanding scientific and technological risk and how it is communicated, has become so important and why risk communication programs will only be successful if they 'raise the level of understanding of relevant issues or actions, and satisfy those involved that they are adequately informed within the limits of available knowledge'. Covello et al (1987) highlight some of the

difficulties with risk communication and analyse the issues under four main problem areas: message, source, channel and receiver. Risk communication needs to address all four of these areas.

Risk perceptions are important in a business decision-making context because most of the early literature dealing with risky choice behaviour assumed that decision makers are risk averse (Fiegenbaum and Thomas 1988). Prospect theory, however, developed by Kahneman and Tversky (1979) indicates that when managers anticipate negative changes in wealth, they display risk seeking behaviour, but when anticipating positive changes in wealth, they exhibit risk averse behaviour. Adams (1998) describes this as being the 'balancing act between risk and reward'. Recent advances in behavioural decision theory have also confirmed that most individuals exhibit a mixture of risk seeking and risk averse behaviour (Fiegenbaum and Thomas 1988), a view supported by Wiseman and Gomez-Mejia (1998) who develop a behavioural agency model of risk taking which suggests that manager's risk taking varies according to the 'type of monitoring they are subject to' by the principals of the business (shareholders). Depending upon the circumstances, managers may exhibit risk seeking as well as risk averse behaviour. This balance between the two behaviours is illustrated vividly by Schwab and Schwab (1997) who describe a good manager as one:

> "who will always have his foot on the throttle, driving innovation, improvement, staying ahead of competition, building the best team, motivating the team to grow and be a winner (risk seeking). At the same time, the other foot constantly needs to be just a fraction of an inch above the brake pedal, ready to stop for detailed analysis and questioning (risk averse)".

However, not all managers can be good managers in the sense described by Schwab and Schwab (1997). Other research into risk taking behaviour (Hendrickx and Vlek 1991) has

highlighted how two factors, perceived control and the nature of the risk information available, have an important role to play in influencing the risk taking decision they will make. Information can play an important part in the decision making process about a risk and Menkes and Lave (1987) note that 'little attention has been given to the information requirements of risk management decisions'. Keeney (1996) argues for more explicit and quantified values whilst Straub and Welke (1998) suggest that risk management decisions about systems security matters can be significantly improved when 'managers are aware of the full range of controls available to them'.

The practical realities of decision making in an operational environment are developed by Beroggi and Wallace (1994) who propose the use of Decision Support Systems for 'interactive real-time risk management' where the decision maker is able to 'analyse risks and make decisions in real time during unexpected disruptions in the operations of large-scale systems thanks to advances in computer technology'. Pablo (1999) provides an interesting insight into the interpretation of risk and the decisions made across three industry sectors, oil and gas, commercial banking and software development. He finds that managers in these three different groups show different 'distributions of attention' reflecting different cognisance of risk and the likely decision they will take to mitigate it.

It should be apparent from the previous discussions that the aspect of risk perception is important in determining the decision made by the manager. There does not appear to be a 'one size fits all' model because the number of different variables at play are large and diverse. Baird and Thomas (1985) in developing a contingency model of strategic risk

taking identified a number of key variables that they consider affect the risk decision. For example, the self-confidence, knowledge, biases, heuristics and preferences of the decision-maker are important, whilst in the environmental area, the economy, government regulation, technological change and cultural values will need to be taken into account.

2.4.4 Focus on Operational Risk

2.4.4.1 Reviewing the definition of Operational Risk

Basle (1998b) noted that there is no universal definition of operational risk with many banks defining it as any risk not categorised as market risk or credit risk whilst others associate it with human or technical error. Basle (2001) defines operational risk as

"The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or external events"

This definition is taken from the major operational risk survey undertaken by the British Banking Association and PriceWaterhouseCoopers (BBA 1999a). Whilst it may be that this definition becomes universally accepted, the literature evidences a large number of definitions have been formulated to describe the term 'operational risk'. The following is a cross section of some of the definitions:

> *"Operational risk is the difference between the inherent risk of an activity and the hedges used to mitigate that risk"* – Senior (1999)

> *"The risk of fraud by employees and outsiders, unauthorised transactions by employees, and errors relating to computer and telecommunications systems"* – BBA (1999a), sample definition from one bank

"The risk that improper operation of trade processing or management systems will result in financial loss. Operational risk encompasses the risk of loss due to the breakdown in controls within the firm including, but not limited to, unidentified limit excesses, unauthorised trading, fraud in trading or in back office functions including inadequate books and records and a lack of basic internal accounting controls, inexperienced personnel, and unstable and easily accessed computer systems" - IOSCO (1998)

"The risk of loss resulting from breakdown in administrative procedures and controls or any aspect of operating procedures" Treasury Management Association of Canada (1998)

"The problems of accurately processing, settling, and taking or making delivery on trades in exchange for cash. It also arises in record keeping, computing correct payment amounts, processing system failures, and complying with various regulations" - Oldfield and Santamero (1997)

Apart from the first definition which appears to leave open many questions, such as what is an activity, and the last one which is very specific, the others appear to have as a theme: a loss resulting from a breakdown (failure/deficiency) in the internal controls (systems/procedures). This breakdown can occur for a variety of reasons some of which are quoted above – inexperienced employees, unauthorised trading and fraud. Equally, a

breakdown can occur because there is no control (or controls) in place to reduce the possibility of the risk occurring. Only one of the definitions (Treasury Management Association of Canada) places a boundary around the definition by linking the breakdowns to operating (as opposed to strategic) procedures. It is probably safe to assume that this boundary is implied in all the others, although the definitions of Senior (1999) and Oldfield and Santamero (1997) appear to have a narrower focus than the others.

Operating procedures are, however, a broad area and an understanding of what they mean would help to explain the areas that are covered. According to the British Banking Association and PriceWaterhouseCoopers (BBA 1999a) banks categorise operational risk into a number of different areas to help managers understand what the definition encompasses. Such areas include:

1. system failure/error;
2. transaction processing/control error;
3. business interruption;
4. internal/external criminal act;
5. personnel.

However, different banks use different categories, suggesting that operating procedures are interpreted differently by different banks.

A common theme in the definitions is that a loss will occur when an operational risk problem manifests itself. This would happen, for example, when there is a breakdown in

the control systems, which are designed to mitigate the risk. This establishes a link between a risk and a control[28], i.e. a risk is mitigated by a control (or a series of controls) and a control acts to reduce the probability of a risk occurring. A further common feature of the definitions is that risk resides within the business/processes/ procedures/systems or putting it more succinctly the internal control environment that exists within a company. This emphasises that operational risk resides in the internal control environment as per Basle (1998a) who in their consultative paper note, "operational risk is principally addressed through a firm's internal control framework". Continuing with this logic, it can be seen that the internal control framework (or the processes within it) give rise to (operational) risks which are in turn mitigated by controls. Diagrammatically this can be represented as in Figure 12:

Figure 12 The process/risk/control equation

Source: Developed by the author

Whilst this simple diagram may draw together the common components of operational risk and be intuitively easy to understand it does not necessarily illustrate the potential for loss arising from external as opposed to internal events. The author, however, offers it as a pictorial way of describing what is meant by operational risk from an internal perspective.

[28] The term control is used to describe any action which serves to mitigate a risk. This could include but is

2.4.4.2 The Increasing Importance of Operational Risk Management

"It is inherently difficult for banks, investment firms and insurance companies to understand the extent of the risks they are assuming at any given moment. Their ability to understand risk often lags seriously behind their urgent need to do so"

This quote from Dembo and Freeman (1998) illustrates a growing problem for financial institutions, how to ensure that the risks that they manage today are the ones that could affect their performance tomorrow. How well do banks understand their operational risks and the impact that they have on the business? In 1998 operational risk was seen as a 'priority for banks' (Price Waterhouse Coopers 1998b). Cade (1997) considers that the 'wholesale re-engineering of the business in recent years has forced bank management to look afresh at the challenges of operational risks'. A new impetus has taken shape driven by a number of factors. Blacker (1998) identified the following:

- *Globalisation* - there is an increase in risk exposure when a company leaves its home market and ventures into uncharted waters. Whilst companies can reduce the risks through joint ventures and strategic alliances the balance will be between the cost of the risk (we're going to do this on our own) and the cost of the control (we're going to play safe and share the risk with somebody else). Santamero (1996) discussed the 'global financial markets' that many banks now operate in and Dale (1994) sees globalisation in banking on a number of levels: the cross border delivery of financial services to foreign residents; the penetration of foreign financial markets; the transactions between banks from different countries. McConnell (1996), in his analysis of market risk, noted the increasing trend

---

not limited to internal accounting controls, risk management policies and any other form of management

towards globalisation with its "attractiveness to customers". A point re-iterated by Bell and Onillon (1992) who emphasised the marketing economies that can be made, but who warn that "greater concentration implies greater risk". All these studies illustrate how managing operational risk exposures, requires a global rather than a national mindset.

- *Outsourcing* - the trend towards outsourcing was noted by Thompson and Frost (1997) as being important since this type of service implies that operational implications need to be considered and understood as part of the contractual negotiations.
- *Information Technology* - McConnell (1996) illustrated how the rapid developments in Information Technology provide the platform from which financial services companies can provide new and enhanced services to their customers. The reduction in transaction costs brought about by these developments has seen new entrants into the UK banking market - supermarkets such as Tesco and Sainsburys and retailers such as Marks and Spencers. This is a dual edge sword in the management of risk since it requires new processes to deal with the new technologies (operational risk) and new strategies to deal with the competition.

- *Business Climate* - Santamero (1996) cited informed customers, new entrants and financial innovations as being the main driving forces that were leading to increased competitive pressures and a greater need to manage operational risk. Shackleton (1997) discusses the "current climate of rapid change" and how it is,

---

control (see Merchant 1982)

for example, reducing decision-making timeframes and making people less aware of "unusual" events. In such an environment the management of risk should be an ongoing, and not a static, process.

- *Regulation* - Basle (2001) is discussed in section 2.4.4.6 in the context of what regulators will require of banks vis-à-vis operational risk and in the UK environment. Turnbull (ICAEW 1999) has placed more emphasis on risk management and the disclosure and reporting of risk management activities.

Banks, however, should expect some benefits to accrue from this more formal/active/ explicit management of operational risk. Jameson (1998) identifies some of the expected gains:

- A quantifiable reduction in losses;
- Better risk mitigation;
- More efficient allocation of capital;
- Risk 'comfort' for senior managers;
- Risk 'comfort' for regulators;
- Improved project investment analysis.

This last point is particularly important in large-scale information technology projects where significant risks (high impact) can occur and where there is a greater need for 'more comprehensive risk frameworks able to catch where and how risks arise' (Willcocks and Griffiths 1994).

As a result of the increasing emphasis that has been placed on operational risk, the seeds of academic research have begun to develop. Examples of research into theoretical propositions for operational risk in the financial services arena remain few and far between. Two examples are given below:

- Wiseman and Catanach (1997) – examines the relative contributions of prospect theory and agency theory explanations for specific operational risks and subsequent firm performance in both regulated and non-regulated environments;
- Sheedy (1999) – critiques three of the techniques used for operational risk measurement, concluding that they are all flawed, and proposes that financial institutions should focus their attention on using an agency theory framework for managing operational risk;

2.4.4.3 Operational Risk and Internal Control

Olive (2000 p 137 - 145) provides a detailed analysis of why sound internal control systems are fundamental to the management of operational risk. He reviews a number of well-known operational risk incidents involving fraudulent conduct and reckless management and finds that the general consensus as to why they occurred are because of the critical absence of or failure to enforce: (1) internal control systems; (2) internal audits of those mechanisms and; (3) corrective actions to mitigate or prevent opportunities for fraud, reckless management, or conflicts of interest raising the potential for such behaviour.

The Basle (1998a) report has placed a bank's internal control system firmly at the centre of operational risk management. It proposes a framework consisting of 14 principles that banking supervisors should use when evaluating a bank's internal control systems, with paragraphs 20 to 23 examining risk assessment in the context of internal control systems. A risk assessment should be carried out to evaluate the internal and external factors that could adversely affect the achievement of the banking organisation's "operational, information and compliance objectives" (these are the main objectives of the internal control processes that should be in place). The linkage of processes, risks and controls discussed previously, forms the basis by which "senior management should ensure that the risks affecting the achievement of the bank's strategies and objectives are continually being evaluated" (Basle 1998).

The implementation of a comprehensive system of internal control within a defined framework is the key to ensuring that risk in general, and operational risk in particular, can be managed down to an acceptable level. An ongoing evaluation of internal control is, therefore, an important element in identifying operational risk exposures.

2.4.4.4 Operational Risk Mitigation

"The challenge of risk management is to minimise the probability and magnitude of adverse events without incurring excessive costs" or from a manager's perspective, "how safe is safe enough". These two quotes from Rayner (1987) capture the essence of risk mitigation and can be applied to operational risk and any other risk that the organisation faces.

Basle (1998b) discusses a number of techniques used to mitigate operational risk. The most important two mentioned are internal controls (which act to reduce the impact/probability) and the internal audit process (which is part of the internal control process). Insurance is also mentioned as an important mitigant. This issue is taken up by Hommel (2000) and also Cade (1997 p197) who discuss the ways in which insurance can be used to manage 'catastrophic risk'.

Risk (in banking) is also mitigated when key decision-makers in organisations see the 'big picture' (Roberts and Libuser 1993). They go on to point out that the organisation should be designed so that information about risk flows to those decision makers who can put together warning signals from various areas in the organisation, thus forming a picture of a risky or hazardous situation in its early stages of development. These warning signals or key risk indicators are discussed in a banking context by Cheaney (2000) who provides a number of examples of the indicators that may be used. Some examples of specific risk mitigation actions in an information technology environment are given by Bandyopadhay et al (1999). They discuss, for example, data security risks being controlled by backup files, password control, fingerprinting and voice recognition. Computer viruses can be controlled by monitoring computer usage, scanning software, stringent audit procedures and employee education.

Selecting the most appropriate mitigation/control strategy is seen as being central to risk management (IIA 1998a). Such strategies are noted as either:

- Avoiding the risk by suggesting alternative courses of action;
- Eliminate the cause of the risk;
- Reduce the likelihood of the risk occurring;
- Reduce the direct consequences of the risk;
- Minimise its impact in business terms;
- Instigate further investigation to gather further information before a final decision is made;
- Accept the risk as unavoidable.

Whilst these are generic risk mitigation strategies, they can equally be applied to operational risk exposures.

2.4.4.5 The Quantification of Operational Risk

Market risk[29] exposures are typically quantified in terms of a 'value at risk' (VAR) estimate (Kupiec 1995). The history of VAR is traced by Reed (1997) to Dennis Weatherstone , the chairman of JP Morgan bank who asked for a one page report to be delivered to him summarising the company's 'exposure to moves in the markets' and providing a 'decent estimate of potential losses over the next 24 hours'. Titus and Lewis (1997) provide a practical working definition of VAR as:

> "Value at Risk is the largest likely loss from market risk (expressed in currency units) that an asset or portfolio will suffer over a time interval and with a degree of certainty selected by the decision-maker"

VAR has become a common tool in measuring market risk and the majority of the literature deals with its application in this area: "VAR is found to work best for

frequently-traded instruments for which market values are easily available" (Simons 1997).

VAR essentially defines the maximum a firm could lose given a certain level of confidence over a given time horizon, should exchange rates, interest rates and commodity prices move against it. The calculation of VAR in this context is well covered by a number of authors (see Titus and Lewis 1997, Smithson and Minton 1997 and Kupiec 1995) and can involve a number of methods normally based on historical information, simulated information or a combination of the two.

The application of a VAR approach in the area of operational risk is, however, less well developed, and the recent Basle (2001) guidelines offer three alternative approaches to 'valuing' operational risk:

1. Basic indicator approach – calculates a value for operational risk capital using a single indicator as a proxy for an institution's overall operational risk exposure;
2. Standardised approach – calculates a value for operational risk capital based on standard business units using a broad financial indicator (e.g. income) multiplied by a beta factor (i.e. proxy for the operational loss experience);
3. Internal measurement approach – uses the bank's own internal loss data and a combination of qualitative and quantitative methods to calculate a value for operational risk capital.

[29] Market risk may be defined as the risk that a bank's assets/liabilities may move in such a way that it will lose money (McConnell 1996)

The practitioner's literature has a number of articles which deal with operational risk valuation (BBA 1999a, Kimber and Hoffman 1999, Hoffman and Johnson 1996, Parsley 1996) and academic papers have also been appearing on the subject (McConnell and Blacker 1999, Sheedy 1999).

It is clear from Basle (2001) that banks still have work to do in adequately measuring operational risk exposures and even the basic concept is not without critics (Sheedy 1999, Ong 1998). It may be that the application of a judicious approach to measuring operational risk would be sufficient for most organisations, but as one practitioner told the author, "you set aside capital for the unexpected and not the extreme", a view supported by Dowd (1998) who states that whilst some operational risks may be easily quantified, others are 'clearly impossible' (Dowd 1998 p 198). A further assessment of risk measurement models is given by Kupiec (1995) who finds that performance based VAR models require a 'large sample to produce a reliable assessment'.

This brief analysis of the current debate on operational risk quantification illustrates that there is still some work to do. Whilst operational risk measurement will remain an important goal in the long term, operational risk management will continue to remain the focus of attention for bank management.

2.4.4.6 Regulatory Issues

The recent regulatory pronouncement of Basle (2001) has been discussed in section 2.2.4.

Reaction in the financial press has been generally positive to the regulations – 'a step in the right direction' (Economist 2001) and the timescale for implementation (2004) should allow banks plenty of time to ensure that they can comply with the requirements.

Basle (1998b) initiated some qualitative research work into operational risk management looking at six specific areas: management oversight, risk measurement, monitoring and management information systems, policies and procedures, internal controls and the role of the supervisors. The results of the survey showed that the most important types of operational risk involve breakdowns in internal controls and corporate governance, whilst other aspects of operational risk include major failure of IT systems or events such as major fires or other disasters. The British Bankers Association produced a discussion paper (BBA 1999a), which identified a number of key issues for the regulators to address, focusing specifically on the introduction of a capital charge for operational risk.
Other regulatory pronouncements in the financial services sector have appeared over recent years (IOSCO 1998, IOSCO 1994) discussing, inter alia, operational risks issues. These papers also aim to provide guidance to supervisors, and indirectly financial institutions, on risk management principles and, in particular, the policies, procedures and internal control systems that need to be in place to manage risk effectively. Further advice comes from Zeckhauser and Viscusi (1996) who looked at the challenge that governments face in risk regulation efforts. They call for an 'appropriate balance' and an 'avoidance of institutionalising common irrational responses to risk'.

2.4.4.7 Operational Risk Management Roles

According to Ealy (1993), effective risk management is the result of a sound risk management strategy that is grounded in the realities and culture of the company and has top management support. Tschoegl (2000) argues that the key to (operational) risk management is management, a point taken up by Sheedy (1999) who says that such management, if they are to act in the best interest of the owners of the business should have 'character'[30]. The personal characteristics of individuals who have to manage operational risk are beyond the scope of this thesis, but are nonetheless important points to recognise, since ultimately it is people who have to manage operational risks in an organisation.

A brief overview of the management structure required to manage operational risk in a trading environment is presented by Rotberg (1992). The Board and Senior Management responsibilities in respect of operational risk are described as setting policies and tolerances (FSR 1999) and irrespective of how risk management is structured, each business line must be responsible for understanding the operational risk inherent in its activities (Basle 2001, FSR 1999). Jameson (1998) notes how 'an increasing number of financial institutions have been creating specialist operational risk manager roles at a senior level'. Their role is described as 'the creation of a group-wide culture of operational risk awareness'. Jameson (1998) also points out that many institutions make use of their (internal) audit function to monitor the implementation of group operational

[30] A person of character does what is right not because of a set of rules, or a reward structure, or because his/her actions will be noted by superiors, but because of the intrinsic merit or worth of those actions (Sheedy 1999)

risk policies, while deliberately excluding them from the actual formulation of rules about operational risk (a point which enhances their independence). This latter point is also noted by the BBA (1999a) who note three organisational models for operational risk management: internal audit driven – here the Internal Audit unit takes a lead role in operational risk management; Head Office driven – here a small, centralised function assumes responsibility often supported by local operational risk managers and Internal Audit; Non-head office driven – here dedicated decentralised operational risk management units are in place in the Divisions/Business Units with Internal Audit providing a supporting role.

2.4.5 Summary

This section has provided an analysis of risk management with a particular focus on operational risk. The concept of risk was discussed with the distinction between proactive and reactive risk management being noted. Risk pervades all aspects of society and business and there have been a number of developments over recent years which have produced a generic risk management process model which can be applied to operational risk. The process is subjective and value laden and relies on people making judgements. Risk perceptions of managers and individuals are, therefore, important in formulating these judgements. Risk perceptions were found to linked closely with risk communication and the use of a common risk language. A number of theories of risk perception were presented illustrating the complex nature of the subject.

The decision-making that takes place in the risk management process can be enhanced if the right information is made available to the manager. This was seen to be important factor because there can be so many variables at play in making a risk management decision.

The literature review then focused on operational risk. It was noted that there had been a move towards more explicit (as opposed to implicit) operational risk management. There is as yet no universally accepted definition of operational risk although there are number of common themes around the definitions that were reviewed and generally speaking, the focus of operational risk is in the internal control environment. Operational risks were seen to be embedded in the processes (of the internal control systems) and were mitigated by the controls that management put in place. The reasons why operational risk has become important in the banking industry were identified and the scarcity of academic research was noted. This is no more so than in the area of operational risk mitigation where the processes that may be used to mitigate risks were described.

A distinction between operational risk management and operational risk measurement was noted, with the former being concerned with creating an adequately controlled internal environment and the latter being concerned with quantifying the total operational risk exposure. The two activities appear to be mutually exclusive but both are recognised by the regulators as being of equal importance. A discussion on the Value at risk (particularly in the market risk area) concept was presented, although it was noted that there was still some way to go in the measurement area.

The section concluded with a review of the regulatory situation following the recently published Basle (2001) accord and an examination of the role of the operational risk manager.

2.5 Management and Organisations

2.5.1 Theories of Management and Organisations

According to Hatch (1997 p 76), some of the earliest research on organisational environments built upon the observation that organisations differ considerably depending upon whether they operate in stable or rapidly changing environments. In stable environments, organisation are characterised by strict hierarchies and clear lines of responsibility whilst in rapidly changing environments, organisations require flexibility and employees are not subject to the same rigorous control. Thus the notion of contingency theory was born: the organisational style is contingent upon the environmental conditions. Contingency theory is used by organisation theorist Henry Mintzberg (1989) to provide strategists with a framework for deciding which is the most appropriate strategy process for their organisation, and the importance of adopting the correct posture is highlighted by Fenton (1999) who notes that scientific studies show that:

- Organisations which are too set in their ways (having too many rules and too much central control) ultimately cease to exist;

- Organisations which are too loose (have few rules and everyone looks after themselves with little interest in others) also don't survive for long.

Salancik and Meindl (1984) provide evidence to indicate that the managements of 'unstable firms' seem reluctant to attribute poor performance to uncontrollable environmental events and instead demonstrate 'illusions of control' by manipulating casual attributions, or the words they use to describe the outcome of events. This has important implications for the way managers behave when times are difficult and when the need for sound judgement and 'honest' management is paramount.

Management behaviour was studied by Petit (1967) who argued that there are three types of managers who may be differentiated according to task, viewpoint, techniques, time horizon and decision making strategy. He describes a behavioural theory of management as 'the actions they take in dealing with the firm's primary needs of technical rationality and uncertainty avoidance' based upon a composite-system view of the organisation.

UK retail banks operate in a fast moving and rapidly changing environment and according to the above analysis will need to continuously adapt to survive. Fundamental to this will be the role of management in deciding upon the most appropriate strategy, and the importance of managers as a distinctive occupational category has long been recognised by a number of scholars (Taylor 1911, Fayol 1949).

The term management, however, is described by Tsoukas (1994) as 'ambiguous'. Does management imply a 'collective institutional process or simply a set of individuals

distinguished by the activities they carry out' (Tsoukas 1994)? He goes on to identify four perspectives on management;

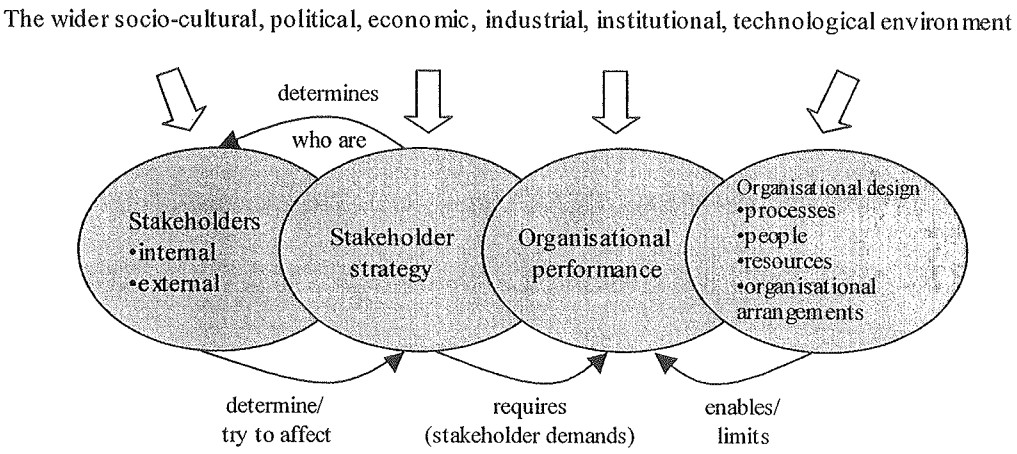
1. Management functions – the essence of management can be distilled into a number of functions (production function, administrative function, innovative function and so on), which need to be carried out in all organisations although how they are carried out may differ (Fayol 1949, Mintzberg 1973);
2. Management task characteristics – the tasks that management have to do within the functions are characterised by a number of different features such as being highly interdependent and context-dependent (Whitley 1989);
3. Management roles – managers' jobs can be analysed into a number of interrelated roles related to behaviours and attributed to relative hierarchical position (Mintzberg 1973);
4. Management control – arising from the nature of the relations of productions in capitalist economies, management is 'compelled' to create structures of control over the labour force (Thompson 1983).

Tsoukas (1994) concludes his analysis with the development of a metatheory of management, which proposes that the four perspectives may be viewed as ontological layers of management with different layers exhibiting different rates of change depending upon how various contingencies influence a particular layer.

Whilst the development of organisational theory has been well researched, its application for organisation design, functioning and performance in operations management is an

area for fruitful research (Ruffini et al 2000). Figure 13 illustrates the relationships between the core elements:

Figure 13 Relationship between core elements of operations management



Source: Ruffini et al (2000)

Operational risk management is seen as an integral part of operations management and the development of an appropriate organisational design and performance measurements (see Figure 13) are part of the generic research agenda in this area. The development of appropriate performance measures is picked up by Broadbent (1999) who advocates a contingency theory approach to performance measurement since 'as the environment becomes more flexible and unstable then performance measures must be sufficiently flexible to reflect these discontinuities'. The establishment of performance-measurement systems that are wrongly focused and too rigid may precipitate the fall into organisational decline and operational risk performance-measurement systems must fall within this area.

2.5.2 The Organisation and its Environment

Preparing for an uncertain future is best done by identifying major events that have already happened and that will have predictable effects in the next decade or two (Drucker 1997). External environmental factors can play an important role in determining strategy and questions such as 'what external forces are shaping competition' are viewed by Gordon (1997) as helping to 'stake out the future'. Porter's (1985) work on the five[31] forces now provides a well-established framework from which an organisation can objectively view its environment and the threats and opportunities that may lay ahead.

Environmental uncertainty has been well researched over the last forty years (Jauch and Kraft 1986) with the dominant focus being on 'internal uncertainty reduction strategies' or a focus on acquiring knowledge about the operation of the organisation. External uncertainty reduction strategies are described by Jauch and Kraft (1986) as a means of acquiring knowledge about the environment and, where possible and desirable, creating more uncertainty for others in order to try and gain competitive advantage. Acquiring this knowledge is often done by units within the organisation, which perform staff functions (Mintzberg 1979), such as market research, or it may be integrated into the responsibilities of those who operate in the external environment, such as salesmen (Jauch and Kraft 1986).

UK retail banks are currently subject to much environmental uncertainty in the area of operational risk. This is being driven by a number of factors including; the regulatory

situation (Basle 2001) which, at the time of writing (April/May 2001), was still only a consultative document and likely, therefore, to be revised; the Cruickshank (1999) report, which has a number of recommendations designed to remove the monopolistic grip of the main high street banks; and the spate of mergers and acquisitions which continue unabated[32].

2.5.3 Decision Making in the Organisation

"It is refreshing to find that the perfect decision making environment exists only in the minds of theorists"

This quote from Barnard (1992) is based on a study of 200 Chief Executive Officers in small fast growing companies and the processes and problems they encounter when making decisions. She concludes that even successful companies have not yet solved some of the 'nagging problems of management'. Whilst some may contest her quote on the theoretical positioning of decision-making or praxeology (Skyttner 1999) as it has come to be known, nobody would dispute that decision-making in one form or another, has been around for a long time[33].

The influential work of Simon (1977) provided a four phase decision making model (p 40) covering:

1. Intelligence activity – searching the environment for conditions calling for decisions;

---

[31] Gordon (1997) notes that Porter has acknowledged a sixth force, government, which may impact on all the others

[32] At the time of writing (April/May 2001) a merger between Bank of Scotland and Halifax bank had recently been announced and the proposed takeover by Lloyds TSB of Abbey National was with the monopolies commission

[33] For an excellent history of decision making see Arlington (1998)

2. Design activity – inventing, developing and analysing possible courses of action;
3. Choice activity – selecting a particular course of action from those available;
4. Review activity – assessing past choices.

Nutt (1984) expands upon this last activity and describes it as an implementation phase where the 'action plan' from the choice activity is implemented. Nutt (1984) goes on to explore the choice process in some detail and came up with 5 main[34] types used by decision makers:

1. Historical model – the solution would be drawn from the practice of others and would involve the decision maker selecting a procedure which is known to work
2. Off-the-shelf – the solution is drawn from a selection of best ideas overtly collected by the decision maker
3. Appraisal – the decision maker begins with an idea that has an unknown value and seeks to implement it rationally and top down (NB at worst, this could involve imposing the solution)
4. Search – the decision maker seeks a new solution but needs help in knowing where to look
5. Nova – the decision-maker seeks to implement a solution which is innovative and aims to challenge the way things are being done in the organisation.

Simon's model is, however, not without its critics. Anghern and Jelassi (1994) argue that the framework is a 'serious obstacle for the evolution of DSS (Decision Support Systems) theory and practice' arguing that different types of DSS could emerge from the adoption of alternative perspectives of human decision-making. DSS aims to extend methodologies

[34] Nutt had variations within the types which were essentially sub-categories of the main theme

and techniques developed in several research areas and to combine them into a new form of computer-based system able to support and enhance managerial decision-making (Anghern and Jelassi 1994). Such systems may be developed to (Eierman et al 1995):

- facilitate the structuring of a decision so that analytical tools, possibly several in combination, can be used in generating solutions;
- facilitate the use of the analytical tools that have been brought together through a structuring process;
- facilitate the manipulation, retrieval, and display of data.

Despite the growing interest in DSS , Kharbanda and Stallworthy (1990) note that 'subjectivity cannot be removed from the decision-making process' and that 'there is no substitute for intuition, experience and judgement' when it comes to making decisions. A view supported by Richardson and Bartley (1998) who state that 'people do not work mechanically in their business nature, they work by experience, instinct and analysis'.

Citing Kersten and Michalowski (1996), Rahman (1998) supports the use of Simon's model in helping to structure a DSS because:

- the generic aspect of the framework allows decision makers to concentrate on actions and supporting tools specific for particular phases of decision-making processes;
- its dialectical character helps to position the actions or tools and specify their role in the transition of the decision making activity;
- its analytical feature contributes to the decomposition of the decision problem and specification between its components.

From an operational risk mitigation perspective, it is unlikely that any DSS will have been developed to support the risk mitigation decision. The management of operational risk is in its infancy and banks are unlikely to have developed such systems at this early stage, although it is certainly an area where further research would be useful.

Tarter and Hoy (1998) provide an analysis of a number of decision making models and propose a contingency theory of decision-making which relates the situational contingencies facing the decision maker to the type of model to be used. They do, however, point out that 'decision-making theories are probabilistic not deterministic'. A further detailed analysis of normative models in decision-making is provided by Gordon et al (1975). Their analysis looks at process models by functional area, by process, by level (in the organisation) and by output and in all they analyse over 40 types. They make a number of specific recommendations some of which are important in the context of operational risk:

- Normative theorists must carefully study the real world of decision-making – the focus should be on understanding the application of the (operational risk mitigation) model in the field where dynamic factors such as political pressures, non-operational goals can be assessed in the context of the model;
- Normative decision models must encompass the whole decision process – the need to look at operational risk mitigation in the context of the wider management of operational risk and, in particular, a need to focus on the softer parts of the process;

- Normative models must deal particularly with dynamic factors and multiple goals – the need is for open-system models of decision-making which recognise conflicting goals, limited data, timing difficulties, possible interruptions, delays to implementation and of the factoring of larger decisions into smaller ones. In short, the constraints/barriers to operational risk mitigation.

Kahneman and Lovallo (1993) provide an analysis on decision makers and their behavioural attitude to risk when making a decision. They note that decision makers have a strong tendency to consider problems as 'unique' and the natural way to think about a problem is to bring to bear all one knows about it (experience), whilst paying special attention to its unique features. They also find that people also 'exaggerate their control over events' and 'the importance of the skills and resources they possess in ensuring desirable outcomes' from the decision, leading to more decisions being taken without fully appreciating the risks involved. In looking at whether organisations provide effective controls against the optimistic bias of individual executives they observe that a rational organisation would want to base its decisions on unbiased odds but that 'arrogance of optimism' can lead to mistakes in decision-making that can cost the organisation dearly. Evidence to support this view comes from Drummond (1992) who suggests that managers can spend 50% of their time dealing with the consequences of bad decisions.

This raises some interesting issues for banks in the context of operational risk mitigation. A consistent approach to operational risk mitigation (decision making) is arguably

required if management are to act rationally when faced with an operational risk problem. The challenge facing management is to articulate and spread their approach as an integral part of the operational risk management control strategy.

2.5.4 Barriers to Decision Making

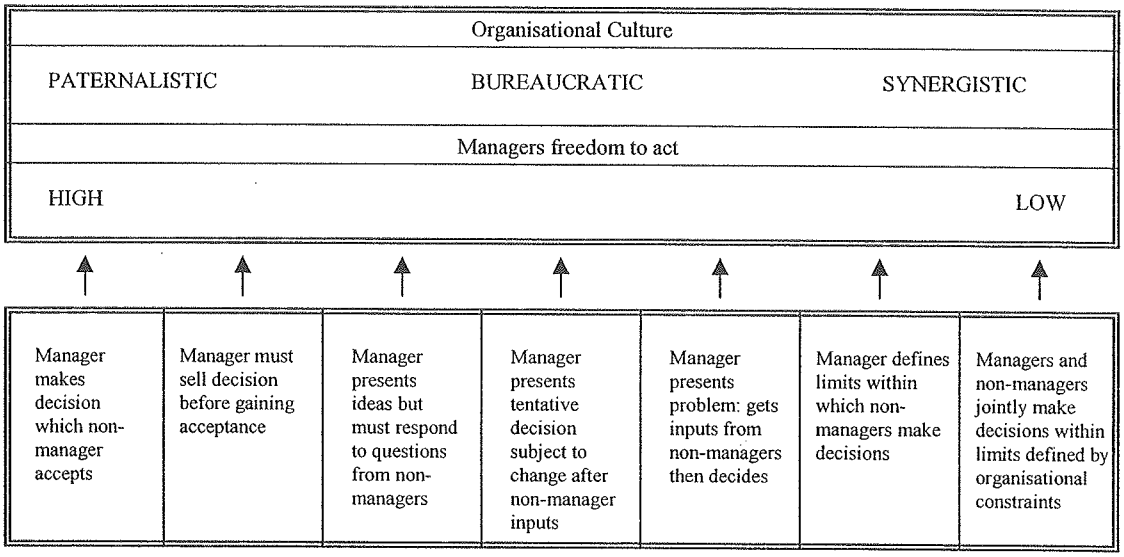
Hammond et al (1998) discuss how decision-making is one of the toughest as well as one of the riskiest jobs of any executive. They point to a number of well-documented psychological traps that are particularly likely to undermine business decisions: the anchoring trap, the status-quo trap, the sunk-cost trap, the confirming-evidence trap, the framing trap and the estimating and forecasting traps. Many of these traps can work in isolation or in concert. This argument supports the view of Glazer et al (1992) who discuss Simon's (1972) theory of bounded rationality which 'locates the constraints of decision-making not in the external environment, but in the decision maker'.

'The games that decision makers play' is explored by Brindle (1999) in her review of the cognitive decision processes. She identifies four common games that managers play, framing, criteria selection, misuse of analogy and rationality, and argues that whilst 'we cannot control human nature at the decision-making table, we can learn to be more adept at the games which are played every day'.

Another aspect of decision-making that is noted in the literature is based on the position of the decision maker in the organisation and the organisation culture (Basi 1998). Basi (1998) provides an analysis of decision-making styles vis-à-vis organisational cultures

and illustrates the freedom to act of the manager on a decision-making continuum. This is illustrated in Figure 14.

Figure 14 Organisational culture and managers decision-making ability



Source: Adapted from Basi (1998)

As can be seen from the diagram, the degrees of freedom available to the manager vary considerably depending upon the type of organisational culture that exists.

The references in this section identify some of the barriers or constraints that occur when decision-making has to take place in the organisation. Taken together, they illustrate some of the complexities involved in the decision-making process, all of which have implications for the way on operational risk mitigation decision is taken.

2.5.5 Implications for Operational Risk Management

There is evidence to indicate that UK retail banks are facing a changing external environment and that management will need to keep abreast of the changes that are

occurring and the operational risks that they may bring. Part of the management process requires looking ahead, planning for expected and unexpected outcomes, organising adequate resources, and controlling the work done. The operational risks associated with the future strategic intent of the bank in this turbulent environment, will require effective mitigation strategies. Management behaviour in dealing with these risks must take account of any 'delusions' of control that may exist and the development of appropriate performance measurement systems to monitor operational risks will assume increasing importance.

Operational risk mitigation involves making a decision and, as the analysis in this section has shown, this can involve a complicated set of processes contingent upon the nature of the problem. The complexity and subjectivity of the process provide illustrations of some of the constraints that put pressure on managers when the choice has to be made about what to do. This suggests that there should be a drive towards a more uniform and structured approach to the risk mitigation process taking into account the organisational culture and the freedom of managers to act.

2.5.6 Summary

This section has provided some theoretical propositions relating to organisations, management within organisations, how the organisation copes with environmental factors and decision-making. The emphasis within this section has been to provide a theoretical underpinning for the research and to place the research area, operational risk mitigation, in the wider body of knowledge concerning management and organisations. The review

highlighted how contingency theory can play a part in both the organisational structure and the decision making process. The behavioural aspects of management and the internal environment in which they have to operate also feature in the day-to-day decisions that managers have to make. The section concluded with a review of the implications for operational risk management

2.6 Summary of the Literature Review

This section has reviewed the literature in the areas of banking, internal audit, risk management, with specific emphasis on operational risk management, and finally management and organisations. The emphasis has been to describe existing theories in the context of operational risk management and also to provide an overview of some of the current issues in each of these areas. The author has not attempted to describe each area in detail, as this would be beyond the scope of this research. A general discussion is, however, warranted in order to place the research into a theoretical framework and illustrate to the reader the importance of the research in the context of the current business environment.

Section 2.2 was focused on the current challenges being faced by UK retail banks and illustrated how many of these challenges will impact upon their operational risk profile. The competitive climate in the UK is intensifying and the range of products and services offered by banks, building societies and insurance companies are almost identical. In this type of climate, differentiation and brand strength can add a lot of value to the customer

proposition, and he/she in turn may then be influenced to buy the name first followed by the product. Several key areas in the regulatory area illustrate the importance and timeliness of this study. Basle (2001) is likely to introduce a major shift towards even more explicit operational risk management as well as forcing the pace of change on how operational risk should be measured. The jury is still out, however, on their proposals and the implementation date of 2004 should provide a reasonable cushion for banks to 'get their act together'. Banks have always been in the business of taking risks and the discussion on risk management (in the current banking environment) confirmed the need for banks to establish clear risk policies that were understood by all as a first step to preventing some of the disasters that have beset the banking industry over the last decade.

Internal auditing and the Internal Audit function were discussed in section 2.3. Risk management has provided a new impetus for internal auditors and a new paradigm is emerging in the way that internal audit work is conducted. Risk-based auditing, as the term has become known, provides an opportunity for internal auditors to focus their work on the key risk areas of the business as well as assisting in the overall management of operational risk by focusing their audit work on how well risks in the business units are being identified, appraised and mitigated. A link between Internal Audit and the internal control environment was established and control theory was seen as an important part of the operational risk mitigation process. Most operational risks must be managed within the internal control framework and Internal Audit act as a control over the activities of management, including operational risk management. Some of the theoretical concepts

underpinning the role of Internal Audit were discussed with agency theory being noted as important in describing its role.

Risk management with a particular focus on operational risk was discussed in section 2.4. The concept of risk was discussed with the distinction between proactive and reactive risk management being noted. Proactive risk management uses a generic risk management process model to manage risk whereas reactive risk management is, in effect, resolving a problem that has occurred. The risk management process can be applied to operational risk and is recognised as being subjective and value laden, relying on people making judgements. The overall context in which risk management takes place is rooted in contingency theory and underpinning this are a number of other theoretical propositions relating to risk perceptions, or how the managers who have to manage risk view the risk they have to manage. These risk perceptions are important in helping to formulate the 'subjective and value laden' statements. The risk perception can be enhanced if the right information is made available to the manager before the decision is made.

In the operational risk area, it was noted that there had been a move towards more explicit (as opposed to implicit) operational risk management. There is as yet no universally accepted definition of operational risk although there is agreement that operational risks are embedded in the bank's internal control systems. A distinction was also made between operational risk management and operational risk measurement. This point is important when viewed in the regulatory context because whilst Basle (2001) discuss the

two activities, it is not clear whether they are viewed as mutually exclusive. To date little work appears to have been done on integrating the two.

Section 2.5 provided some theoretical propositions relating to organisations, management within organisations, how the organisation copes with environmental factors and decision-making. It was noted how contingency theory can play a part in both the organisational structure and the decision making process. The behavioural aspects of management and the internal environment in which they have to operate also feature in the day-to-day decisions that managers have to make. The theory of bounded rationality as it is described, identifies one of the barriers to decision making and is seen as important in the context of operational risk mitigation, which involves 'making a decision' about the most appropriate action to take.

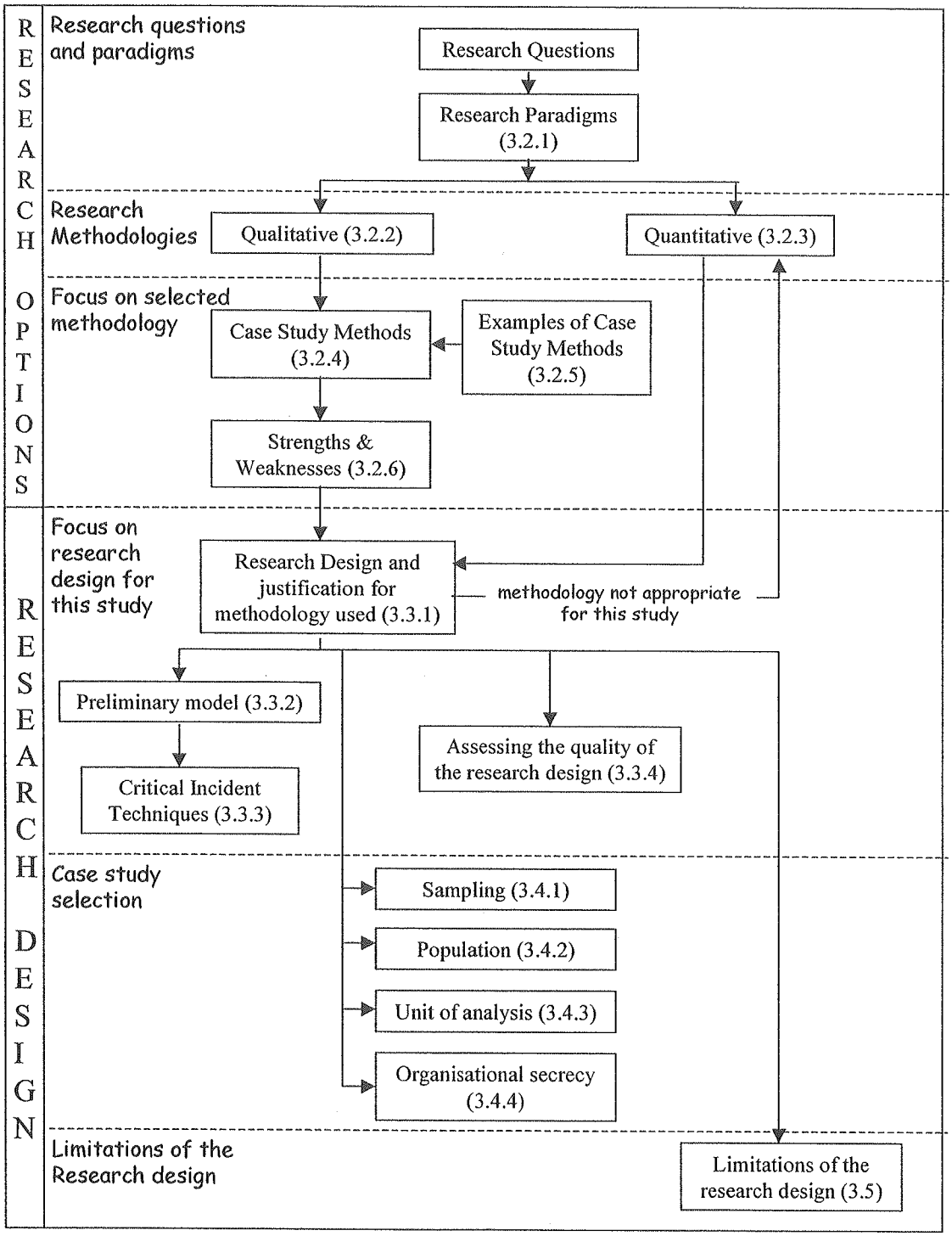
Following this review of some of the theoretical perspectives of operational risk management, the remainder of the thesis examines operational risk management (and mitigation) in practice. Chapters 3 and 4 describe the overall research design and the methods that have been used to collect and analyse the data. Chapter 5 then summarises the results of the data analysis and presents the findings of the study. Chapter 6 considers the implications of the findings for three groups arguably most interested in operational risk management: risk managers, internal auditors and the operational managers in the Business Units.

3. METHODOLOGY

A description of the research methodology and the logic for using the particular approach is described in this section. Following an overview of the proposed methodology (section 3.1), the structure of the remainder of this section is shown in Figure 15. The section is broadly divided into two main sections:

1. Research Options – linking back to the research questions, section 3.2 examines research paradigms, the two main research approaches and then focuses on case study methodologies as the most appropriate option for answering the research questions;
2. Research Design – section 3.3 focuses on the research design for the study and argues for the methodology used. Section 3.4 identifies the logic for selecting the case studies and section 3.5 discusses limitations of the design and strategies that have been used for mitigating these limitations.

Figure 15 Structure of section 3 showing sectional links



Source: Developed by the author

3.1 Methodology – In Outline

According to McGrath (1982) all research strategies are seriously flawed as the very strengths in regard to one desideratum function as serious weaknesses in regard to other, equally important goals. He goes on to advise researchers that they should be aware of the dilemmas facing them and be fully armed with possibilities on how to handle them. Gummesson (2000 p.111) describes the research process as a "taboo", arguing that the traditional model of research is presented as an idealized model but when confronted with reality, researchers, and particularly student researchers, realise the process is characterized by complexity and intractability. These truisms reinforce the need for the researcher to describe objectively his research methodology and the methodological position adopted and the appropriateness of the methods used to the questions posed.

The theoretical foundation upon which the research is based has been described in section 2, where the research problem was placed in the wider body of knowledge. The research is described as largely exploratory because no prior work was found to have been undertaken in this area and the research output may be viewed as building blocks of theory on operational risk mitigation. No hypothesis testing has been undertaken and the focus of the study was to collect data that would answer the research questions and enable a risk mitigation model to be developed. From the beginning the author was keen to model *core practice* in the field of operational risk mitigation.

The data was collected using multiple exploratory case studies, which are favoured for hypothesis generation (Yin 1994, McCutcheon and Meredith 1993, Bonoma 1985). An

initial pilot case study was undertaken to test the appropriateness of the key issues and revise the case study protocol which was based on that suggested by Yin (1994 p.63). Four UK retail banks were selected and four or five senior managers within each of the banks were interviewed. From the beginning it was hoped that the opportunity to discuss the day-to-day issues concerning the management of operational risk would provide a rich insight into how and whether any core practice was emerging. The author was equally concerned to ensure that the research deliverables would help such managers in mitigating operational risk. Managers treat theories as tools (Worren et al 1997). Their primary goal is to use theories, and the knowledge that they bring, to achieve organisational goals[35]. The scientific validity of this knowledge is of lesser importance to managers than its practical usefulness (Worren et al 1997). The managers were the unit of analysis within the study and each case was treated as a separate entity before cross case analysis and comparison was undertaken.

For reasons of confidentiality, the banks in question cannot be named and each has been referred to by a Greek letter. The author was keen to study banks that were appropriate for the type of exploratory research envisaged. Otley and Berry (1994) note the following in this context:

> "Work should take place in fast-moving companies operating in rapidly changing environments so as to provide illustrations of developing best practice at the leading edge of adaptive activity".

The author is nervous about using the words 'best practice' when discussing operational risk in the financial services sector. Whilst operational risk has existed within UK retail

[35] The author is aware from some of the interviews and other anecdotal evidence that some of these goals

banks for many years, the literature review shows that the explicit management of operational risk has only developed over the last few years. Ten years ago, the term operational risk did not exist in financial services and the management of such risks was done implicitly as part of day-to-day responsibilities. It is for this reason that the term 'core practice' has been used. Notwithstanding this position, the selected banks all operate in the rapidly changing UK retail banking sector and each has been subject to significant change, over the course of the last few years.

The epistemology behind the research is rooted in postpositivism. Whilst postpositivism accepts that empirical observations are important, it rejects the idea that such observations are an immutable foundation for knowledge claims (Schwandt 1997). This is not to say that a positivist approach cannot be used within a case research methodology and the author has focused his work on providing a theoretical grounding, multiple sources of evidence (including the use of critical incidence techniques) and on persuasiveness of logical argument (Cavaye 1996). The logic of positivism applied to case studies ensures that the research can be evaluated against certain criteria: (1) the research should make controlled observations; (2) the research should be able to be replicated; (3) the research should be generalisable; (4) the research should use formal logic (Cavaye 1996, Yin 1994). The author believes that the methodology adopted and the case study results satisfy these criteria.

---

are linked to the management of risk within the organisation

A research process was developed at the start of the study as a means of guiding the work. Data was collected from a variety of sources including press articles, Annual Report and Accounts, Internet material, relevant internal documents (reports/memorandum/manuals /presentations) as well as the main data source, the interview transcripts. Most interviews averaged an hour and all interviews were taped and transcripts sent to the interviewees for correction. For each case study a detailed report was produced (the structure of the report can be found in Appendix B) and sent to the lead contact in the bank for corroboration. A follow-up discussion about the findings was then arranged. The interviews were held between February 1999 and July 2000.

To summarise, the research methodology involved developing a set of research questions and an *a priori* model based on the literature review. The model was used to focus the work in the principal area of interest, operational risk mitigation. Multiple exploratory case studies were used to collect the data. Data triangulation (Easterby-Smith et al 1991 p 133) was employed, with particular emphasis on the use of critical incident techniques where secondary data was normally available. A pilot case study was used as a basis for refining the case study protocol and the research model itself was revised and updated in the light of the research findings.

3.2 Research Methods in Perspective

3.2.1 Metaphysics and Research Paradigms

Questions concerning the methodological approach and posture[36] selected by a researcher

[36] Posture may be defined as the relationship that the researcher wants to have with his or her subject (Wolcott 1992)

are secondary to the choice of beliefs that govern the methods employed (Guerrier 1997). The author started this research recognizing that positivist beliefs appear to have dominated research in the physical and social sciences over the last fifty years but equally noticing the trend towards using post-positivist methodologies.

Researchers have an obligation, however, to fully describe their theoretical posture (Janesick 1998, p. 5) in order that the critical reader can understand how he/she construes the shape of the social world in which he/she operates, particularly in the context of the research project itself. Despite the author's early academic leaning towards the logic of positivism, subsequent job responsibilities, more heightened self-awareness together with the process of researching the underlying philosophies of research design, have moved this positioning on. The author's thinking is very much constructivist within the postpositivist paradigm. Constructivism is defined (Schwandt 1997) as being interested in the ways in which human beings individually and collectively interpret or construct the social and psychological world in specific linguistic, social and historical contexts. Guba and Lincoln (1994 p 105) describe constructivism as "a wide ranging eclectic framework".

To identify where this epistemological paradigm fits in the qualitative research approach, it is necessary to examine the research process itself and then consider how the different paradigms fit within this process. Denzin and Lincoln (1998) have summarized the research process into five phases, which are reproduced in Table 5.

Table 5 The Research Process

Phase 1	**The Researcher as a Multicultural Subject** • History and research traditions • Conceptions of self and the other • Ethics and politics of research
Phase 2	**Theoretical Paradigms and Perspectives** • Positivism, postpositivism • Constructivism • Feminism • Ethnic models • Marxist models • Cultural Studies model
Phase 3	**Research Strategies** • Study design • Case study • Ethnography, participant observation • Phenomenology, ethnomethodology • Grounded theory • Biographical method • Historical method • Action and applied research • Clinical research
Phase 4	**Methods of Collection and Analysis** • Interviewing • Observing • Artifacts, documents and records • Visual methods • Personal experience methods • Data management methods • Computer-assisted analysis • Textual analysis
Phase 5	**The Art of Interpretation and Presentation** • Criteria for judging adequacy • The art of politics of interpretation • Writing as interpretation • Policy analysis • Evaluation traditions • Applied research

Source: Denzin and Lincoln (1998)

Phase two provides the interpretive paradigms that guide the research and Denzin and Lincoln (1998) go on to provide a summary for each paradigm, reproduced in Table 6.

Table 6 Interpretive Paradigms

Paradigm/Theory	Criteria	Form of Theory	Type of Narration
Positivist/postpositivist	Internal, external validity	Logical-deductive, scientific, grounded	Scientific report
Constructivist	Trustworthiness, credibility, transferability, confirmability	Substantive-formal	Interpretive case studies, ethnographic fiction
Feminist	Afrocentric, lived experience, dialogue, caring, accountability, race, class, gender, reflexivity, praxis, emotion, concrete, grounding	Critical, standpoint	Essays, stories, experimental writing
Ethnic	Afrocentric, lived experience, dialogue, caring, accountability, race, class, gender	Standpoint, critical, historical	Essays, fables, dramas
Marxist	Emancipatory theory, falsifiable, dialogical, race, class, gender	Critical, historical, economic	Historical, economic, sociocultural analysis
Cultural Studies	Cultural practices, praxis, social texts, subjectivities	Social criticism	Cultural theory as criticism

Source: Denzin and Lincoln (1998)

This research is seen as being positioned at the boundary of postpositivism. The labels used by Denzin and Lincoln are necessarily broad and research is normally conducted within a predominant paradigm, although there have been calls in case study research for more 'plurality of epistemology' (Otley and Berry 1994).

Other texts provide the researcher with a guide to establishing a suitable posture before embarking on the detailed work ahead. For example, Chenail (2000) attempts to simplify these into the seven C's:

- Curiosity and qualitative methods

- Confirmation and quantitative methods
- Comparison and comparative methods
- Changing and action methods
- Collaborating and collaborative methods
- Critiquing and critical methods
- Combinations and mixed methods

The author recognizes his research posture as one of curiosity in the context of knowing more about the subject, thus further aligning the research strategy to a qualitative approach.

3.2.2 Qualitative Methods

The label, qualitative methods, has no precise meaning in any of the social sciences (Van Maanen 1979). It is at best an umbrella term grounded in the assumption that features in the social environment are constructed as interpretations by individuals and that these interpretations tend to be transitory and situational (Winegardner 1998). According to Denzin and Lincoln (1998 p.3) qualitative research is multi-method in focus, involving an interpretative, naturalistic approach to its subject matter. Eisner (1991) notes the following features of qualitative studies:

1. Qualitative studies are field focused
2. Qualitative studies rely on self as research instrument
3. Qualitative studies are interpretative in character
4. Qualitative studies rely on the use of expressive language and the presence of voice in the text

5. Qualitative studies attend to particulars
6. Qualitative studies become believable and instructive because of their coherence, insight and instrumental ability

Miles and Huberman (1994 p.10) claim that qualitative methods are the best strategy for exploring a new area and developing hypotheses, a point which is particularly pertinent to the area of operational risk mitigation.

Qualitative research is not without its problems. Denzin and Lincoln (1998 p. 6) describe how critics see qualitative research as being unscientific, or only exploratory, or entirely personal and full of bias. Citing Kerlinger (1986), Gable (1994) identifies three major weaknesses of qualitative research : (1) the inability to manipulate independent variables; (2) the risk of improper interpretation; and (3) the lack of power to randomise. A number of authors (Easterby-Smith et al 1991, Miles and Huberman 1994, Yin 1994, Janesick 1998, Gummesson 2000) provide guidance on how disadvantages may be minimized, if not eliminated. Jick (1979) points towards using multi-methods or methodological triangulation as one way of overcoming the inherent problems although he notes that research designs that extensively integrate both fieldwork and survey research are rare. In the risk management field the author noted one previous study (Smallman 1996) where methodological triangulation had been used. This was based on the development of a relationship between risk perception and organisational performance within the Chemical Industry where the population size is large and the opportunity to use questionnaires is, therefore, available. McConnell (1996) also used methodological triangulation in his

study of market risk but this was based on a research model developed in the Information Systems field (Gable 1994) rather than risk management, per se.

Hair (1998) provides a pragmatic attitude towards qualitative research, describing it as the precursor to the quantitative study. The qualitative work develops the model and provides a definition of the concept. The quantitative work can then operationalise the variables and measure adherence to the model. In this scenario both methodologies have an equally important role to play in the development of knowledge. In reflecting on the research that the author undertook, one of the major strengths with a qualitative approach is its openness to opportunistic possibilities that emerge during the period of study. For example, the author was able to witness a change to the risk management structure in one of the banks studied and discuss how this could impact upon operational risk mitigation. In fact, no process changes were noted, only structural, reporting and responsibility arrangements within the Corporate Risk Management Function were affected.

3.2.3 Quantitative Methods

The quantitative approach focuses on measurement, and is of significant help in validating relationships that may exist (Hair 1998) and more importantly direction and strength of causality. Quantitative research uses large sample surveys, or other instruments such as experiments, to gather data and then submits the data to appropriate analysis to prove that the relationship either exists or it doesn't, or the hypothesis is confirmed or otherwise. If the results are to be valid then control of the variables that are being tested is a key issue. In the context of operational risk in UK retail banks, for

example, an appropriate study could have been an investigation into operational risk problems of bank teller operations.

The author recognises that scientific studies, in particular, may be set up in such a way that the desired level of control can be achieved. This level of control, however, may be more difficult to achieve in a business environment, as Gummesson noted (2000 p.91):

> "the research conditions in business are such that conceptualization and the operational definitions used for measurement and observation are rarely subject to the same control as those in the natural sciences".

There has also been a strong preference in social science research toward preserving data integrity, through the use of quantitative research methods, whenever this has been possible (Bonoma 1985). Such research, however, has to start with a prior body of theory in order that appropriate and relevant hypothesis may be tested. Where such a prior body of theory either does not exist or is very limited, as the author has argued for operational risk research, then there is a danger of a "premature application of theory testing in situations where context-preserving theory-building methods might have been more appropriate" (Bonoma 1985).

As with qualitative methods, quantitative methods are not without their critics. Citing Van Maanen (1982), Bonoma (1985) describes the sources of disenchantment with quantitative /deductive tools as being many and notes in particular: the relatively trivial amount of explained variance; the abstract and remote character of key variables; the lack of comparability across studies; the failure to achieve much predictive validity. Gummesson (2000 p.139) talks about how "successful business leaders have always lived

with ambiguity, chaos and complexity" and how "within the positivistic and scientific paradigm, such 'disorder' is a token of weakness, failure and need for further research".

The author does not believe that using quantitative methods for this research study would have necessarily enhanced the reliability and validity of the research findings. Quantitative methods could have been used if operational risk was much better defined and the study population was large enough to warrant the use of questionnaires. According to the BBA (1999b) the number of UK retail banks is quoted as 11 major banking groups with a further 8 smaller ones.

The focus and contribution of this research has been on developing a theory, which described reality with a good fit. A theory that had "predictive usefulness" (Gummesson 200 p.143), and was "user-friendly" (Worren et al 1997). The author believed that achieving this would then provide some new insights into the management and mitigation of operational risk (of use to practitioners), which in turn might serve as an indicator of where further research work was needed (of use to academics).

3.2.4 Case Study Methods

Yin (1994 p.13) defines a case study as "an empirical enquiry that investigates a contemporary phenomenon within its real life context especially when the boundaries between phenomenon and context are clearly not evident". Case study research investigates pre-defined phenomena but does not involve explicit control or manipulation

of variables: the focus is on in-depth understanding of a phenomenon or its context (Cavaye 1996).

Case studies have been described in a number of different ways: exploratory, explanatory and descriptive (Yin 1981); descriptive, illustrative, experimental, exploratory and explanatory (Ryan et al 1992); intrinsic, instrumental and collective (Stake 1995 p.3). These descriptions, whilst helpful in illustrating the type of case study being undertaken, must be preceded by an understanding of the researcher's epistemology. Cavaye (1996) reminds researchers that "case study research can be used in the positivist and interpretivist traditions, for testing or building theory, with a single or multiple case study design, using qualitative or mixed methods". Positivist does not mean quantitative research but implies a qualitative study in which the rigor of design and methodology provide the reliability and the validity (Winegardner 1998). Yin (1994) constructs a case study model from a positivist perspective. An interpretivist approach, on the other hand, rejects the notion of value-free research and is not concerned with the repeatability of an explanation (Darke et al 1998, Cavaye 1996). The interpretivist case study researcher attempts to gain a deep understanding of the phenomena being investigated, and acknowledges their own subjectivity. The value of a particular explanation is judged in terms of the extent to which it allows others to understand the phenomena and makes sense to those being studied (Walsham 1995). Citing Gall et al (1966), Winegardner (1998) notes that the epistemological orientation of most case study researchers is interpretive. Lee (1989) argues that both approaches may in fact be usefully combined

and uses previously published MIS (Management Information Systems) case studies to illustrate his discussion.

Using case studies as a particular research strategy is suggested when the following conditions exist (Yin 1994 p.6):

1. when the form of the research question is how/why;
2. where there is no control over behavioural events;
3. where the focus of the study is on contemporary events.

Benbasat et al (1987) add the following "key characteristics" of case studies:

1. Phenomenon is examined in its natural setting;
2. Data are collected by multiple means;
3. One or few entities (person, group, or organisation) are examined;
4. The complexity of the unit is studied intensively;
5. Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process – the investigator should have a receptive attitude towards exploration;
6. No experimental controls or manipulation are involved;
7. The investigator may not specify the set of independent and dependent variables in advance;
8. The results derived depend heavily on the integrative powers of the investigator;
9. Changes in site selection and data collection methods could take place as the investigator develops new hypothesis;

The author believes that the area of study, operational risk, and the research questions within the study satisfy many of the criteria referred to above.

Case studies may be single or multiple in nature. Multiple-case studies can be used for two purposes – replication and theory development (Ryan et al 1992). Yin (1994 p. 45) describes the evidence arising from multiple cases as "more compelling" and the design is "more robust" although he warns that the decision to undertake multiple case studies cannot be taken lightly because of the time commitment and resource required. Miles and Huberman (1994 p.26) argue that "multiple cases offer the researcher an even deeper understanding of processes and outcomes of cases, the chance to test (not just develop) hypotheses, and a good picture of locally grounded causality". Additionally they consider that multiple case studies "add confidence to findings....they can strengthen the precision, the validity, and the stability of the findings" (p.29).

3.2.5 Case Study Methods in Business Research

A sound methodological positioning can also be based on research that has previously addressed the same field of study. The author has previously alluded to the poverty of any form of theory and, therefore, academic studies in operational risk research within financial services. This suggested that a review of case study research in other areas of business research might provide some guidance in developing the approach. The following list has been drawn from the literature reviewed by the author and represents examples of case study research in the business environment. In the author's view, it

highlights the growing move towards using case studies as a suitable method of study which, when used correctly, can meet the requirements of rigorous academic research:

- Accounting (Oldman 1997, Ryan et al 1992, Humphrey and Scapens 1992)
- Business Ethics (Brigley 1995)
- MIS – Management Information Systems (Darke et al 1998, Cavaye 1996, McConnell 1996, Walsham 1995, Gable 1994, Lee 1989, Benbasat et al 1987)
- Marketing (Bonoma 1985)
- Operations Management (McCutcheon and Meredith 1993)
- Quality Management (Sohal et al 1996)
- Risk Management/Organisational Behaviour (Smallman 1996)

The study of operations management by McCutcheon and Meredith (1993) is probably the closest fit to the area of operational risk. Put simply, operations managers have to manage operations risk, which in turn falls under the umbrella of operational risk. According to McCutcheon and Meredith (1993),

> "Operations management involves complex interplays of people, technological systems, and organisational and physical processes, most of which change in their nature over time"

Operational risk mitigation has been described by the author as "involving a complex series of interactions between people, process and technology" (Blacker 2000). There appears to be a strong similarity. McCutcheon and Meredith (1993) go on to say,

> "Attempting to test theories about this environment requires considerable knowledge about the interactions of important variables.....Adept as we are with theory-testing methodologies that mimic the natural sciences, strict adherence to these techniques may preclude the consideration of methods, such as case study research, that are inherently better for initially developing the theories".

The paper goes on to analyse what they consider to be true Operations Management case studies which have been published in some mainstream Operations Management journals[37]. The results of this analysis are reproduced in Table 7.

Table 7 Breakdown by research intent/methodology among listed cases in Operations Management Journal

Methodology	Research Intent			Totals
	Descriptive	Exploratory	Explanatory	
Pure case	7	33	1	41
Multiple methods	2	3	2	7
Totals	9	36	3	48

Source: McCutcheon and Meredith (1993)

The 'Research Intent' column uses Yin's (1994) terminology as the basis of analysis, thus:

- Descriptive – describe a hitherto unstudied situation
- Exploratory – focus on theory development
- Explanatory – involve hypothesis testing

As can be seen from Table 7, the basis for most of the case studies was exploratory with an emphasis on using a pure case methodology rather than multiple methods to triangulate the results.

3.2.6 Strengths and Weaknesses of Case Studies

Many of the writers on case study methodologies have documented the relative strengths and weaknesses of the approach. The reader is reminded that all forms of research have

[37] Specifically these are the Journal of Operations Management, OMEGA, International Journal of Operations and Production Management, IEEE Transaction on Engineering Management and International Journal of Production Research

limitations (McGrath 1982) and that some of the strengths and weaknesses quoted reflect an argument for or against qualitative research rather than the case study methodology. Table 8 represents a selection of the comments made in the reviewed literature.

Table 8 Strengths and Weaknesses of Case Studies

Analysis of Case Studies	
Strengths	**Weaknesses**
1. Case studies are strong in reality - they are down to earth and attention holding as they report actual behaviour (Buchanan 1999, Cavaye 1996) 2. Case studies are a non-disruptive research method – they are in harmony with the reader's own experience (Buchanan 1999) 3. Case studies recognise the complexity and embeddedness of social truths (Buchanan 1999) 4. Case studies allow for a large number of variables and different aspects of the phenomenon (Cavaye 1996) 5. Case studies are valuable in developing and refining concepts/theories for further study (Cavaye 1996, Ryan et al 1992) 6. Case studies offer the opportunity for a holistic view of a process (Gummesson 2000, Ryan et al 1992) 7. Case studies are of particular value in the applied social sciences where research often aims to provide practitioners with tools (Gummesson 2000)	1. Case studies rely on analytical generalizations (Gummesson 2000, Buchanan 1999, Cavaye 1996, Yin 1994) 2. Case studies can take a long time to complete and result in drowning in the data (Buchanan 1999) 3. Case studies lack statistical reliability (there is always an element of bias) and validity (Gummesson 2000, Cavaye 1996, Hamel et al 1993) 4. Case studies can be used to generate hypotheses but not test them (Gummesson 2000) 5. Case studies represent interpretations of social reality and as such cannot be objective (Ryan et al 1992, Hamel et al 1993) 6. Some case studies, for reasons of confidentiality, have to disguise the identity of the organisation(s) being studied thus limiting an appreciation of the context of the study (Ryan et al 1992) 7. Within-case analysis is essentially intuitive, primitive and unmanageable and may establish relationships between variables but not necessarily the direction of the causation (Miles 1979, Cavaye 1996) 8. Cross-case analysis is even less well formulated than within-site analysis (Miles 1979)

Source: Developed by the author

Many of the texts quoted provide counter arguments to the weaknesses. Gummesson (2000 p. 88 – 97) in particular, provides a robust and detailed defence against the criticisms made. Winegardner (1998) also discusses mitigating factors and counter arguments and in particular points to the use of multiple case studies, which can

"strengthen or broaden the analytic generalizations" as well as "strengthening the precision, validity, and stability of the findings". It behoves upon all researchers to recognise the inherent weaknesses in their approach and then to develop an appropriate research design, which overcomes as fully as possible the shortcomings.

3.3 Research Design for this Study

3.3.1 Research Design

Yin (1994, p 18) defines a research design as the "logic that links the data to be collected (and the conclusions to be drawn) to the initial questions of a study". He points out that there are three elements to consider when determining a research strategy (p 4):

1. The type of research question posed,
2. The extent of control an investigator has over actual behavioural events,
3. The degree of focus on contemporary as opposed to historical events.

The answers to these three questions give an indication of the type of strategy to be adopted in undertaking the research as per Table 9.

Table 9 Relevant Situations for Different Research Strategies

Strategy	Form of research question	Requires control over events	Focuses on contemporary events
Experiment	How, why	Yes	Yes
Survey	Who, what, where, how many, how much	No	Yes
Archival analysis	Who, what, where, how many, how much	No	Yes/No
History	How, why	No	No
Case study	How, why	No	Yes

Source: Yin (1994)

Using this analysis, the strategies suggested for completing this research were case studies and/or surveys.

The author has previously argued that a quantitative approach, such as surveys, would not be appropriate for answering the research questions since operational risk is an ill defined area and there is little prior body of theory from which to develop hypothesis suitable for answering the research questions. This latter point would have made it difficult to know which variables in the mitigation process are "relevant or important and should, therefore, be controlled" (McCutcheon and Meredith 1993).

This does not preclude using surveys after the case studies have been completed and the variables are better understood. Methodological triangulation should enhance the reliability of the results but, as Gable (1994) noted, a factor that must be considered is the "perceived magnitude of the benefits/weaknesses" that integrating case study work and survey methods would bring, particularly in relation to the assessing the quality of the research design. This suggests that methodological triangulation is a judgemental issue, which researchers must be cognisant of throughout the course of the research project and should be taken into account during the development of the research proposal. The initial research proposal for this study noted the possible use of surveys to triangulate the results, but they were not used for the following reasons:

1. It is unlikely that quantitative sampling would have produced a sufficient number of units of analysis due to the embryonic nature of operational risk management in the UK retail banking sector;

2. Identifying appropriate individuals within other UK retail banks who could participate in the survey would have been a difficult exercise due to the diverse nature of operational risk and the number of potential actors involved. A survey of one set of actors, for example, Internal Auditors could have been done but this would have produced biased results;
3. The use of surveys would have had less control over certain key variables, which in turn could have distorted the results. For example, as there is no agreed definition of operational risk the term itself could have been open to misinterpretation;
4. It is unlikely that surveys could have been used to provide examples of critical incidents, one of the key strategies which have been used to support the theoretical propositions concerning operational risk mitigation;
5. The banks selected are major and influential players in the industry. Given this, it is believed that the results from the four case studies are sufficient to answer the research questions and develop a theoretical model for operational risk mitigation.

Exploratory case studies were used as the primary research strategy since the objective was one of theory development rather than description or explanation of events. Case studies are particularly appropriate in developing theory "especially in new topic areas" (Eisenhardt 1989) and "most appropriate when little is known about a topic and where in consequence there can be little reliance on the literature or previous empirical evidence" (Gill and Johnson 1997 p.124). Multiple case studies "add confidence to findings" (Miles

and Huberman 1994 p.29) and help with replication and theory development (Ryan et al 1992).

Gable (1994) notes that practical issues of access, availability of secondary data, budgets, time pressures and the experience of the potential users must also be considered in the research design. Darke et al (1998) point out that the design and scoping of the research project requires a "comprehensive literature analysis to be undertaken in order to understand the existing body of research literature within the research area and to position the research questions within the context of the literature". They also point to other factors that could impact upon the design, including the purpose for which the research was undertaken, the resources available[38] to the researcher and the deliverables required.

The overall design for this study showing the research phases, dates undertaken, processes involved and documentation produced is shown in Table 10.

[38] This research study was funded by the author (which facilitated access) and no other resources were used.

Table 10 Research Design: Phase/Date/Process/Documentation

Phase	Date	Process	Documentation
1. Literature Review	March 1997 – June 1998	Define framework/methodology	Working paper
2. Research Framework	June 1998 – Sept 1998	Define strategy/context/ preliminary model Define questionnaire Identify potential cases	Research Proposal Research Questions Study population
2. Pilot Case Study	Feb 1999 – Sept 1999	Define pilot case study protocol Conduct pilot case study Analyse pilot case data	Case study protocol Pilot case documentation Pilot case results
3. Pilot Case Study Review	Sept 1999 – Dec 1999	Refine questionnaire Refine case study protocol	Research Questions vers 2 Case study protocol vers 2
3. Multiple Case Studies	Jan 2000 – Jan 2001	Conduct case studies Analyse case study data Evaluate results Corroborate findings	Multiple case documentation Multiple case results Multiple case results Multiple case results
4. Model development	Jan 2001	Refine model Develop theory	Revised model Theory documentation
5. Conclusions	Jan 2001 – March 2001	Interpret findings Identify Implications	Study implications (Chap 6) Implications for Further Research (Chap 7)

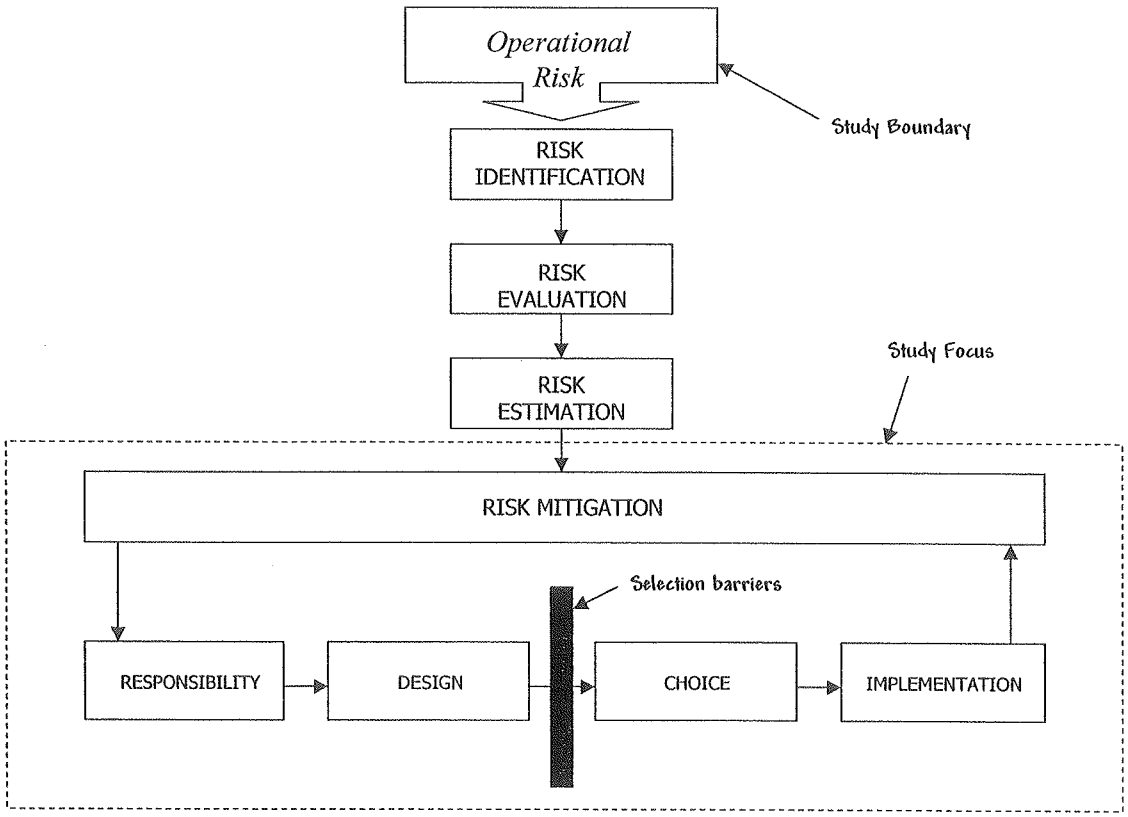
Source: Developed by the author

3.3.2 Preliminary Research Model

Eisenhardt (1989) argues that a research focus is necessary in order to avoid being overwhelmed in data. Otley and Berry (1994) state that "it is incumbent upon researchers using case-based methods to be clear about their initial theoretical propositions" a point supported by Dey (1997) who warns of the dangers of "completely disregarding any existing maps of the ground being explored".

It has been argued that risk mitigation involves making a decision. Decision-making theory has been explored in the literature section of this study and it was decided that an appropriate starting point for this research would be an extension of the risk management model (see figure 9), as applied to operational risk, using the decision making model of Simon (1977) and Nutt (1984). This provided the author with a preliminary model for the risk mitigation process as shown in Figure 16.

Figure 16 Preliminary Risk Mitigation Model



Source: Developed by the author

The four risk mitigation phases are described below:

1. **Responsibility** - who has responsibility for operational risk mitigation (not included in the decision making model)?

2. **Design** - what tactics are employed to mitigate operational risk exposures?
3. **Choice** - what is the process for selecting and implementing risk mitigation actions?
4. **Implementation** - what follow-up (e.g. reporting) is carried out to ensure that the risk has been effectively mitigated?

The basis for extending the model in this way was supported by the literature review.

The researcher will also need to identify the categories or groups of people which, in combination, can provide both a comprehensive picture of the phenomenon under examination, and a variety of perspectives on that phenomenon (McKinnon 1988). The literature review identified those areas with a primary concern for effective operational risk mitigation as being the Risk Management Unit, Internal Audit and Operational Management themselves. The view points of these three groups were considered important because:

1. The Risk Manager's viewpoint - the risk manager plays an integral part in the overall management of risk within the business;
2. The Internal Auditor's viewpoint - the internal auditor has a indirect role in mitigating risks through his examination of the internal control systems;
3. The Operational manager's viewpoint - the operational manager acts as the 'owner' of the processes within which the risks have to be identified and mitigated.

The reason for selecting these groups is that the preliminary model included all of these groups in the 'responsibility' phase of risk mitigation. There are, however, other groups

who it could be argued have a secondary concern for operational risk mitigation, such as external auditors, consultants, outsourcing companies and Regulators. By selecting the primary groups the research data was kept more manageable and the opportunity to triangulate different viewpoints and different disciplines, together with different banks, helped to identify commonalities of approach. Additionally, maintaining an internal bank focus, ensured that stronger controls were achieved over the data since external parties would have approached the problem of mitigation from their own agenda.
Stakeholders with a secondary concern are not directly responsible for operational risk mitigation and the author believes there is scope for future research to be undertaken in this area.

The reporting of risk mitigation actions is less well defined in the literature and the model assumed that there would be some form of reporting so that follow up or tracking could be undertaken to ensure that the (risk mitigation) action is being or, has been, carried out and is working effectively. This assumption was justified on the basis of the authors personal knowledge of reporting systems in banks and more generally, it was considered highly likely that later regulatory pressures (Basle 2001) would require documentary evidence of risk mitigation actions to be available for inspection, for example, audit reports on control improvements and recommended actions. The absence of such reporting could be seen as a weakness in the risk management system.

Another important part of the model is shown as "selection barriers". It was assumed there would be constraints placed on the organisation/functional units/individuals on what

choices can be taken forward to implementation. The author approached the identification of these barriers with knowledge and experience of operating as an Operations Director and used this to probe the interviewees about their views on selection barriers. Within the literature, the risk maturity of the organisation (Hillson 1997) was seen as a possible constraint against selecting a particular course of action.

3.3.3 Critical Incident Techniques

Easterby-Smith et al (1991) describe the use of critical incident techniques as a way of supplementing interviews. The idea behind critical incident techniques is to encourage the manager (unit of analysis) to explain an issue/problem (operational risk incident) in some detail and then to illustrate how the issue/problem was eventually overcome (how it was mitigated). In the context of operational risk mitigation, this could be a useful strategy when exploring the link between the mitigation action selected, i.e. when the decision was made, and the final outcome, i.e. the effectiveness of the action.

The author believes the use of critical incident techniques within the case study approach helped to overcome some of the problems concerned with comparability of data from the basic units of analysis. This comparability arises since risk managers and internal auditors are generally governed by external regulations and professional standards, whereas operational managers in different disciplines can have a wide variety of functional responsibility, vested interests, experience and skills. Support for using 'critical events' is also found in Nutt (1984) who describes how collecting data about such events can "tell stories about organisational processes" and enable patterns in the data to be identified.

Chell (1998) defines a critical interview technique as:

> "a qualitative interview procedure which facilitates the investigation of significant occurrences (events, incidents, processes or issues) identified by the respondent, the way they are managed, and the outcomes in terms of perceived effects. The objective is to gain an understanding of the incident from the perspective of the individual, taking into account cognitive, affective and behavioural elements".

Erlandson et al (1993 p.105) see a critical incident as having the following characteristics

1. It should contain only one event or chief description;
2. It should identify persons, locations and times as specifically as possible;
3. It should either be observed by the writer or be verifiable by more than one source;
4. It should help define the operation of the organisation by focusing on either a typical event or one that is distinctively atypical.

They also counsel (p. 104) against making sure that critical incidents: (1) are not written in judgemental terms and, (2) do not attempt to summarise too much and be too general.

The important point with critical incident interviews is that they probe an event which has already taken place and where it is highly likely that secondary data will be available to confirm who was involved, what did they contribute, what was the eventual outcome and why the course of action was chosen. This technique can be applied to operational risk mitigation incidents, which have already been actioned or are in the course of being actioned. The questions used to discuss the critical incident in this study were part of the case study protocol and can be found in Appendix B.

3.3.4 Quality of the Research Design

Yin (1994 p.33) identifies four common tests for judging the quality of research designs:

1. Construct validity: establishing correct operational measures
2. Internal validity (for explanatory or causal studies only, and not for descriptive or exploratory studies): establishing a causal relationship, whereby certain conditions are shown to lead to other conditions, as distinguished from spurious relationships
3. External validity: establishing the domain to which a study's findings can be generalised
4. Reliability: demonstrating that the operations of a study, such as the data collection procedures can be repeated, with the same results

It has been stated that this research is exploratory and the author was, therefore, concerned with ensuring the research design had construct validity, external validity and reliability. Yin (1994 p.33) provides guidance on tactics that may be used (and the phase within the research process) to ensure such conditions are met. Table 11 provides further details.

Table 11 Case Study Tactics for Four Design Tests

Tests	Case study tactic	Phase of research in which tactic occurs
Construct validity	- use multiple sources of evidence - establish chain of evidence - have key informant review draft case study report	Data collection Data collection Composition
Internal validity (n/a to this study)	- do pattern matching - do explanation building - do time-series analysis	Data analysis Data analysis Data analysis
External validity	- use replication logic in multiple case studies	Research design
Reliability	- use case study protocol - develop case study data base	Data collection Data collection

Source: Yin (1994)

In the context of this research study, the author followed the counselling of Yin (1994 p.33) and employed all the suggested tactics. The use of critical incidents was seen as an effective way of providing evidence about the theoretical territory within which the study

was bounded, thus enhancing construct validity. External validity which indicates that the findings can be generalised from companies in the sample to other companies or industries (Worren et al 1997) is, of course, a matter of degree since no empirical study can offer certainty that its findings are valid for other populations (McCutcheon and Meredith 1993). In this study, however, it is anticipated that the results will be generalisable to other sectors of the UK financial services industry, such as building societies and insurance companies, since their operations are similar and many UK retail banks are known to have insurance subsidiaries. The issue of reliability and, in particular the reliability of interview data, is of concern in any case research. The goal of reliability is to minimise the errors and biases in a study (Yin 1994 p. 36). Yin (1994 p.37) goes on to suggest that a good guideline is to "conduct the research so that an auditor could repeat the procedures and arrive at the same results". The author considers his background in auditing, and the need to develop properly documented audit files, create sufficient evidence to support audit findings and present them in such a way that a verifiable audit trail is created, was of considerable help in satisfying this particular element.

3.4 Selection of Cases for Study

3.4.1 Sampling

The number of cases studies used in the research was four. This number was determined using the following criteria:

- The number of UK retail banks satisfying the criteria, i.e. fell within the definition of a UK retail bank, i.e. large ATM network, use of the cheque clearing system, and so on;

- The inherent difficulties in gaining access and discussing in detail a new area where sensitive information could, an indeed was, disclosed during the probing of critical incidents[39];
- The fact that any further cases studies would have only marginally contributed to a better response to the research questions. If the results from the four selected had been divergent, the 'reserve' banks identified in the case study protocol would have been contacted and further work done;

Hamel et al (1993 p.34) talk about the problem of how many cases are needed. They discuss the emphasis placed on numbers as being important but not "a paramount issue" because "although the number of studies conducted is important, no sociological investigation can be defined on the basis of that issue alone" (p. 35). Darke et al (1998) state that there is no ideal number whilst Eisenhardt (1989) suggests that between four and ten cases are desirable for theory building. This study has used four for the reasons noted above.

Practicalities played an important part in selecting the number of cases studies. There was a need at the outset to identify retail banks that were known to have an operational risk management function. This type of approach is referred to as purposive sampling where the objective is to choose sources that "will help to answer the basic research questions and fit the basic purpose of the study" (Erlandson et al 1993 p.83). Random or representative sampling is not preferred in this type of environment because the researcher's major concern is not to generalise the findings of a study to a broad

[39] The author was made aware of one particular incident which resulted in a hefty regulatory fine and the

population or universe but to "maximise discovery of the heterogeneous patterns and problems that occur in the particular context under study" (Erlandson et al 1993 p.82).

3.4.2 Study Population

Chapter 1, section 1.1 has already described the logic behind selecting UK retail banks as the study population. A UK retail bank has been defined as one which falls under the jurisdiction of the Bank of England, is regulated by the Securities and Futures Authorities, has a large customer base, is a member of the clearing system and has a significant network of branches/ATMs (Bank of England 1983).

UK retail banks represent a homogenous and discrete group although they may differ in terms of size and business focus. They are, however, all regulated by the same body and will, therefore, be required to maintain similar general standards of operation in their business activities, including risk management. Additionally, it was believed they would have similar operational risk problems to manage.

Another element to consider is the bounding of the case study (Otley and Berry 1994) or deciding what is included and what is excluded. Exercising control over the boundaries can be difficult with large organisations, which may themselves contain a number of business units that could, on their own, be bounded as a case study. In the case of UK retail banks, they are known to operate in other market sectors such as insurance (Brown 1992). This study was bounded at the organisational level and not confined to any particular business unit.

---

dismissal of some senior people some six months before it hit the Press

3.4.3 Unit of Analysis

Yin (1994 p. 21) provides detailed guidance on selecting the unit of analysis. He defines the unit of analysis as being "related to the way the initial research questions have been defined". Typical units of analysis include the individual, the organisation or even society itself. The unit of analysis in this study was the manager, i.e. person interviewed, within the bank since it is his interaction with the operational risk mitigation process that was the focus of the study. Whilst this study was concerned with how the organisation mitigates operational risk, it was at the level of the individual that the mitigation action is formulated.

Selecting a function within the banks as the unit of analysis was not possible because the managers selected came from a variety of departments and business units and to restate, the focus of the study was on how the organisation, and not how a certain function(s), mitigates operational risk.

3.4.4 Organisational Secrecy

Benbasat et al (1987) state that two key points to be addressed in order to gain co-operation are confidentiality and benefits to the organisation. The author was aware of the need for confidentiality given the sensitive nature of the subject matter and provided assurance both to the banks involved and the interviewees that their confidence and trust would be respected. The managers interviewed needed to be assured that the information given, particularly when discussing critical incidents, would not affect, for example, the

analysts' views of the banks. Data collected from the critical incidents was in some cases extremely price sensitive.

"Obtaining approval from the companies took a considerable amount of time and effort" according to Sohal et al (1996) in their case study research into quality management. The author knew from the outset that gaining access was one of the major risks of the study. Operational risk incidents within the UK retail banking sector have occurred regularly throughout the course of this study as press reports will attest to (see for example Independent 2/8/2000). Access was gained through a variety of channels following which an initial meeting was set up to discuss the aims and objectives of the research project, who needed to be interviewed and the likely duration of the interviews. The author had made contingency plans if access was not granted and in the event only one bank in the original list of four declined[40] the invitation to participate.

None of the banks or the managers interviewed have been named and no interview quotes have been attributed. Each case study report produced is completely anonymous and each bank is referred to using a Greek letter.

3.5 Limitations of the Research Design

By concentrating on UK Retail Banks, there are a number of biases built into the research. Table 12 documents the possible limitations and illustrates the strategies adopted to mitigate the effect of the limitations.

Table 12 Limitations of the Research Design

Possible Limitation	Comment
1. The results of a single industry study may not be generalisable to other business sectors within financial services or other countries.	The selected banks operate in a number of sectors within financial services and have overseas operations.
2. The selected managers may themselves be biased in their approach to operational risk mitigation and may not necessarily be representative of the bank as a whole.	The semi-structured interview was designed to cover all aspects of the operational risk mitigation process and not just a focus on one area.
3. There may be an element of 'group speak' in the way the managers responded to the interview questions.	This rests to a certain extent on the skill of the interviewer and the need to be vigilant when conducting the interview. The probing of a critical incident pertinent to the manager avoided, in particular, any possibilities of Group speak.
4. The study gives a 'snapshot' of the operational risk mitigation strategic positions at the time the work was carried out.	The study of secondary data enabled a more consistent picture of how the banks arrived at their current operational risk mitigation position.
5. During the period of this study the trend towards amalgamation in the UK banking industry continued (a process which in itself creates operational risk) and the reader should be aware that some of the cases selected were subject to organisational and structural changes.	The author maintained open communication links with the lead contact and discussed any possible effects that the changes had on the mitigation process.
6. There is no clear definition of operational risk and the categories within it.	The opening part of the semi-structured interview focused on establishing whether a definition existed and whether the respondent understood it and agreed with it.
7. The global organisational approach to operational risk management within the bank may not be standardised.	This was discussed before any detailed work began to ensure that the approach was universal or if it was not, then there was an intention to implement the approach across the whole group.
8. There is a possibility that the banks chosen for case study purposes may not provide a good representation of the industry as a whole.	The selected banks were chosen because they are key players in the industry and are likely to represent core emerging practice.
9. The design of the interview questions may reflect the author's personal bias.	The development of the questions was based on the generic risk management framework established from the literature review and was subject to revision after the pilot study.
10. Open-ended questions can be interpreted in different ways and the responses may be prone to exaggeration.	Secondary data is available to support the key responses and data analysis has concentrated on identifying key themes.

Source: Developed by the author

This section has focused on the research options available to the researcher and the actual research design used in this study. Case study methods have been selected as they offer

[40] The invitation was declined because the bank was going through some significant organisational changes including a review of the operational risk management function.

the best opportunity to answer the research questions. The use of case studies was reviewed and appraised and the research design highlights the use of an *a priori* model to guide the work and the focus on critical incidents as a source of data triangulation. The research design was assessed and critiqued and strategies for overcoming the limitations were identified.

4. CASE STUDIES

The previous section has justified the use of case studies as the research methodology and illustrated how the banks were selected. This section discusses the application of the case study approach to this particular study and describes the different processes and techniques that were used. The phases of the approach are well documented in the literature (see for example Yin 1994, Stake 1995) and will be discussed in more detail throughout this section. Finally, the common themes and major differences that were found amongst the banks are presented.

4.1 Cases Studied

4.1.1 Selection Criteria

Yin (1994 p.46) advises that when multiple-case studies are used each case must be carefully selected so that it either (a) predicts similar results (literal replication) or (b) produces contrasting results but for predictable reasons (theoretical replication). Theoretical replication involves selecting cases "because of suspected intrinsic differences between them" (Gummesson 2000 p.95) and will be required to make any general statements about differences and similarities. Yin (1994 p.46) goes on to say that when only a few (two or three) are selected then 'literal replication' or selecting cases so that they are likely to predict similar results, is appropriate. The author, therefore, selected the cases on this basis.

The selection criteria for the sample chosen was based on a number of factors including how well established the bank was, how successful (in terms of profits, reputation, and so on) the bank had been, the information in the public domain about the bank's risk management policies, information in the public domain concerning operational risk problems in the bank and the personal knowledge of the author. It was hoped that by adopting this criteria the selected banks would recognise the relevance of the research to their own organisation thus facilitating access. Researchers should work with organisations and identify "what is in it for them" according to Darke et al (1998). The author hoped from the outset that the research study would be of interest to UK retail banks since operational risk and the development of appropriate methodologies to manage operational risk are of topical interest in this sector of business.

The author has stated that for reasons of organisational secrecy the banks cannot be named. All four banks, however, are large both in terms of asset size, staff numbers and branch network. They all have business units that operate in the retail market, the commercial market, treasury markets and insurance. They all have operations overseas and are involved in joint ventures. The author believes they represent a homogeneous group and were appropriate for 'literal replication' (Yin 1994 p 46).

4.1.2 Managers Interviewed

Erlandson et al (1993 p. 91) discuss the selection of "respondents", when interviews are to be used to collect data, and suggest that they should be chosen "on the basis of what the researcher desires to know and from whose perspective that information is desired".

The author was aware from a literature review (Blacker 1998) that the key actors in operational risk management were the risk management unit, Internal Audit and operations management in the various business units. For each of the banks involved, initial contact was made with the Head of Operational Risk[41]. As part of the project briefing the author indicated that he would like to interview the Head of Operational Risk and a manager from each of the other areas, the objective being to have at least one interviewee from the key actor groups as well as a good spread of people across the bank. The final choice was left with the Head of Operational Risk although the author was alert to the possibilities of 'group speak' during the interviews. Table 13 shows the positions of the people interviewed (generic titles have been used) for each of the banks involved in the study and where in the organisational structure they worked.

[41] This is a generic title and represents the most senior person responsible for the corporate operational risk function

Table 13 Table of managers interviewed

Bank	Person interviewed	Functional Area
Alpha	Head of Operational Risk	Corporate Risk Function
	Director of Risk Management	Corporate Risk Function
	Head of Internal Audit	Corporate Internal Audit Function
	Operations Manager	Treasury Business Unit
	Security Manager	IT Business Unit
Beta	Head of Operational Risk	Corporate Risk Function
	Operational Risk Manager	Treasury Business Unit
	Head of Internal Audit	Corporate Internal Audit Function
	Operations Manager	Retail Banking Business Unit
Gamma	Head of Operational Risk	Corporate Risk Function
	Head of Business Risk	Corporate Risk Function
	Internal Audit Manager	Corporate Internal Audit Function
	Operational Risk Manager	Corporate Banking Business Unit
	Operational Risk Manager	IT Business Unit
Delta	Head of Operational Risk	Corporate Risk Function
	Head of Risk Finance	Corporate Risk Function
	Head of Internal Audit	Corporate Internal Audit Function
	Internal Audit Manager	Treasury Business Unit
	Operational Risk Manager	Finance House Business Unit

Source: Developed by the author

The interviews were held between February 1999 and July 2000, most averaged an hour and were conducted according to the interviewees schedule and availability as suggested by Tellis (1997).

4.2 Case Study Methods

4.2.1 Data Collection

Yin (1994 p.80) lists six sources of evidence (together with their relative strengths and weaknesses):

1. Documentation – such as letters, memorandum, internal reports, press reports, minutes of meetings, or emails
2. Archival records – such as organisational charts, personnel records, internal magazines or internet material
3. Interviews – either open-ended questionnaires or focused
4. Direct observation – by using field visits to the site
5. Participant observation – where the researcher takes an active role in the case
6. Physical artefacts – such as a technological device, a work of art, trophies or photographs

Tellis (1997) considers that "no single source has a complete advantage over the others; rather, they might be complementary and could be used in tandem" and most case studies have one or two sources of data as the primary collection vehicle (Winegardner 1998, citing Merriam 1988). The goal is to obtain a rich set of data surrounding the research issue, as well as capturing the contextual complexity (Benbasat et al 1997) but collecting case study data from case participants can be difficult and time-consuming (Cavaye 1996).

The main data collection source used in this study was an open-ended interview designed to elicit information from the selected managers about operational risk management and, in particular, the mitigation process. Erlandson et al (1993 p.86) describe the open-ended interview as a process where "the researcher and respondent dialogue in a manner that is a mixture of conversation and embedded questions". Open-ended interviews were considered highly appropriate for this study since they enabled face-to-face interaction to

take place, enabling the author, for example, to see how long respondents took to answer a particular question when some 'thinking time' was required (barriers to mitigating operational risk). The author noted the comments of Erlandson et al (1993 p.90) concerning the disadvantages of taped interviews: (1) the respondent is sometimes self-conscious or overly aware of the recorder and (2) the equipment may malfunction. In response, each interviewee was given the option of having the interview taped (none declined) and the author had a spare machine available at all the interviews. Each interview was transcribed and the transcript sent to the interviewee for verification, correction and reflection vis-à-vis the responses given. The author concluded each interview with a statement ensuring that lines of communication remained open (on both sides). In some cases follow-up questions were raised by the author to clarify issues that had been discussed during the interviews.

The questionnaire was developed by the author as part of the case study protocol. It was subject to revision after the pilot case study had been undertaken. The final document is attached as part of the case study protocol in Appendix B. The use of an *a priori* model for the operational risk mitigation process enabled the author to specify the potential variables/factors and discuss them at the interviews. Data can thus be organised in a systematic way which aids subsequent analysis. Secondary data pertinent to the banks was also collected by the author during the field work. Such data includes internal reports, emails, Powerpoint presentations, organisational charts, press reports, annual report and accounts, and articles/papers written by the persons interviewed.

Interviews were also the most appropriate method for collecting data about the critical incidents cited by the managers. Gummesson (2000 p.136) notes that the critical incident technique is a method for coming close to direct observation but avoiding some of the hardships. He goes on to say that "the method allows more incidents, minicases, to be collected than would be possible through direct observation" although the data obtained is coming through an intermediary.

The overall data collection method enabled a good, albeit subjective, level of data triangulation to be achieved in the study, one of the important criteria for construct validity.

4.2.2 Case Study Protocol

Yin (1994) suggests that a detailed case study protocol is "desirable under all circumstances, but is essential if you are using a multiple case study design". Both Yin (1994) and Stake (1995) have developed case study protocols for conducting case study research which they believe enhance the reliability and validity of the investigation. A protocol helps to focus the research and provide a framework within which the case studies may be carried out. A copy of the final case study protocol used for this research is attached as Appendix B.

4.2.3 Pilot Case Study

Yin (1994 p.74) states that a pilot case study "helps investigators to refine their data collection plans with respect to both content of the data and the procedures to be followed". Gable (1994) describes a pilot case study as being "exploratory" enabling

problems and issues to be identified which may point to further investigation. The author believes the objective of a pilot case study is, therefore, to provide the researcher with a solid foundation by confirming that the variables/factors, which relate to the theoretical proposition, are likely to be in tune with the reality of the situation in the field. The research began with a detailed pilot case study, which aimed to confirm this position and provide the author with feedback concerning the development of the final case study protocol. The bank selected for the pilot was chosen on the basis of the author's personal experience in the field and ease of access.

4.2.4 Data Analysis

The interpretation of data is recognised as a critical and difficult phase in qualitative research (McCutcheon and Meredith 1993) and there are some excellent sources of reference available to the researcher to guide him through the process (Coffey and Atkinson 1996, Miles and Huberman 1994, Dey 1993). There is no one kind of qualitative data analysis, but rather a variety of approaches, related to the different perspectives of the researcher (Dey 1993 p.1). Researchers are also advised that successful qualitative research is entirely dependent upon a constant interaction among research design, data collection and data analysis (Coffey and Atkinson 1996 p.193). Robson and Foster (1989 p.94) believe that one of the most important parts of analysis is the "mulling" that takes place of the data and how the "the muddle of information clears into patterns". The author recognises this mulling process as involving an inquisitive, reflective posture, allowing the data to speak for itself, and organising the emerging thoughts into a coherent pattern.

Data analysis is described as "examining, categorising, tabulating, or otherwise recombining the evidence to address the initial proposition" (Yin 1994 p.102) and it is incumbent upon the researcher to develop a general data analysis strategy as part of the case study data design (Yin 1994 Chapter 5).

Prior to the collection of the data, a coding system, based upon the best practice suggested by a number of authors (Slagmulder 1997, Miles and Huberman 1994, Yin 1994), was developed by the author. Coding is defined as "a procedure that disaggregates the data, breaks it down into manageable segments and identifies and names those segments" (Schwandt 1997). The coding system was based upon the preliminary research model and enabled a structured approach to be taken from the beginning of the data analysis. The coding was revised after the pilot case study had been completed. The final version is presented in Appendix B with the case study protocol.

Miles and Huberman (1994 p.10) discuss the analysis of data in three 'flows of activity':

1. **Data reduction** - the process of selecting, focusing, simplifying, abstracting, and transforming the data that is collected during field work,
2. **Data display** - organising, compressing, and assembling the information to permit conclusion drawing and action,
3. **Conclusion drawing and verification** - noting regularities, patterns, explanations, possible configurations, causal flows and propositions.

These three themes are interwoven and provide a well-established framework to undertake a thorough analysis of the captured data. Data analysis under this framework becomes an iterative process.

Computer software, ATLAS/ti[42], was used to facilitate data analysis and provide a repository of the data that could be collected and stored electronically, thus forming part of the case study database. This process is key to ensuring that the data can be interpreted correctly and equally related back to the main and secondary research questions. Once the coding was complete Atlas/ti was used to summarise and order the data so that key themes were displayed and the first tentative conclusions could be highlighted and related back to the theoretical propositions. Each case was examined individually and conclusions drawn (and a case report produced) before cross case analysis was undertaken. Cross case analysis was completed using the data from Atlas/ti to produce case-ordered matrix data displays (Miles and Huberman 1994 p.187) which enables the cases to be ordered by variables of interest.

Buchanan et al (1999) and Gill and Johnson (1997 p.124) warn about "drowning in data" and "being unable to distinguish the most significant variables from those peculiar to a particular case", something which is easy to do when such a variety of data sources exist. How much data to collect and analyse is a judgemental matter which must, *inter alia*, consider how much additional data would help to validate the rigorousness of the research approach and results. The experience and skills of the researcher play an

important part in this process and the author was curious to note the words of McCarthy (1991) cited in Erlandson et al (1993 p. 109) who refers to the term "grokking":

"The term derives from the popular science fiction novel Stranger in a Strange Land, written in the 1960s by Robert Heinlein. The hero of the book, a human born and raised on Mars, returns to Earth with some remarkable powers, including the ability to "grok". As the hero explains, "Grok means to drink...to understand thoroughly..." The term is a metaphor for a profound concept and experience; the ability to understand something completely, to set it in an intuitive, "aha!" way".

The author does not wish to trivialise the matter of data analysis by quoting this source but the words of Erlandson et al (1993 p.109) that follow captured an important innate ability relating to the human psyche, "human beings are born with the ability to "grok", to drink in a vast amount of information and make sense and order of that information". A view that was in fact supported by Miles and Huberman (1994 p.245) who state that "people are meaning-finders; they can very quickly make sense of the most chaotic events". But, as Miles and Huberman (1994 p.245) go on to say, the critical question then becomes "whether the meanings you find in qualitative data are valid, repeatable and right".

4.2.5 Drawing Conclusions

The ability to draw valid conclusions rests in the hands of the researcher and his skills and experience are tested to the full at this stage of the process. Several texts describe the qualities of a good qualitative researcher (Janesick 1998 p.69, Winegardner 1998). The researcher is in fact the research instrument as it is he/she who is at the centre of the research process and who drives the whole effort forward. Miles and Huberman (1994 p.38) based on their many years experience in the field believe that,

---

[42] ATLAS/ti is a computer software package designed to support computer-aided text interpretation and theory building

"a knowledgeable practitioner with conceptual interests and more than one disciplinary perspective is often a better research instrument for qualitative research: more refined, more bias resistant, more economical, quicker to home in on the core processes that hold the case together, and more ecumenical in the search for conceptual meaning".

Whatever the researcher's skill base, there are still a number of issues that must be considered in assessing the quality of the conclusions drawn from the research study. These are described by Miles and Huberman (1994 p. 278) and are related to this study in Table 14.

Table 14 Issues in assessing the quality of the research conclusions

Issue	Method used in the study
Objectivity/Confirmability – the extent of relative neutrality and freedom for researcher bias	1. The general methods and procedures have been fully described and critiqued; 2. The data collection and analysis is fully auditable enabling repetition of the study; 3. There is an audit trail of evidence and research files; 4. The researcher's bias is highlighted.
Reliability/Dependability/Auditability – relates to the issue of quality control over the study	1. The research design is congruent with the research questions; 2. Basic paradigms and beliefs are articulated and related to theory; 3. A monthly supervisory reporting mechanism was established at the outset of the study.
Internal Validity/Credibility/Authenticity – do the findings of the study make sense?	1. Triangulation of data sources produced convergent findings; 2. A multiple-case study strategy used; 3. Findings related back to the literature wherever possible.
External Validity/Transferability/Fittingness – the generalisability of the results	1. The study focused on major retail banks in the UK market; 2. Critical incidents and other published operational risk incidents support the theoretical proposition.
Utilisation/Application/Action Orientation – the pragmatic validity of the results in the research/practitioner's community	1. The study results are important to a number of stakeholders, for example, regulators, shareholders, Board directors and senior managers; 2. Early results of the study have been published; 3. Study findings have been used at various conferences/workshops/consulting assignments; 4. An operational risk mitigation checklist has been developed. 5. A high level audit overview document for reviewing the work of the Operational Risk function has been produced.

Source: Developed by the author (based on Miles and Huberman 1994)

4.3 Case Summaries

The cross-case data analysis identified a number of emerging themes and important differences between the banks. This section summarises the results of this analysis.

4.3.1 Common Themes

The following themes appear to be the most common across the banks:

1. The definitions of operational risk used by the banks are either (two cases) identical to Basle (1998a) or (two cases) very similar to Basle. All the managers interviewed were aware of the definition and had a good understanding of it.
2. All the Corporate Operational Risk units within the banks reported into the Corporate Risk function and had a good working relationship with Internal Audit.
3. All banks used a bespoke risk-mapping framework to manage operational risks although Delta bank was piloting its use in two Business Units at the time the study was undertaken. All banks had some form of key indicators to monitor operational risk exposures.
4. Responsibility for the management of operational risk (all phases) was found to be with the managers in the Business Units, i.e. the operational managers. The broad nature of operational risk meant that they could be helped by specialists when the need arose. The factors that would influence them to seek assistance with mitigating an operational risk were varied but seemed to revolve around the complexity of the risk and the control issue involved.

5. The processes involved in managing operational risk were subjective and judgemental and relied heavily on the skills and experience of the people involved in the processes.
6. The core tactics used to mitigate operational risk appear to be similar in all the banks. The most commonly used tactic emerging from the study is reducing the risk (probability and/or impact) by improving the internal control framework.
7. All banks recognised a number of barriers or constraints in mitigating operational risk. The two which appeared to be the most important for the banks were (1) cost, in the context of cost versus benefit equation and (2) ignorance, meaning the lack of risk awareness of the 'management and staff'.
8. Despite much coverage in the practitioner literature, the quantification of operational risk appears to be some way off in all four banks. Many of the managers questioned the benefits that it would bring to them in their day-to-day work. There appeared, however, to be a recognition by those who will be responsible for quantification (Corporate Operational Risk unit) that this will be the next phase in the evolution of operational risk.

Headlines that have appeared in the practitioner's literature about operational risk such as 'New Frontier' (BBA 1999a) and the 'The Last of the Risk Frontiers' (Withey 1998) testify to the embryonic nature of the subject. It is somewhat surprising, therefore, to find that the frameworks for managing operational risk are so similar. There is no central body providing guidance and a common approach on how to manage operational risk. Indeed, no formal definition of the term operational risk has ever been proposed until the recent

Basle (2001) paper. Equally, all of the bank's operational risk frameworks are aimed at managing rather than measuring operational risk. This is despite a plethora of articles, conferences and regulatory pronouncements that focus on the latter rather than the former. The banks involved in this study have been focusing their attention on implementing a framework to solve the problem of explicitly managing operational risk rather than actively pursuing a measurement strategy which will, in theory, help them to better capital allocation.

4.3.2 Major Differences between the Banks

Despite some commonalities in approach, there were nonetheless some important differences. These have been summarised in Table 15.

Table 15 Major differences between the banks

Area	ALPHA	BETA	GAMMA	DELTA
Operational risk definition				
Exclusions	market, credit	market, credit, strategic	market, credit, strategic	market, credit, possibly strategic
Organisation				
Use of Business Unit ORMs	Developing	Developing[44]	Well-developed	Early days
Other OR risk roles	None	None	Part-time risk officers	None
Operational Risk Committee	No	Part of risk committee	Yes, several	Yes, one
Role of Corporate OR function				
Mitigating OR which span BU	Coordinate effort	Coordinate effort	No	No
OR Unit work with BU ORM	Often	Often	Very often	Developing
OR Unit work with Business Units	Often	Occasionally	Occasionally	Developing
ORM techniques				
Extent of coverage	50% complete[43]	One cycle done[45]	One cycle done[46]	Pilot stage
OR identification and appraisal				
Processes	Mainly formal plus informal	Mainly formal plus informal	Mainly formal	Mainly formal
Impact focus	£: 1 to 5 scale using 6 scenarios	£: figure	£: 1 to 5 scale + Prob > £1m: 1 to 4 scale	£: number ranges + Consequential impact
OR mitigation				
Other tactics	Sharing	-	Exploitation	Sharing Relaxation
Follow-up	Mainly IA tracking system	Informal at Business Unit level IA review where agreed in advance	Tracking system at Business Unit level with review	Informal through IA reviews, KPIs, and personal objectives
Barriers	Various, mainly specific to the bank	Various, mainly specific to the bank	Various, mainly specific to the bank	Various, mainly specific to the bank
Training				
Approach	Formal Framework	Informal Framework	Informal Framework	None
Methods	CRSA Training module			None
Focus	Management and staff	Management	Management	None

Source: Developed by the author

[43] This figure had reached 66% by the end of the study
[44] This had become well-developed by the end of the study
[45] Two cycles had been done by the end of the study
[46] Four cycles had been done by the end of the study

The differences tend to be 'variations on a theme' rather than specific differences in approach, for example, the impact assessment of an operational risk used different scales to measure the financial impact. In some cases it appears that a bank has developed a particular area to a high degree of resilience. For example, the tracking system in Gamma bank seemed to be very robust and offered a high degree of certainty that the agreed mitigation would be implemented.

This section has focused on the case study approach adopted in this study and explained in more detail the approach adopted in collecting and analysing the data. A summary of the data analysis was presented highlighting the common themes and major differences in preparation for the next chapter, which describes in more detail the findings of the study.

5. STUDY FINDINGS

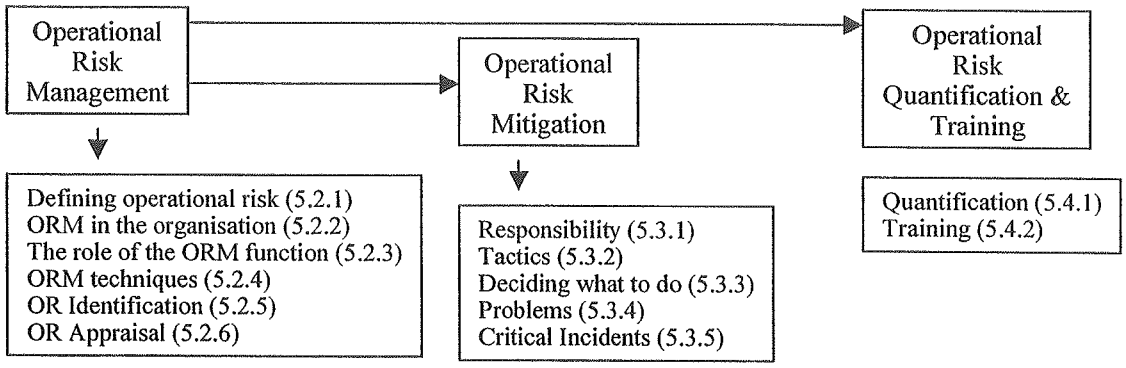
5.1 Introduction

This section provides a summary of the results of the data collected from the case studies. The section is split into fours main parts:

1. Operational risk management (section 5.2) – discusses the findings related to the operational risk environment and the pre-mitigation phases;
2. Operational risk mitigation (section 5.3) – discusses the findings related to the principal research area and provides answers to the related research questions;
3. Operational risk – quantification and training (section 5.4) – discusses the findings related to two areas of operational risk that are important elements of an overall operational risk management strategy;
4. Summary (section 5.5) – provides a summary of the section.

The sequential flow of this section is shown in Figure 17.

Figure 17 Sequential flow of Research Findings



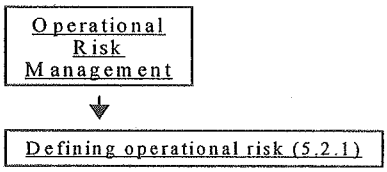
Source: Developed by the author

This diagram provides a roadmap for this important chapter of the thesis and will be constructed at the beginning of each sub-section to help the reader follow the sequence of findings.

The reader should be aware of one important point before examining the rest of the section. Delta bank was implementing its operational risk framework during the time the author was working with them. The author was aware of this when they were chosen and selected them on the basis that they represent a 'newcomer' to the field and would, therefore, bring a different perception to the phenomenon (McKinnon 1988).

5.2 Operational Risk Management

5.2.1 Defining Operational Risk



It has been previously illustrated that operational risk is a broad area encompassing a range of risks that typically fall outside of the market and credit risk areas. This negative definition of operational risk, i.e. any risk other than market and credit, has certainly been adopted by some organisations (Blacker 1998, Withey 1998). The four banks in this study had, however, adopted a positive definition of operational risk. Table 16 illustrates this point and provides further analysis relating to the definition.

Table 16 Definitions of Operational Risk

Definition of Operational Risk	ALPHA	BETA	GAMMA	DELTA
Positive/negative	Positive	Positive	Positive	Positive
Source	Bespoke	Bespoke[47]	Basle	Basle
Types	5	5	11	5
Categories	20	31	44	-
Sub-categories	-	13	-	-
Specific exclusions	market, credit	market, credit, strategic	market, credit, strategic	market, credit, possibly strategic
Level of understanding	Good	Good	Good	Good

Source: Analysis of survey data

The Basle definition used by two of the banks was cited in section 1.1.3 and is re-stated here for completeness:

"The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or external events"

The other two definitions used were:

"Operational risk is the exposure to financial or other damage arising through unforeseen events or failure in the Group's operational processes/systems"

"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."

These definitions are similar, although the two bespoke ones do not explicitly refer to external events as being a source of potential operational risk. Other evidence[48] from these two banks does, however, support the notion that such events are included.

[47] The Basle definition had been adopted by the end of the study

[48] Specifically, Alpha bank has external events on its high level risk schedule and Beta bank has external risks as a type

One Head of Operational Risk described how he has two definitions of operational risk, one which is used from a purely 'measurement perspective' and the other quoted above from a 'responsibility perspective'. This particular Operational Risk Unit is in the process of developing their approach to operational risk quantification (or measurement).

All the managers were aware of their bank's definition and agreed that it describes their own understanding of operational risk. As one interviewee put it:

"It's as good as it can be when you're trying to be succinct about something which is so large".

The results show that all four of the banks break down their definition into types. In some cases categories and sub-categories are also used. This categorisation was used as a means of helping business unit managers to recognise and understand the nature of operational risk, although as one interviewee noted:

"At this stage we're not just concerned with putting badges on the risk. We're just looking closely at what the risks actually are and where those risks may appear in a number of operations across the bank."

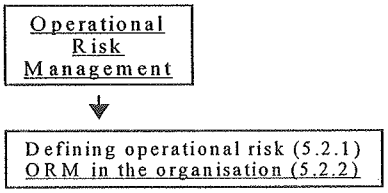
The research found that the inclusion of strategic risk under the umbrella of operational risk was not consistent across the banks. The precise definition of strategic risk was not discussed although it was broadly seen as risks relating to the strategies being adopted by the bank. Delta bank provided the most interesting analysis of this area as the author noted differences of opinion within the organisation. One Delta bank manager believed that strategic risk could feed into operational risk when, for example, a particularly high growth (risky) strategy was being adopted, thus 'creating new risks and affecting the

impact and probabilities of existing ones'. A similar argument was used by another Delta bank manager in the context of environmental risk, which does fall within the definition.

"You could again use a set of words to describe environmental risk in a way that it could be seen as an operational risk, but you could also see it as a credit risk. Because if you've got contaminated land and a commercial loan that goes belly up, people walk away from the site because they've been caught out by the Local Authority and they're facing a remediation bill, that's a credit risk But you can also think of ways that environmental risks can be translated into operational risks."

The findings are consistent with previous observations in the practitioner literature related to defining operational risk: there is no one generally accepted definition and whilst all banks exclude market and credit risk, certain other types, in this case strategic, may or may not be included.

5.2.2 Operational Risk Management in the Organisation



This section examines the organisational arrangements for operational risk within the case studies. Table 17 provides the summarised findings of the analysis.

Table 17 The Operational Risk Management Functions in the Organisation

Organisation	ALPHA	BETA	GAMMA	DELTA
Corporate OR Unit reporting lines	=> Group Risk	=> Group Risk	=> Group Risk	=> Group Risk
Internal Audit reporting lines	=> Group Risk	=> Deputy CEO	=> Group Risk	=> Group Risk
Relationship OR/Internal Audit	Very close	Close	Close	Close
Size of Corporate OR Unit	Small (< 5)	Small (< 5)	Small (< 5)	Small (< 5)
Establishment of OR Unit	1998	1995	1998	1999
Use of Business Unit (BU) ORMs	Developing	Developing[49]	Well developed	Early days
BU ORM reporting lines	Local mgmt	Local mgmt[50]	Local mgmt	Local mgmt[51]
Operational Risk Committee	No	Part of risk committee	Yes, several	Yes, one
Other OR roles	None	None	Part time risk officers	None

Source: Analysis of survey data

The research found that the establishment of a corporate Operational Risk function was a relatively recent phenomenon. One of the units had been established several years ago, two had only just been established when this research study started and one was established during the research study. This finding is important because it confirms the relative 'newness' of explicit operational risk management in UK retail banks and further supports the methodological approach undertaken. Some of the reasons given for the creation of these units were:

"grew out of the need to separate a role which combined operational risk, business continuity planning, corporate insurance risk financing, environmental risk, corporate governance and one or two odd jobs"

"greater recognition that we suffered 'incidents'...that were not credit or market risk by nature"

"provide more of a 'front end focus' to operational risk management, i.e. what could happen to the business if we take this decision?"

[49] This was well developed by the end of the study
[50] Dotted line reporting to the Corporate Operational Risk Unit was introduced towards the end of the study
[51] Dotted line reporting to the Corporate Operational Risk Unit was introduced towards the end of the study

The use of local operational risk managers in the Business Units is at different stages of development in the banks. Gamma bank had fifteen at the time of the interviews, together with some risk officers[52], whilst Delta had two (one of whom was doing the role on a part-time basis) but were in the process of appointing more. None of the local operational risk managers reported into the Corporate Operational Risk function although they had close links and maintained regular contact. All the local operational risk managers interviewed stressed that they were part of the Business Unit:

" (my role is) to facilitate the business units to be able to address operational risk and give them the tools to do it without creating a cottage industry!"

"...prompt, mentor, coach on all matters relating to operational risk (in the Business Unit)"

All of the Corporate Operational Risk Units reported up through the Group Risk line, ultimately to a Group Risk Director. In all but one of the banks the Internal Audit function had a similar reporting line. This is an interesting finding because it leaves open the question as to how the Internal Audit function can independently review the work of the Corporate Operational Risk Unit if they both report into the same executive? The relationship between the Corporate Operational Risk Unit and Internal Audit has been assessed by the author (in subjective terms) and is seen as very close at one bank and close at the other three. Alpha bank, where the relationship was judged to be very close, initially established operational risk as a unit within Internal Audit before separating the two in 1999. This links into to another interesting finding: in all of the banks at least one person working in the area of operational risk had an Internal Audit background. This could have influenced the development of the working relationship, although there were other comments, which indicate a relative proximity of objectives of the two functions:

[52] The risk officer was only part-time in the sense that the individual had other responsibilities

"we (Internal Audit) will begin to use the risk map much more effectively as a tool to assess areas of operational concern, operational risk if you like within the organisation"

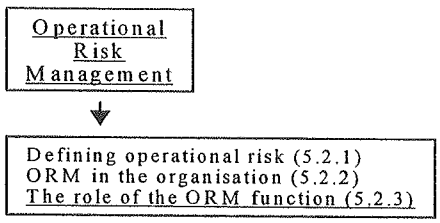
"Operational risk is part of the control framework to help the business to define what its policy towards operational risk should be.....Internal Audit's role is to stand outside of the corporate governance framework and look in at it and actually give an overall level of assurance to the Board at the end of the day that all those things that have been created by management, including that operational risk framework, is actually an effective set of controls"

"It (Internal Audit) is there to be a monitor of the actual implementation of operational risk management policy and the effectiveness of the controls that sit in that environment"

"we meet regularly. I don't think there are any issues. There is always the danger of overlap, but I'm quite clear about the distinction"

The development of Operational Risk committees was, in some cases, more advanced than others; Alpha bank effectively used its Group Executive committee as its Risk Committee; Beta bank had a separate Group Risk committee; Gamma bank had a Group Operational Risk committee and a number of Divisional Operational Risk committees; Delta bank had a Group Operational Risk Committee. It was outside the scope of this research to examine the role and effectiveness of (operational) risk committees and how they may be structured to provide the most effective contribution to the risk management framework. Given the relative 'newness' of the Operational Risk function, it suggests that this is an area that will continue to evolve.

5.2.3 The Role of the Operational Risk Management Function



This section concentrates on the role of the Corporate Operational Risk function. The previous section discussed how the organisation of operational risk management had developed with two specific roles: the corporate operational risk manager and the business unit or local operational risk manager. The early analysis of the data highlighted that whilst both have a role to play in the overall risk management framework, the corporate function was the driver behind the policy and overall strategic direction of operational risk management. The business unit operational risk managers operate at the 'sharp end' and are much more involved in the day-to-day management of operational risk.

The results of the data analysis in this area indicate that there is a reasonable degree of commonality amongst the banks in the general role that the Corporate Operational Risk function undertake (see Table 18). Whilst this might initially seem somewhat surprising given that the creation of these departments is relatively recent, it may reflect the developments that have taken place in other risk (principally market and credit) areas within the bank, which are believed to be more mature. It may also be that managers involved in the establishment of the Operational Risk management function had discussions at an informal level as the generic problems they face in managing operational risk are similar across the banks.

Table 18 Role of the Corporate Operational Risk functions

Role of Corporate OR function	ALPHA	BETA	GAMMA	DELTA
Policy setting	Yes	Yes	Yes	Yes
Monitoring function	Implicit in role	Yes	Yes	Yes
Scope of role	All Op. Risks	All Op. Risks	All Op. Risks	Not environmental[53]
Custodians of the framework	Yes	Yes	Yes	Yes
Assurance on 'key' risks	Yes	Yes	Implicit in role	Yes
Mitigating OR which span BU	Coordinate effort	Coordinate effort	No	No
OR Unit work with BU ORM	Often	Often	Very often	Developing
OR Unit work with Business Units	Often	Often	Occasionally	Developing

Source: Analysis of survey data

A number of managers captured succinctly the role of the function:

"to act as a catalyst, to provide a framework, a process, facilitation, to gain people's appreciation that operational risk exists"

"embedding it (risk management culture) in the business units so they all become much more risk aware on an everyday basis"

"giving these operational risk managers as much guidance and support and general mentoring as to what it is we expect of them, how they should do their work to the best effect, and how they should in turn interact with the business in a positive way and be seen to be helpful and adding value rather than another burden that the business has to bear"

The scope of the role was expected to be operational risks as prescribed in the relevant definition. This was the case in all the banks with the exception of Delta where environmental risks were managed in another area for what appeared to be partly historical reasons (the operational risk function grew out of a unit that originally included environmental risk) and partly because of the emphasis which the bank placed on managing this particular risk.

Different business units have different risk profiles and aggregating these profiles at the group level was done by all of the Group Operational Risk functions. This aggregation of

[53] By the end of the study, environmental risk had been included in the scope of the role

all the risks should provide the clearest vision of where the key operational risks in the organisation may be found. This is an important finding because it illustrates how the Corporate Operational Risk function acts as a conduit between the Board and the Business Units on significant operational risk matters. Their independence from the Business Units enables this to be done in an objective fashion.

The mitigation of operational risks that span Business Units[54] was in two cases managed by the Corporate Operational Risk function. The word 'mitigation' implies co-ordinating effort rather taking direct responsibility for reducing the risk. One manager described it as 'co-ordinating mitigation where it's economic to do that'. The specific responsibility for these types of risks would lie with a specialist area (e.g. IT Security, Insurance) or another Business Unit (e.g. Personnel) and the Corporate Operational Risk function would act as the interface with these other units ensuring that (mitigation) action plans were in place. The other two banks operated a different model: one had other specialist risk areas in Group risk who picked them up; the remaining bank used the hierarchical Business Unit structure to escalate such risks to a level where they could be managed. This is an interesting finding because it highlights specific differences of approach to mitigating operational risks that span Business Units, suggesting that operational risk mitigation has still to mature in some areas.

The interface between the Corporate Operational Risk function and the Business Units also revealed differences of approach. In Gamma bank, very close liaison existed amongst

[54] Examples of such risks include business continuity, misuse of the Internet and loss of key staff

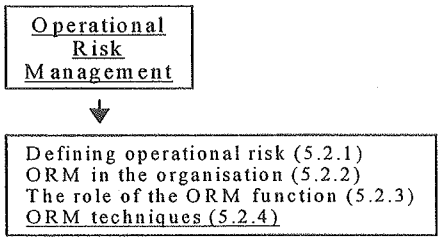
operational risk personnel both at the Corporate and Business Unit level. This has been a deliberate strategy and reflects the needs of the Corporate function to 'work through' the Business Unit operational risk managers if they are to discharge their responsibilities. As Delta bank were piloting the implementation of their operational risk framework, the interface was still developing although evidence seen concerning the roles and responsibilities suggest that they will operate on a similar basis to Alpha and Beta bank.

Evidence drawn from the cases suggests that the core responsibilities of the Corporate Operational Risk function are as follows:

1. Policy – establishing operational risk policy;
2. Aggregation – providing a 'portfolio' view of the operational risks in the group;
3. Reporting – high level reporting of operational risks;
4. Assurance – monitoring levels of operational risk and providing assurance that key operational risks are being managed;
5. Framework – providing the Business Units with the right tools and techniques to manage operational risk;
6. Measurement – developing the techniques for quantifying operational risk

The emergence of operational loss databases (BBA 1999c) occurred during the course of the research. While no written evidence was found to support the notion that the maintenance of these databases will be undertaken by the Corporate Operational Risk function, the discussions with the managers interviewed suggested that this would fall within their remit. This finding is consistent with the description of the roles of the Corporate Operational Risk function that have appeared in the practitioner's literature.

5.2.4 Operational Risk Management Techniques



In all of the banks studied a form of operational risk mapping technique was being used. The end result of the risk mapping process is a 'register of risks' although the objective was seen to be much broader than just this:

"One of the things that obviously we're trying to drive forward with this (risk management framework) is implementing a risk culture. Now that is different to having a risk process. I think what a lot of organisations have traditionally done as far as operational risk is concerned is they have created these centralised units which are staffed up with, don't get me wrong, fairly good and knowledgeable people, but they're divorced from the business"

"To enable businesses to do business according to the terms that they find acceptable. It is not about precluding people from doing business it is enabling them to do business within a safer environment. So if you think of it in terms of walking out into the water they can actually go in deeper and take more risk than they might otherwise have done, but they are ultimately safer than they would have done because they have gone through a conscious process of evaluating and determining what is acceptable and what controls and what is the other criteria they wish to put round it"

"Our (risk-mapping) framework actually covers a number of areas which credit and market risk don't tend to cover, such as research and development, looking at how organisational structures might be out of place, communication on operational risk issues"

The framework was the principal tool used to manage operational risk and was built around the generic risk management process model identified in the literature review. Table 19 provides further analysis of the data.

Table 19 Operational Risk Management techniques

ORM techniques	ALPHA	BETA	GAMMA	DELTA
Framework in place	Yes	Yes	Yes	Pilot stage
Type of approach	Top down and Bottom up	Bottom up	Bottom up	Bottom up
Extent of coverage	50% complete[55]	One cycle done[56]	One cycle done[57]	Pilot stage
Change management projects	Several processes	Framework	Separate process	Framework
Loss Database	Yes	Yes	Yes	No[58]
Key indicators	Yes	Yes	Yes	Yes

Source: Analysis of survey data

Three of the banks use a framework based on a 'bottom up'[59] approach. The exception to this was Alpha bank, whose approach was initially 'top down', as it began with discussions with the Business Unit senior management about the key risks that most concern them in running their operation (identification process). This is followed by workshops with the operations staff to 'determine the residual exposure to key risks' identified by senior management. Any additional risks would also be picked up at this stage. This finding suggests that the starting point may be different but the desired end result is the same. The author undertook further analysis in this area examining the actual data output from the process in order to establish similarities/differences. The results are shown in Table 20.

[55] This figure had reached 66% by the end of the study
[56] Two cycles had been done by the end of the study
[57] Four cycles had been done by the end of the study
[58] Work had begun on this by the end of the study

Table 20 Risk Mapping Frameworks - data output

Framework – data output	ALPHA	BETA	GAMMA	DELTA
Business Unit				
Objectives	No	No	No	Yes
Materiality threshold	No	No	No	Yes
Identification				
Process	No	No	Yes	No
Risk – description	Yes	Yes	No	No
Risk – event/cause	No	No	Yes	Yes
Risk category	Yes	Yes	Yes	Yes
Note on whether risk has been experienced	No	No	Yes	No
Assessment				
Likelihood	Yes	Yes	Yes	Yes
Financial impact	Yes	Yes	Yes	Yes
Consequential impact	Yes	Yes	No	Yes
Mitigation				
Assessment of controls in place	Yes	Yes	Yes	Yes
Indicators to monitor	Yes	Yes	No	Yes
Action plans	Not formal	Not formal	Yes	No
Implementation date	No	Yes	Yes	No

Source: Analysis of primary data documents

Further differences are apparent which indicate that whilst the core process follows the risk management process model, there are matters of detail that differ, doubtless resulting from the different slant or emphasis that a particular bank places on the phase in the process. This finding is interesting because it would appear to demonstrate that banks still have opportunities to refine (and possibly improve) their risk mapping approaches.

A further finding that emerged during the study was the extent to which the risk mapping process had been implemented within the banks (see Table 19). As has been previously mentioned, Delta bank was piloting the process and still had some way to go before the whole bank has been subjected to the framework. Alpha bank had completed around 50% of the bank whilst both Beta and Gamma had done at least one complete cycle.

[59] The term 'bottom up' implies the risk process is driven from the lowest level in the organisation and the

The risk management of significant change projects[60] was covered by all of the banks (see Table 19). Processes were in place to assess project risks some of them being fairly recent developments resulting from the introduction of the operational risk framework.

"We have recognised that there is a need to give a particular focus to that area of business because I think it is an area that has been perhaps not as well recognised or as well identified or as well managed than it has been in the past. But we regard the (project risk) process as very much a subset of the operational risk mapping exercise as a whole"

The final piece of analysis in Table 19 highlights the common use of indicators to monitor operational risk and the use of incident loss databases in all but one of the banks (although Delta bank indicated they would be developing one). Indicators were seen as an important feature in the ongoing monitoring of operational risk. One manager described how the use of such indicators would move managers out of their 'comfort zones' when it came to managing operational risk as they would have to 'be more proactive in taking action when indicators were moving in the wrong direction'. This finding is important because the use of key indicators to monitor operational risk is a key part of preventing the manifestation of operational risk.

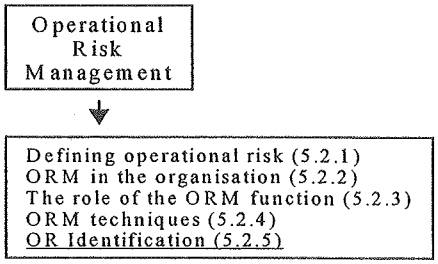
The operational loss database has taken on a new importance since the British Bankers Association invited banks to contribute to an anonymous pooling of data on risk incidents (see BBA 1999c). The findings suggest that the banks view this as an important operational risk management tool.

---

results are filtered up to executive management.

[60] There is no definition of what constitutes a 'significant' project but new product developments was mentioned a number of times

5.2.5 Operational Risk Identification



(Operational) risk identification has been defined as perceiving hazards, identifying failures, recognising adverse consequences (White 1995). It is the first stage in the risk management process. An analysis of the data revealed that the risk identification process can be split into three phases:

1. Responsibility – who is responsible for identifying operational risks?
2. Process – what process(es) are used to identify operational risks?
3. Data – what data sources are used to identify operational risks?

The results of the data analysis are shown in Table 21.

Table 21 Operational Risk Identification: data analysis

Operational Risk Identification	ALPHA	BETA	GAMMA	DELTA
Responsibility	Business Unit	Business Unit	Business Unit	Business Unit
Support	When required	When required	When required	When required
Focus	Management concerns	BU objectives	Management concerns/BU objectives /processes	BU objectives /material events
Instrument	Framework	Framework	Framework	Framework
Process	Workshop IA process Networking Project Develop.	Workshop IA process Networking Project Develop. Internal Forums Questionnaires Software Risk indicators	Workshop IA process Project Develop.	Workshops Meetings Interviews Questionnaires IA process Project Develop. External monitor Strategic plan
Data sources	People	People	People Loss Database	People
Output	List of risks	List of risks	List of risks	List of risks

Source: Analysis of survey data

5.2.5.1 Responsibility

The initial discussions that took place in this area concerned the responsibility for identification and as Table 21 illustrates there was a common view that this responsibility rested with the 'people who manage the processes and systems' or the managers in the Business Unit. One manager pointed out how the framework had been developed in such a way as to highlight who must take responsibility:

"What we're trying to do is say, 'hang on', operational risk is a business unit responsibility. It doesn't matter how you divvy it up within your business unit or who you give it to. That's one of the things we're doing with the methodology"

It was, however, pointed out in all the banks that other units do get involved in their various specialist roles, for example, Internal Audit was seen as key to helping identify operational risk by, 'matching the risks with the systems of internal control and where there are weaknesses reporting them'. This they do as part of their audits of the various

Business Units. This finding supports the view of Basle (2001) and others that the responsibility for operational risk management, and, therefore, identification lies with (operational) managers (within the Business Units). One interviewee pointed out that this responsibility is effectively delegated down from the Board who are ultimately accountable for risk management in the organisation (Turnbull 1999).

5.2.5.2 Process

The process of risk identification does not take place in a vacuum and the results of the analysis indicate that for three of the banks the initial focus is the Business Unit objectives.

"Each business unit is asked during its risk assessment to identify what it feels to be the key risks, the ones that are most important to it in terms of failing to achieve its objectives"

The starting point for Alpha bank was slightly different in that the process begins with a discussion with the directors and senior management in the Business Unit on what they consider to be the 'risks that most concern them'. Materiality emerges as a key word in the risk identification process for all of the banks. 'Trivial risks', as they were referred to by one bank, may be captured but are not seen as the key focus. This is a particularly interesting finding because it illustrates how the processes of identifying and appraising the operational risks are done simultaneously, i.e. managers in identifying their operational risks are also assessing them as 'key' or otherwise. The risk-mapping framework described in section 5.2.4 is used to capture this data.

The processes mentioned by the managers that were used to identify operational risks are quoted in Table 21. The two most common, used in all the banks, are workshops (of operational management) and the internal audit process. The workshops can involve a number of different people including operational managers, operational risk managers, internal auditors and specialists. All the internal auditors interviewed confirmed that they use a risk based audit approach (McNamee 1997, Paul 1994). A number of other processes were mentioned but perhaps the most interesting one (mentioned in two of the banks) is networking, both internally and externally. Whereas the other approaches mentioned tend to be more formal and structured, networking is more informal:

"I wouldn't say it was a structured thing. It definitely works as an informal thing"

"We do rely to an extent on our network of contacts"

Three out of the four banks mentioned the project (or product) development process in the context of operational risk identification. Such a process is seen as key in the Treasury function because of the potential financial impact that an operational risk could have. The only bank where the product development process was not mentioned was Alpha. They do, however, have a well-defined and documented project approach, which includes a risk management activity, and project risk is included within their definition of operational risk.

These findings indicate that a number of core (formal) processes exist to identify operational risks. Other processes mentioned appear to supplement and support the core processes. These formal processes combined with the informal networking processes provide a wide range of opportunities for operational risks to be 'captured' and the fact

that a number of different processes are used supports the argument that operational risk is broad and eclectic in nature.

These findings must also be viewed against the current background of operational risk management, which it has already been confirmed, is still developing in UK retail banks. It may be that as the operational risk management processes mature the focus of operational risk identification will change. At present, the use of (infrequent) workshops, serve to capture any new risks and re-assess any old ones. In future the use of (frequent) monitoring of both potential operational risk sources (to capture any new risks) and key risk indicators to assess existing ones may be sufficient.

5.2.5.3 Data

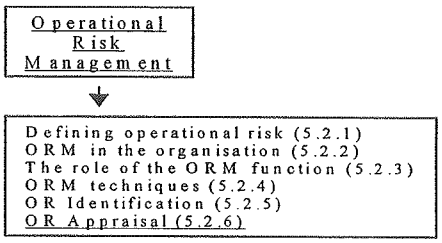
The research found that the main data source used to identify operational risks was the skill and experience of the people involved in the identification process. Where these people are bank employees, they represent probably the most valuable asset that the banks have in both identifying and managing operational risk. One manager pointed out the importance having a 'varied skill base' particularly where the project/product development process was involved in examining a new operational risk situation,

"If you're looking at a fairly mature area, then you probably don't need anything much more than the people who are actually working there who understand the processes, because they will have a good understanding of what they are dealing with. If you're talking about a new venture, then I think it's very different because what we are trying to do is brainstorm what are the things that might be potential risks"

Table 21 also shows that Gamma bank uses its incident loss database as a data source for identifying potential operational risks. The database currently captures only internal

events within the Business Units. These events, however, can be shared across other Business Units to establish whether they have been identified and assessed correctly. This finding illustrates the importance of people in operational risk identification and, as a consequence, the inherent subjectivity that they will bring into the process.

5.2.6 Operational Risk Appraisal



The risk management process model identifies the two phases following identification as evaluation and estimation. These two phases have been defined by White (1995) as:

- Evaluation - estimating the impact of the risk, judging acceptability of the risk, comparing risks against benefits;
- Estimation - estimating risk probabilities, describing the risk, quantifying the risk.

Following the pilot case study it was noted that these two phases were being done concurrently, and not sequentially as suggested in the model. The output from each phase had a different emphasis with one focusing on at least financial impact (evaluation) and the other on probabilities (estimation) but the two were combined to give an overall risk profile/rating/definition/report. The author has, therefore, grouped these two phases together and referred to it as 'risk appraisal'.

As with operational risk identification, an analysis of the data revealed that the risk appraisal process can be split into three phases:

1. Responsibility – who is responsible for appraising operational risks?
2. Process – what process(es) are used to appraise operational risks?
3. Data – what data sources are used to appraise operational risks?

The results of the data analysis are shown in Table 22.

Table 22 Operational Risk Appraisal: data analysis

Operational Risk Appraisal	ALPHA	BETA	GAMMA	DELTA
Responsibility	Business Unit	Business Unit Corporate OR	Business Unit OR (healthcheck)	Business Unit
Support Instrument Process	When required Framework Workshop	When required Framework Workshop IA process (challenge)	When required Framework Workshop IA process (challenge) OR healthcheck	When required Framework Workshop
Likelihood focus Impact focus	Prob: 1 to 5 scale £: 1 to 5 scale using 6 scenarios	Prob: % £: figure	Prob: 1 to 5 scale £: 1 to 6 scale + Prob > £1m: 1 to 4 scale	Prob: 1 to 6 scale £: number ranges + Consequential impact
Data sources	People Current mitigation External environ. Historical data	People Current mitigation Historical data Capital	People Current mitigation Loss Database Risk indicators	People Current mitigation Performance indicators
Output	BU Risk profile Risk measure	Risk rating	Risk definition and risk rating on a scale of 1 to 8	Risk report

Source: Analysis of survey data

5.2.6.1 Responsibility

The results in Table 22 show that the responsibility for operational risk appraisal mirrors that of operational risk identification. The managers in the Business Unit have responsibility for appraising operational risks although they may be aided by specialist resource when the situation demands. One manager in Beta bank, however, pointed out that in his view, Business Unit managers had a "lesser responsibility" and were

influenced by the Corporate Operational Risk unit who acted as 'facilitators to this process using the standards and parameters (for appraising operational risk) that are agreed by the Board':

"...this is where I see the Operational Risk Group has helped to facilitate that (operational risk appraisal). Just as the Market Risk Group facilitates Value at Risk and The Credit Risk Group tries to somehow put a number on credit risk. But it's more difficult for operational risk and I've got a lot of sympathy for that"

This finding probably reflects the framework within which the Business Units are 'obliged' to operate, although a manager in one of the other banks (Delta) considered that there was still some way to go in terms of ensuring the Business Units clearly understood their responsibility:

"You'll find sometimes that they (the business unit managers) consider that group (Corporate Operational Risk Unit) has responsibility for some of these things when in truth they don't, because group can't, because you need the business knowledge to know what your level of exposure is to know the level of mitigation you need."

To further reinforce the role that the Corporate Operational Risk Unit play in this area, within Gamma bank they have specific responsibility for performing a 'health check' on the results and running 'a slide rule across it for any nonsenses or apparent contradictions'.

The findings in this area suggest that whilst the primary responsibility appears to be well articulated, the Corporate Operational Risk unit are more 'influential' in the results that are produced. This may be a reflection of the subjective and judgemental nature of the

appraisal process (discussed in the next section) and the need to have some form of control over the results.

5.2.6.2 Process

"There are some gradings there on the risk assessment form that we have and then we also ask them to assess what the likelihood of the risk occurring at that level would be, again bandings from very low up to very high. And using the combination of those two factors we then produce a risk rating on that. It's basically a matrix, a two dimensional matrix, with the intention of giving the likelihood and the potential financial impact as a rating from one to eight of how crucial that risk is if you like"

In all of the banks the process used to appraise operational risks involved a subjective/judgemental assessment of the probability and impact of the risk, primarily through the workshops. As can be seen in Table 22 each of the banks had developed a simple grading system from which an appraisal rating may be made. The probability assessment was straightforward being either on a scale, for three of the banks, or a % figure for the remaining bank. The impact assessment varied quite considerably with the simplest being Beta bank where a £ figure was allocated to Alpha bank where a 1 to 5 scale was used within six different scenarios covering financial, media, regulatory, customer, shareholder, problem management.

The emphasis on estimating a financial impact was summed up in the following comment from one of the managers:

"... we will try and encourage people to put a financial impact on because I think that is, especially in banking, that is the only thing that still really gets people interested"

But the problems in doing this were equally recognised:

"The difficult thing for operational risk is it's still quite a new discipline and it probably doesn't really have off-the-shelf packages that you can quickly assimilate that. It's probably as much an art as a science".

Delta bank saw the output from the risk appraisal process as being an important way of making sure that managers in the Business Units were focusing their priorities in the right areas and avoiding them to concentrate on areas where they may have a particular interest or areas which they understand well and were, therefore, happy to manage. This is an important point and highlights the emphasis that needs to be placed on scaling so that the risks and the Business Unit themselves can be judged and compared in relative rather than absolute terms.

In some cases, the role of Internal Audit independently reviewing and challenging the appraisal ratings that had been established, was identified. Internal Audit would normally leave the area with an agreed audit report, which may necessitate changes to the risk map for that particular Business Unit or area within a Business Unit. This finding is important because it serves to reinforce the role of Internal Audit as the 'Board's guardians' of the operational risk management framework.

The analysis of the data in the risk appraisal process, whilst revealing some consistent patterns, also illustrates the importance of controlling the resultant output to ensure that consistent and meaningful conclusions can be drawn from what is an inherently subjective process. This will remain a constant challenge for banks if they are to ensure that they have correctly identified their 'key' risks.

5.2.6.3 Data

The research found that the principal source of data used in the risk appraisal process was the experience of those involved in the process (see Table 22):

"It's just a case of sitting down with the right people and trying to get out of them the knowledge they have in their head"

Where workshops are used, the risk appraisal would typically have a number of different levels of personnel present to ensure a broad perspective was gained. This would help to remove 'appraisal bias':

"The people who know the nuts and bolts are typically fairly junior but they don't know enough about the big picture to make that kind of assessment. And people that know about the big picture may have lost touch with some of the nuts and bolts"

"One of the things we have recognised is really making sure we get the right people at the workshop. If you get people who are too low down the management hierarchy then they don't necessarily see the bigger picture of bringing these things together. Yes, we've found we have had to put the groups together quite carefully"

This finding reinforces the subjective and judgemental nature of operational risk management, vis-à-vis, both identification and appraisal.

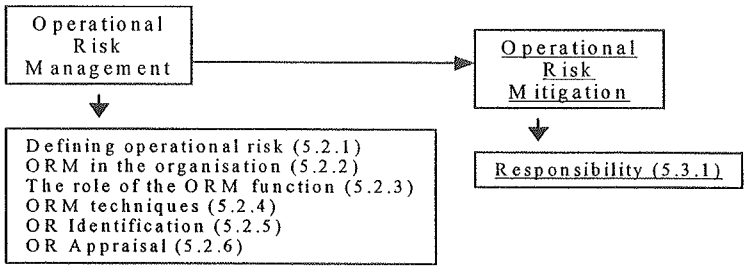
A further interesting finding of the study relates to the assessment of current operational risk mitigants as a source of data for appraising an operational risk exposure. Current mitigants are normally documented at this stage in the risk-mapping process and an overall view is taken on the impact and probability. This is not necessarily the end of the story, however, as other data sources are included (see Table 22) which in aggregate aid the development of a more 'robust' appraisal of the operational risk. The external environment data source cited in Alpha bank is an interesting example involving 'keeping

an eye on what is going on'. Events of this nature can have important influences on the operational risks faced by a bank and could easily affect the appraisal rating in terms of either impact or probability. Such events can occur in a variety of places, for example, regulatory pronouncements, changes to legislation, technology issues and product developments. External events are recognised as a potential source of operational risk in the Basle definition (2001) and banks must ensure that they figure prominently in their risk appraisal data.

The output from this part of the process involves summarising the data on the identified risks together with their appraisal ratings thereby producing a total picture of the overall (operational) riskiness of the Business Unit or area within a Business Unit. These are referred to in different ways by the banks but in essence they equate to the same thing. An example of an individual operational risk assessment form used to capture all the data can be found in Appendix C.

5.3 Operational Risk Mitigation

5.3.1 Responsibility for Operational Risk Mitigation



The first set of questions that this research set out to explore were:

- *Who is responsible for operational risk mitigation?*
- *If more than one functional unit has responsibility, on what basis is the operational risk exposure assigned to the unit concerned?*

There emerged a consistent pattern with the previous sections in terms of responsibility for operational risk mitigation, namely, it remains with the managers of the Business Unit. This can be seen in Table 23, which shows the results of the data analysis.

Table 23 Operational Risk Mitigation responsibility: data analysis

Mitigation - Responsibility	ALPHA	BETA	GAMMA	DELTA
Responsibility Support Factors influencing support	Business Unit When required Control issue Option to share risk Complexity of risk	Business Unit When required Cost effective Control issue Potential impact BU skills lacking Complexity of risk	Business Unit When required Control issue Best practice sought Complexity of risk	Business Unit When required Scale of risk Type of risk Control issue Internal skills lacking

Source: Analysis of survey data

Comments from the managers interviewed did, however, indicate that the managers of the Business Unit would be supported in their mitigation responsibilities:

"who can best assess the value of the mitigant?"

"draw on certain reservoirs of expertise"

"use as many people as you can!"

"there are quite a lot of specialist areas that you can go to"

Table 23 also identifies the factors that would influence the managers in the Business Unit to seek support. The complexity (type/scale) of the risk is a common element mentioned in all four of the banks. This is not surprising given the range of potential operational risks that exist. For example, the introduction of a control to improve the segregation of duties in a process is a relatively simple exercise to undertake. At the other

end of the scale would be the operational risk(s) associated with the introduction of the single European currency, where a number of people would be involved and a project team would probably be set up. As the Business Unit are responsible for mitigating the risk, it is they who would initiate the call for assistance. Such assistance could come from a variety of sources:

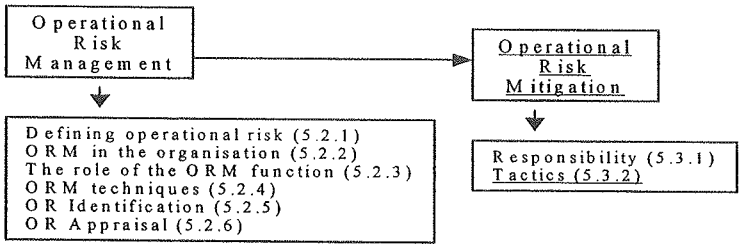
"Sometimes external consultants can act as the catalyst to get the change (mitigating action) in place"

"Sometimes even just asking from the technology side 'look have you got a package that could help'"

"I would certainly encourage managers to approach Internal Audit if they are making major changes to what they are doing in the business. To discuss some of those ramifications on their control framework"

Returning to the research questions, the findings suggest that it is the Business Unit that have sole responsibility for operational risk mitigation. As a result, the assignment of operational risks to different functions is not carried out, although there is evidence to indicate that the Business Units will seek assistance to mitigate an operational risk depending upon the nature and scale of the risk involved.

5.3.2 Operational Risk Mitigation – exploring the tactics used



The second set of questions that this research set out to explore were:

- *What tactics are considered before being used to mitigate operational risk exposures?*
- *How are these tactics established?*
- *What commonality exists across banks in their risk mitigation tactics, i.e. what may be viewed as "core" practice?*

At this stage in the operational risk management process the managers in the Business Unit should already have identified the operational risks and appraised them by assessing, inter alia, the current mitigants (if any) that are already in place. The dilemma that the managers in the Business Unit face is deciding what, if anything, to do to further to reduce the current level (probability/impact) of risk to something which is more acceptable.

"it's not a case of everything requires additional control. In fact there is a very fine balancing act that is being constantly addressed"

Table 24 shows the results of the data analysis.

Table 24 Operational Risk Mitigation tactics: data analysis

Mitigation - Tactics[61]	ALPHA	BETA	GAMMA	DELTA
Terminate	Yes -	Yes New product trade	Yes Leading edge tech. Critical supplier	Yes Strategic Temporary avoid
Treat	Yes Process improve New technology Tightening rules Contingency plans Rulebooks	Yes Seg. of duties Automating checks Process improve New technology Good controls	Yes Process improve Training Procedure guidelines Exception reports	Yes Internal control framework
Take	Yes Outside business Barrier present	Yes Cost/benefit	Yes Cost/benefit Pass on cost	Yes Cost/benefit Potential size
Transfer	Yes Insurance	Yes Insurance	Yes Insurance Outsourcing Internal transfer	Yes Insurance Internal transfer
Other	Sharing cited	-	Exploitation	Sharing Relaxation

Source: Analysis of survey data

The mitigation tactics shown equate to those of Horrigan (1967) thus:

- Terminate: Avoidance – decide that the risk is too great to follow the course of action
- Treat: Reduction – decide to reduce the probability and/or impact
- Take: Assumption – decide to accept the risk and do nothing further
- Transfer: Transfer – decide to transfer the risk to a third party
- Sharing: Combination – decide to share the risk with another (internal/external) party

Horrigan (1967) did, however, propose another mitigation strategy, namely 'Hedging', which involves reducing risk through the operation of future markets.

All of the banks use the four T's as mitigation tactics and Table 24 identifies when a particular tactic is used. The following comments are illustrative of some of the scenarios described:

[61] The reader will note that the tactics all begin with the letter T. One of the managers interviewed introduced the four T's to the author and because of its simplicity, these words have been used throughout the rest of the text

Terminate

"It would be more of a strategic issue but if you looked at two of our more recent disposals..... both of which you might say would be high in operational risk and, therefore, perhaps there was a factor in that"

"...there are major impacts across the whole of the operational risk review because if you move to that type of scenario, it actually changes the materiality of a lot of your operations and how they are controlled and mitigated. So, yes there are times when the risk may be so high that the trigger is we actually don't want to do this"

Treat

"Controls have to be viewed in the wider context of what is it that is absolutely essential to achieve a certain outcome as opposed to that which is nice to have but really perhaps doesn't justify the cost"

"...can we segregate things better, can we move things into other areas, can we add an automated check, do we need a visual check"

Take

"One of the key risks...is that all of the banks rely on a central payments processing system run by SWIFT. SWIFT is a single point of failure. They have their own mitigations, but if you were to take it to its extreme, you would look at avoiding SWIFT and having in place some contingency routing mechanism for payments. Some banks are starting to do this, others aren't"

"Let's take for instance, IT security. You're always going to have people who can have access to every part of your system. There is no computer system that has been built that can remove that risk. Therefore, you have to accept that risk to some extent"

Transfer

"if you can't offset it, you have to guard against financial loss. You may take out some sort of insurance"

"Can I get assistance from anywhere in the business to help with any of that? Part of I suppose bundling the risk up, we're not necessarily talking about insuring the risk internally, but are there internal areas of the business who can help me with this? Can I outsource it to another area of the business because they have expertise in that area? That's certainly looked at".

These findings indicate that the tactics that may be used to mitigate an operational risk are in line with those quoted in the literature. The treat option was the most oft quoted (a point also confirmed by the critical incident analysis – see section 5.3.5) and this finding

confirms the view of Basle (1998b) that operational risk is principally addressed through a firm's internal control framework.

An interesting issue raised in Delta bank relates to the overall level of controls in a given risk situation compared to the appraisal of the risk.

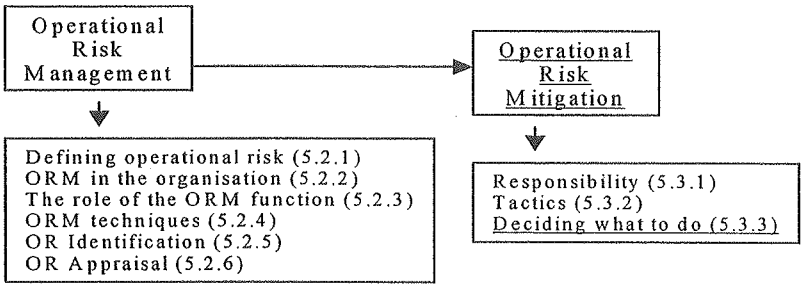
"Where something is a low priority, and it looks like you're controlling it to death, I would like to think the Business Areas will begin to strip out some of the unnecessary layers of control, which I think a big organisation like this has built up over history and controls get layered on top of each other without really questioning why they're being done"

The author has referred to this as 'risk relaxation' as the objective is to reduce rather than increase the number of controls (Kinsella 1995b). This is an important finding as it demonstrates how the operational risk mapping process may be used as a tool to enhance the overall efficiency of the internal control processes in operation.

The final tactic noted by one respondent in Gamma bank was exploitation of the operational risks. The specific example quoted was in using leading edge technology where the bank may evaluate that the business benefit outweighs the operational and strategic risks involved. This tactic is the other side of the coin to risk avoidance and illustrates the positive side of risk taking.

Returning to the research questions, the findings indicate that there are a number of tactics available to the banks in mitigating operational risks, although the core tactics may be represented by the four T's, with the treat option being the most commonly used. These tactics have been established as part of the development of the risk-mapping framework and are based on those found in both the practitioner and academic literature.

5.3.3 Operational Risk Mitigation – deciding what to do



The third set of questions that this research set out to explore were:

- *What is the process used for deciding upon the risk mitigation strategy to adopt?*
- *What is the process used to ensure that the risk mitigation decisions are adequately communicated and reported?*

The focus of the discussions in this area of operational risk mitigation was on who decides the mitigation tactic to employ, what is the process used for selecting and implementing the tactic and what follow-up procedures are used to track the efficacy of the action taken. Consistent with previous phases of the risk management process, the decision maker was for the most part the Business Unit (see Table 25). This caveat arises because it would ultimately depend upon a number of factors relating to the risk and the authority of the manager in the Business Unit:

"the scale of what is being decided"

"for significant issues the Risk Management Committee would be involved"

"within discretionary levels of expenditure".

"anything which is going to involve a project going into £1 million will go up the line"

Table 25 Operational Risk Mitigation selection procedures and follow-up: data analysis

Mitigation – Selection Procedures and Follow-up	ALPHA	BETA	GAMMA	DELTA
Decision maker	Mainly Business Unit	Mainly Business Unit	Mainly Business Unit	Mainly Business Unit
Factors	Proposed tactic Scale of risk Cost of action Approval limits	Scale of risk Level of change Technology impact Customer impact Cost benefit	Scale of risk Resource needs Cost benefit	Scale of risk Cost benefit
Selection process	Informal	Informal	Informal	Informal
Factors	Nature of risk Priorities Amount of work Others involved	Nature of risk Current controls IA tracking	Nature of risk Current controls Previous action	Nature of risk Current controls
Follow up	Mainly IA tracking system	Informal at Business Unit level IA review where agreed in advance	Tracking system at Business Unit level with review	Informal through IA reviews, KPIs, and personal objectives

Source: Analysis of survey data

An escalation procedure existed in the banks when the Business Unit could not unilaterally decide on the course of action. This escalation procedure was linked to a number of factors (see Table 25), which appeared to be well understood in the banks. The scale of the risk was a common factor as was cost, i.e. the estimated amount required to mitigate the risk. Where a cost was involved in taking appropriate mitigating action (normally for 'Treat' as per Table 24) then a cost/benefit justification would normally be prepared. This finding is interesting because it illustrates the constraints that managers face in mitigating *their* operational risks. These constraints are imposed upon them by the internal environment (policies and rules) of the bank in which they operate and will vary from bank to bank. A tight command control structure will impose different and more severe constraints to a less formal empowerment regime. This issue can be extended further to take into account the manager's own perception of the risk (in terms of what can be done to mitigate the risk down to an acceptable level). Where a tight command

control structure exists this perception is of less relevance than in an empowerment regime where managers are able to exercise more personal discretion.

None of the banks had a system of formal procedures for selecting a particular mitigating action (see Table 25). The nature of the operational risk being mitigated combined with the appraisal that has previously been carried out will normally determine by 'default' the mitigation action that needs to be taken. The 'pecking order' usually began with an examination of the internal control environment:

"In practice, I would say if you took any risk issue the first thing is to look at the level of controls you have around that and if you can improve your internal controls that generally is the most cost effective mechanism"

This finding confirms the comments of Basle (1998b) that most operational risks are managed within the internal control environment.

The final phase in the risk mitigation process that emerged from the data analysis was the follow up action that was in place to ensure that the mitigation tactic/action plan was being implemented. There was little consistency across the banks in this area (see table 25). Internal Audit involvement was mentioned in three banks but this was not 'systematic' and linked to the action plan but as part of normal audit procedures. The evidence in Gamma bank indicated that it had a structured approach:

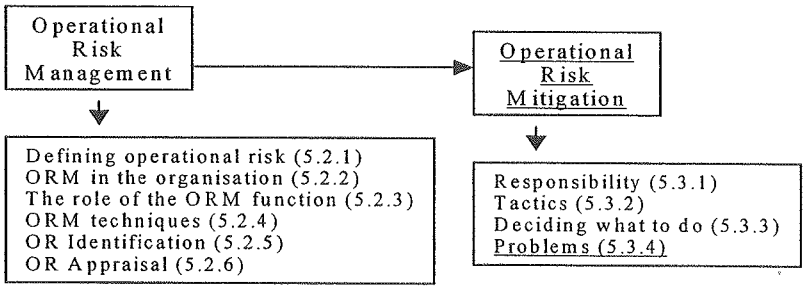
"we also have a record of all the action plans in place, besides all the risks, which we keep on our central database. So that, every quarter currently, we ask for a re-visit exercise, to go back and see what's happening with the action plans, has it been implemented, has it lapsed, is it no longer relevant, etc. to give a status report on how they are going about it"

At the time of the interviews, 86% of the action plans in Gamma bank had been implemented and the controls were in place, roughly 4% had lapsed and the other 10%

hadn't yet been implemented. This finding is important because it suggests that, with the exception of Gamma bank, effective follow-up procedures may not yet be in place to monitor actions to mitigate operational risks, thus leaving the other banks with possible exposures.

Returning to the research questions, the findings indicate that the process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved. The follow-up process, however, is in most banks less structured and could have some important implications in the effective mitigation of operational risk.

5.3.4 Operational Risk Mitigation – the problems faced by management



The fourth set of questions that this research set out to explore were:

- *What are the major barriers to implementing operational risk mitigation actions?*

The results of the data analysis in this area can be found in Table 26.

Table 26 Operational Risk Mitigation barriers: data analysis

Mitigation - Barriers	ALPHA	BETA	GAMMA	DELTA
Main barriers	Cost and resource Inertia No solution Ignorance Organisation	Cost System fragilities Inertia Commercial pressures Customer reaction Ignorance Establish priorities	Cost Change management Timescales Resources Risk Appetite Ignorance	Cost Changing business environment Time Ignorance
Also noted	Politics	-	-	-
Related matters	-	-	Budget constraints	-

Source: Analysis of survey data

The research found that cost (or more precisely cost versus benefits not being justified) linked to budget constraints (in the case of Gamma bank) was a common theme. Additionally, 'ignorance' was mentioned as a barrier in all the banks:

"lack of risk awareness"

"lack of understanding of risk in the particular environment"

"ignorance of how particular risk mitigation techniques may be implemented"

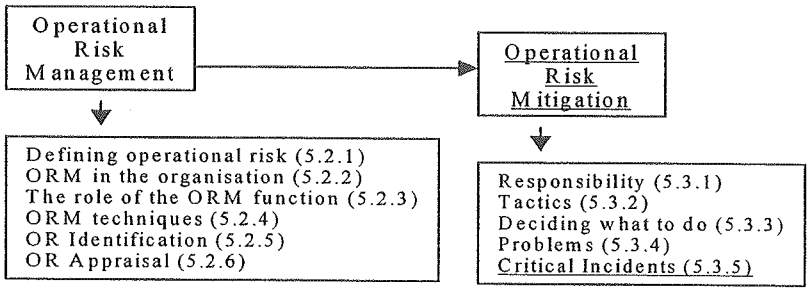
Table 26 illustrates the other barriers that were identified by the managers. The fact that there are a number is probably indicative of the broad nature of operational risk. From a mitigation point of view, this suggests that operational risk can be adversely influenced by a whole range of factors. The risk appetite mentioned at Gamma bank was particularly interesting:

"I think something in the Corporate arena that is interesting is the actual appetite for risk is not clear in some cases. It may be clear to the strategic thinkers at the Centre, and they may have a good idea, but it's not that helpful to the practitioners if they are not aware what the appetite is for accepting operational risk."

The findings related to the research question are important because they identify the types of problems that managers face in mitigating operational risk. The decision as to how to mitigate a particular operational risk will have to take due cognisance of the barriers or constraints that exist within the organisation. Business Units will have different needs in

terms of risk mitigation based upon their inherent risk profile. There is no 'one size fits all' way to mitigate operational risk and the interplay of the various 'actors and factors' involved is an area where further developments will be required if the organisation is to 'guarantee' its level of residual risk.

5.3.5 Operational Risk Mitigation – critical incidents



Critical incidents were used during the course of the interviews as part of the data triangulation strategy for the study. They provide data that can be used to either support or reject the theoretical propositions concerning operational risk mitigation. An analysis of the incidents discussed can be found in Appendix D and further details of the individual incidents may be found in the individual case study reports for each of the banks. The author has selected four from those listed to illustrate the problems that managers face in dealing with operational risk incidents (NB. The incident number refers to Appendix D)

Incident No. 5 - Book of transactions transferred

A book of outstanding transactions was transferred from one Business Unit to another (following an acquisition by the bank). The Business Unit that had taken over the book discovered that the record keeping of the original Business Unit was "not great" and, as a result, errors in the trades were appearing. This situation is still ongoing and the challenge

for the bank, now that the risk has been identified, is to assess whether the amount of work involved in totally mitigating the risk is cost effective and worth the effort involved. As the manager put it:

"We're weighing up at the moment does the risk warrant the manual effort to go back in and review every one of those thousands of trades and go through them all again in detail and highlight whether any of them have been mis-booked. That is an issue on my desk today, I have asked how many trades are there? How long would it take to do it? Or do we accept that we should have some reserve for occasional losses which might occur"

This comment reflects the need to put some form of measure on the risk before deciding how to mitigate it. The two possible tactics being considered by the Business Unit are "Take" - accept that there are errors and live with them – and "Treat" –check all the deals and remove those that have been mis-booked. This incident supports the findings concerning the need to assess the scale of the risk and the remedial cost before deciding the appropriate course of action.

Incident No. 9 – Uncleared effects

This type of fraud is understood to be quite common in Retail banks and involves customers attempting to draw on cheques, which have not yet cleared through the clearing system. As such, it is a well-known risk, which has always existed:

"It's always been a part of our training, part of our processes to check. Historically we've known what the losses are, but they've been accepted by management".

The last sentence indicates that the mitigation tactic used for this risk has been 'Take', i.e. to accept the risk. What happened in this particular case was that the amount of losses started to rise significantly, i.e. the impact moved up. As a result, additional manual procedures were introduced by the Business Unit in an attempt to reduce both the

probability and impact. This was, however, seen only as a short-term measure whilst a full-scale change management project was instigated to resolve the problem. This latter course of action becomes necessary in the bank when any changes to systems and procedures could 'potentially have an impact on customers'. In the meantime losses continued to escalate, i.e. the mitigation tactic was not working effectively and fraudsters were finding new ways to beat the system. A further manual procedure was introduced which curtailed the fraudulent activity and reduced losses to an 'acceptable level'. The end solution to this problem, however, will involve the change management project team developing technological changes so that the manual procedures can be removed.

This is an example of "Treat" being used iteratively to mitigate an operational risk exposure. Crucially, the incident illustrates the importance of having follow-up procedures, once the risk mitigation decision has been taken, to ensure the tactic is working. Another important aspect of this incident is the recognition that there will always be some residual risk (acceptable loss) which will be accepted by the Business Unit, since removing the risk, by including, draconian control procedures, could have a negative impact upon customer relations. This incident supports the findings concerning the constraints (cost and customer reaction) imposed upon the managers when mitigating an operational risk as well as the findings related to the need to ensure adequate follow-up measures are in place.

Incident No. 11 – Incorrect Payment Remittance

The bank involved has a procedure in place to check the remittance of international payments. This was described as a 'four eyes' procedure signifying a 'double check' or supervisory control is carried out before the remittance is made. Despite having a control in place to mitigate this risk, on one particular occasion it did not work and a large payment (several thousands of pounds) was mistakenly sent to the wrong party. When the incident came to light some of the monies were recovered (but not all) and compensation had to be paid to the correct party. This risk had been identified but it was considered that there were adequate controls in place to mitigate it happening and that it, therefore, represented a low probability event. Within the same Business Unit, another operational risk had also been identified relating to training/communication of the staff in this section, which was recognised as being 'weak and in need of improvement'. A training/communications plan had been developed to mitigate the risk and was due for implementation 'a few months after the date of the incident'. The training/communication risk had, therefore, been accepted for a short period and the mitigation action had been postponed. It was this latter risk which manifested itself in the 'four eyes' procedure not being undertaken correctly, thus causing the incorrect remittance to be made.

This in an interesting example of how one risk can cause another one to occur, despite the fact that adequate mitigating actions were in place for both of them. It also highlights the behavioural side of operational risk, a particularly difficult area to manage and quantify. The tactic being used to mitigate these risks was 'Treat' although, as has been noted, the second risk had been 'Taken' for a short period of time. The subsequent decision taken

has been to bring forward the implementation of the training/communications plan. This incident supports the findings concerning the constraints (ignorance) imposed upon the managers when mitigating an operational risk and also illustrates the cross-linkages between operational risks themselves.

Incident No. 18 – Deed Store

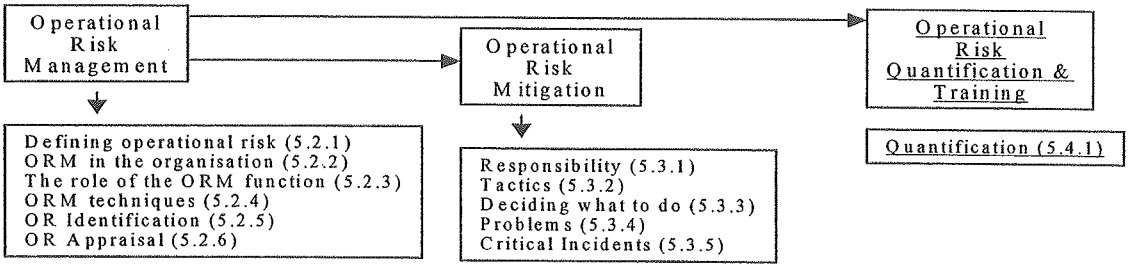
This incident came to light as a result of a competitor having a fire in their deed store with an associated cost of around £80 million. Following this incident, the risks and controls relating to the deed store in the bank were examined and it was discovered that the fire prevention system would not have worked had a fire occurred. The problem was traceable back to the halon gas fire prevention system, which requires a certain pressure to be effective. It was discovered that this pressure did not exist, but the Business Unit responsible for the deed store had already decided to remove this system and replace it with a water-based one, which requires no pressure to be maintained. However, because of costs and budget constraints, a decision was taken not to replace the halon gas and at the same time a new conveyor belt system was installed necessitating a 'large hole in the wall directly into the store', which reduced the pressure even further. The Business Unit were unaware of the potential risk they had created, and the decision not to move forward to a water-based system had not been properly communicated. The net result was the financial impact, had this risk occurred, would have been catastrophic (estimated at £230 million). There would also have been a significant impact on 80 members of staff who worked in the area, as a result of halon gas filtering through the hole that had now been made for the conveyor belt.

The Risk Division became involved in mitigating the risk that now existed and a report was prepared for the Executive Committee and the Board recommending the installation of a sophisticated water-based system at a cost of around £1 million. This was accepted and the author was able to witness the car park being dug up at the time of the interviews! This is an example of "Treat" being used to further reduce the likelihood of the event occurring. In this particular case the risk had also been "Transferred" (via insurance) but this would have been void because the problems with the pressure in the deed store had not been resolved. This incident is particularly interesting because it highlights the importance of monitoring external events and stress testing them in the bank's own environment. The incident also confirms the escalation process that takes place in deciding upon the risk mitigation action (the scale and cost of the mitigation action meant the final decision was taken at Board level) and further emphasises the 'ignorance' constraint as one of the key problems facing management.

5.4 Operational Risk – Quantification and Training

This section discusses the findings in two areas important to the management of operational risk: quantification and training. Quantification has received a lot of attention in the practitioner's literature as a result of banking regulatory requirements, which require capital to be put aside to cover potential operational risk losses (discussed in section 2.4.5.5). Training was identified as an important area in previous work undertaken by the author (Blacker 1998).

5.4.1 Quantification



The results of the data analysis for quantification can be seen in Table 27. None of the banks had a formal methodology for calculating their total operational risk exposure and there was general recognition that there was still a lot to do in this area.

Table 27 Operational Risk Quantification: data analysis

Quantification	ALPHA	BETA	GAMMA	DELTA
Methodology	Not done	Not done	Not done	Not done
Level of support	Sceptical about value of results	Worthy goal, but still a lot to do	Seen as next phase	Mixed, depends on the risk

Source: Analysis of survey data

Support for quantifying operational risk was mixed with a majority of the managers interviewed believing it would not help them in their day-to-day management of operational risk. Those who worked in the Corporate Risk function, who would probably be responsible for carrying out the work, were generally more inclined to accept quantification as something that had to be done:

"At the end of the day, it will make operational risk decisions much easier. At the moment there is far too much analysis, and thought processes having to go around a decision and not enough hard evidence that we can actually sit back and say 'let's make this decision based on the right criteria"

"I think it will be possible for financial organisations to value operational risk but I think what might happen.....is wait and see what Basle is going to say about quantification and then try and impose something from top down that will attempt to quantify operational risk. That will certainly be the case using financial models but I don't think it will be an accurate reflection of what the risks are within those organisations."

For the other managers, and particularly those who operated at the 'sharp end' there were generally adverse comments towards the idea and in some cases contradictory points of view:

"I am sure there are means of devising measures of it, but you have got to bear in mind that any measures might be used in order to take business decisions and if measures are inaccurate you get inaccurate decisions, and I think there is a huge risk of that happening"

"I think you may have greater control over operational risk if you actually put aside the red herring of quantification and simply recognise these are major risks the banks can be running and a certain amount or resource has to be put into controlling them"

"Spending a great deal of time and money on coming up with a number is not necessarily going to get any institution to concentrate on improving its controls"

"with some operational risks, my personal view is that you are better not doing it at all because it might be quite misleading."

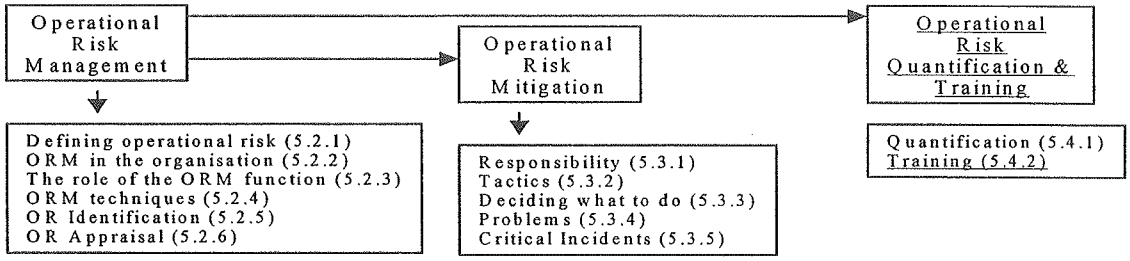
One manager offered some advice to the Regulators:

"If I were a Regulator, I would be looking for distinct evidence that there was a decent operational risk management framework in place. That there was a decent amount of risk awareness in place in the Business areas where the risks are likely to occur and that any quantification was built from a view that the Business areas had of their potential vulnerability of those risks occurring"

These findings are particularly significant as they confirm the view that some banks are not well positioned in relation to developing a methodology for quantifying operational risk but more importantly, they reflect the views of others who have written on this subject (Ong 1998) that operational risk is more of a "management issue and less a quantification issue". This may imply that operational risk prevention (management) and measurement (quantification) should be seen as mutually exclusive since a financial loss

will result from inadequate management control rather than a lack of measurement techniques. This argument is strengthened by comparison with the work of McConnell (1996) who noted that the primary method of controlling market risk in banks was through the use of formal limits, i.e. a qualitative rather than a quantitative assessment.

5.4.2 Training



The results of the data analysis for training can be seen in Table 28. The research found that there is no consistency across the banks in terms of their approach to operational risk training. Alpha bank had developed a formal operational risk awareness training course consisting of two modules for both staff and management. This was separate to their training in CRSA (Control Risk Self Assessment) techniques (see IIA 1999b). At the other end of the scale, Delta bank had not yet considered training, doubtless reflecting the pilot stage of their operational risk framework development.

Table 28 Operational Risk Training: data analysis

Training	ALPHA	BETA	GAMMA	DELTA
Approach	Formal	Informal	Informal	None
Methods	Framework CRSA Training module	Framework	Framework	None
Focus	Management and staff	Management	Management	None

Source: Analysis of survey data

There were many comments in supporting of training:

"...training needs to be focused more on what does it mean 'managing operational risk' and particularly around people's personal responsibilities"

"...educating staff to understand what controls are and where they are required"

"I think the Bank, or the Group, could benefit from some sort of co-ordinated risk training"

"embedding within the organisation at every level an appreciation of the consequences of actions or inactions"

In three of the banks the risk-mapping framework was seen as an 'informal' or indirect training tool for the managers in the Business Unit. Comments from managers who worked in the Business Units indicated that training was seen as an important area:

"We are moving towards getting them (staff in the Business Unit) to think risk. We've got some training packages that talk about operational risk..... in the sense of ticking: here are your key control processes and here are your risk processes"

But, there were other factors that need to be considered in raising the awareness of operational risk:

"Whatever (risk-mapping) process you put in place if you don't have enough experienced people around who have got some grey hairs and been around in the business long enough to understand where the risk is, and if you have a lot of turnover, and if you are not treating your people right, you introduce risk and the soft factors are quite important in looking at that. Training, development and retention of staff"

These findings are particularly important in the context of the problems that managers face in managing, and, therefore, mitigating operational risk. Ignorance (see Table 26) was cited by all of the banks as being an important barrier to effective operational risk mitigation and it could be argued that the best way to overcome this is through an effective training program.

5.5 Summary of Findings

The most significant finding of the research is that all the banks in this study are developing their operational risk management frameworks in accordance with the requirements of the draft Basle (2001) accord. There remains much to be done, however, on the measurement side of operational risk with all of the banks being in the embryonic stages of development. The study confirmed previous findings vis-à-vis the definition of operational risk. There is a common understanding of the broad areas that operational risk covers but strategic risks (however they may be defined) are not always included.

There are two types of operational risk managers present in all the banks: the Corporate Operational Risk manager and the Business Unit Operational Risk manager. The roles of the two appear to be clearly articulated and they have close working relationships although there is no direct reporting line between them. This is not necessarily a problem but it highlights the issue of maintaining good communication channels between the individuals if both parties are to do their jobs efficiently (minimise any overlap) and effectively (sharing best practises). The same comments may be said of the relationship between the operational risk managers and Internal Audit. The study found that the reporting lines of Internal Audit and the Corporate Operational Risk function were identical in three of the banks. This in turn could cause problems with independence, when Internal Audit has to review the work of the Operational Risk function.

The study found that a risk-mapping framework was present in all the banks albeit that the system was being piloted in Delta bank at the time the work was carried out. The

phases within the frameworks were found to be consistent with the literature although there are a number of variations in the modus operandi and documentation produced reflecting the bespoke development of these frameworks and the individual preferences of the banks. All the frameworks were used to manage as opposed to measure operational risk. Whilst the Corporate Operational Risk functions were the 'owners' of the framework, the responsibility for managing (identification, responsibility and mitigation) operational risk was found to be the managers in the Business Unit, a responsibility that was in effect delegated down from the Board.

One of the key findings of the study is that the Managers in the Business Units rely on help from both internal and external specialists in discharging their responsibility. This is the case for all phases in the operational risk management process and again reflects the broad scope of what is defined as operational risk. Identifying when they need help and who can help them is a crucial element in the process and one which managers in the Business units have not always been good at as some of the critical incidents attest to.

Turning specifically to operational risk mitigation and the focus of this study, the findings indicate that the mitigation process for an operational risk varies from a simple improvement to an internal control procedure to the complexity of establishing a project team to resolve the matter. The tactics used were found to be broadly in line with the literature with the 'Treat' tactic being the most commonly used. This is consistent with the nature of operational risk, which is principally found in an organisations internal control environment (Basle 1998a). Another important finding of the study is in relation

to the barriers or constraints that exist in mitigating operational risk. Whilst the issue of cost is unsurprising, more worrying is what was described as 'ignorance' or lack of awareness of operational risk. One of the key ways to improve this is through training and the study found that whilst there was widespread support for the development of formal training, very little had actually taken place.

6. ANALYSIS AND IMPLICATIONS FOR MANAGEMENT

6.1 Introduction

This section considers the implications of the findings of the study (section 5) for the management and mitigation of operational risk in UK retail banks. The experiences of the managers from four of the leading banks involved in operational risk management are used to draw lessons for others who may be embarking on a similar path. The section opens with a discussion of the organisational implications, followed by an examination of the implications for operational management, the Operational Risk function and Internal Audit, the three main players identified in the management of operational risk. Finally, conclusions about the research problem are discussed and a proposed theory offered.

6.2 Organisational Implications

6.2.1 Implications for the Board

The Turnbull (1999) report placed risk management and internal control firmly on the agenda for all Board directors. The directors of banks have a particular interest in managing operational risk because of the requirement to set aside capital to cover expected and unexpected losses. Banks are unique in this respect and tying up capital in this way reduces the amount of money that is available for distribution to shareholders. There can be little doubt that the Board has an influential role in managing operational risk by creating a culture of risk awareness and distilling this down to the operational managers in the Business Units.

"I believe you should start at the top, and have a clearly defined policy and then make sure that is properly understood, communicated down and adhered to in the business"

The Board carries the ultimately responsibility for the risk management activities that are undertaken. Previous high profile operational risk management failures such as Barings have given rise to criticisms of Boards for their failures to establish effective internal control environments and to monitor adherence to laid down procedures. Operational risk is embedded within a bank's internal control environment (Basle 1998). It is a complex issue and the explicit management of operational risk will demand continuous Board attention as risk profiles change due to changes in internal and external circumstances. The following comment from one of the managers seems to capture the mood:

"I would probably suggest that a lot of the major operational losses occurred because management turned a blind eye"

Turning a blind eye never has been an excuse and if it continues then it will remain an important cause for why operational risk incidents occur. So what should Boards be doing to ensure that they managing their risks effectively?

"a Board should know its top 20 risks"

This is probably the minimum that could be expected. If every member of the Board is unaware of the most significant risks that the bank faces then their chances of being able to manage them effectively are severely diminished. Turnbull (1999) lays down criteria that Boards should be following and Basle (2001) is suggesting even more. For example, Basle (2001) is proposing[62] that 'banks should publicly, and in a timely fashion, disclose more detailed information about the process used to control their operational risks and regulatory capital allocation technique they use'. The financial reporting of risk was

[62] Page 4 of the Basle (2001) consultative document

proposed by the ICAEW (1998) 'to encourage better risk management, help reduce the cost of capital and provide enhanced reporting to investors'.

The UK retail banking business involves more than just banking as has been noted in Chapter 2. All of the banks in this study, for example, have large insurance operations, which contribute to the bank's overall profitability and risk profile. The breadth of operations and, therefore, the breadth of operational risks, are large. Boards need to recognise this and ensure they maintain sufficient expertise to understand and manage these risks. A final consideration for the Board is the amount of money that the Bank spends or should spend on managing operational risk:

"The Group spends virtually all their expenses on managing operational risk in one form or another whether it be by the Business or us centrally"

This observation from one of the Heads of Operational Risk suggests it is not just a question of the direct costs of the 'operational risk' people that should be considered but a large amount of the bank's overall budget as 'everyone has a role to play in managing operational risk'. The author considers this to be an area worthy of further research.

6.2.2 Risk Management Committee

As the results of the study have shown, the use of an operational risk committee (or even a risk committee) to look at operational risk is by no means consistent in the banks. There is little in the literature discussing operational risk committees although both audit committees (Turnbull 1999) and generic risk management committees (McConnell 1996) have been mentioned. The breadth and newness of operational risk appears to be a strong pointer towards establishing such a committee or including it within a generic risk

management committee. Whilst the research did not examine this area in detail there are a number of issues arising from the study that are worthy of further consideration.

An operational risk committee would normally be created as a sub-committee of the Board and could fulfil a number of roles in helping to manage and measure operational risk. For example matters of policy may be decided, establishing the boundaries and categories (definition) of operational risk, overseeing key projects, deciding upon mitigation actions which span business units and receiving regular reports on operational risk. Where a risk committee is already in existence then there could be a strong argument for extending the terms of reference of this committee to include operational risk:

"One of the problems with operational risk is it literally covers the operation from beginning to end in reality. Even treasury and financial risks have operational elements to them."

Credit risks could be added to this, as there are operational processes involved in assessing the credit worthiness of an individual/organisation. Equally, the inclusion of the scope of operational risk in a generic risk management committee would help to ensure that all risks in the bank are being managed. Strategic risk within the context of operational risk remains the subject of some debate:

"it was all about getting management to see that what they thought was a really good strategy was actually flawed. And it's flawed not because it's not a good thing to do, it's flawed because you're not managing the operational risks that go with exactly what you are doing"

"Turning around to a division and saying the next year we want you to increase your volume by 200% has operational risks and quite often, what you will find is the operational risk has been assessed based on a static organic growth"

Whilst Basle (2001) has specifically excluded strategic risk from the measurement debate, it still remains a risk and as such needs to be managed explicitly. This raises some

interesting problems about whether strategic risks should be quantified. If not, then the 'holy grail' of being able to quantify a bank's total risk exposure will never be reached. If so, then the question is how should it be done?

The Risk Management Committee could also take on overall responsibility for the measurement of operational risk and the subsequent allocation of the capital set aside to Business Units, thus reflecting the amount of operational risk they are carrying. This latter point is set to be a potential problem area unless a fair and reasonable method can be found to allocate capital.

Finally, the Risk Management Committee could help set the tone for operational risk management in the bank by ensuring that a consistent message is filtered down to the Business Units. The results of the study indicate that the message behind good operational risk management is about being more operationally risk aware rather than being risk averse. This message can be communicated in a number of ways, including for example, training (see section 6.2.5).

6.2.3 The Operational Risk Manager

The research found that there are two types of operational risk manager in the banks studied. The Corporate operational risk manager and the Business Unit operational risk manager. The roles have been well defined and there is evidence that the two work closely together. The Corporate operational risk manager role has developed into the

central monitoring role where a high level and aggregate view of the operational risks being faced by the bank can be assembled. Out of what appears to be a growing need to help the Business Units improve their management of operational risk, the Business Unit operational risk manager role has evolved. They are part of the Business Unit and work with them on a day-to-day basis facilitating, helping and cajoling the managers into achieving the desired level of operational risk.

The existence of these roles in any organisation is confirmation of the explicit nature of operational risk management. They effectively add value by ensuring that the organisation manages the operational risks and not the other way around. As such, they are similar to the internal auditor: they are there to prevent something bad happening. It was beyond the scope of this study to examine the skills and experience required to be an operational risk manager but it is certainly a possible area for future research:

"I think to do operational risk well, there is no substitute for having been an auditor first, preferably an internal auditor"

The author is not surprised that one of the operational risk managers interviewed made this comment as internal auditors focus their efforts on the internal control systems where operational risks are principally found. The challenge for the operational risk manager is in ensuring that the managers with whom he works understand the difference between his/her role and that of the internal auditor. This is particularly so where the reporting lines of both units are through the same line.

6.2.4 Integrated Risk Management

"I think operational risk as a term has not really been widely used within the Bank until it became much more popular in the last three years. Up until then the focus was certainly very

much towards credit risk and perceived credit risk, although in reality, many of the issues about credit risk were actually operational risk issues"

"We must take risks as a bank"

"Banks are in the business of risk...(pause)...at a price"

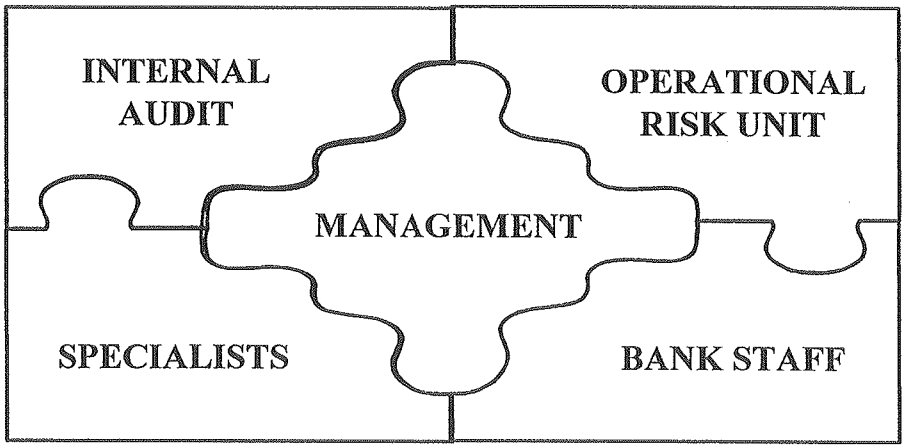
Risk management is an ongoing process and of fundamental importance to a bank because of the regulatory requirements in relation to capital. Prima facia, therefore, it makes good sense to develop an approach to risk management which combines all the major forms of risk[63]: market, credit and operational. Whilst the nature of these risks may be different, operational risk is the 'common denominator' as operational processes exist in both market and credit risk transactions. As a result, the boundaries are sometimes blurred, a point also noted in a recent practitioner's survey (BBA 1999a).

Developing an integrated approach though would be difficult to achieve because of the inherent differences in the nature of the three risks and ways in which they need to be managed, and, therefore, mitigated. Credit risk managers are 'proactive in performing up-front analysis of company and economic data' (McConnell 1996), whilst market risk managers 'analyse risk in multiple transactions after they have been taken' (McConnell 1996). Operational risk managers on the other hand assess the risk profiles of Business Units. Whilst it makes intuitive sense to have a similar reporting line, the approaches adopted to manage these risks will remain different.

[63] The reader is reminded that there are other forms of risk inherent in banking activities such as sovereign risk and liquidity risk. Many banks describe their position on these risks in their Annual report and accounts.

One feature of operational risk that differs from credit and market risk is the number of people who have the opportunity to help manage it. The research indicates that everybody has a role to play since operational risk exists in every procedure used in the bank from the petty cash system to the strategic planning process. This suggests that an integrated form of operational risk management is an objective worthy of further consideration. Looking at this from the point of view of the main players there would be five pieces of the 'jigsaw puzzle' that would have to fit closely together for an integrated and effective approach to be adapted. This is shown in Figure 18.

Figure 18 Integrated Operational Risk Management



What are the drivers behind making the jigsaw fit together? The author would offer the following:

1. A coherent and widely used risk-mapping framework;
2. A risk based internal audit approach;
3. A willingness by management to use specialists to help them manage their operational risks;
4. Good communication channels;
5. Well-trained staff;

6. Support from the Board.

6.3 Implications for Operational Management

6.3.1 Operational Risk Management

The research confirmed that the responsibility for operational risk management lies with the managers in the Business Units, i.e. operational management.

"the whole idea is that every risk within the organisation has a home and someone who is responsible for it"

The risk-mapping process identifies the risk owner in the sense described above and has moved the management of operational risk from being informal and implicit to formal and explicit. In short, operational managers who have always managed operational risk as part of their day-to-day responsibilities, now find that they do it with a better understanding of the problems involved. It is vital that operational managers recognise the pivotal role they play in this process and the demands that are now being placed upon them when (explicitly) managing such a complex area. Some of the issues that have been identified in the study include:

1. The need to consider the effect that one risk can have on another – see Appendix D, critical incident no. 11;
2. The need to focus on managing the key risks and not the risks they like or find easy to manage;
3. The risk appetite of the bank and the Business Unit in which they work;
4. The need to look for support (either internally or externally) when they are unable to manage an operational risk by themselves;

5. The vital role their staff play in helping them to manage operational risk on a day-to-day basis.

Operational risk-mapping is not a one-off exercise. It is a continuous process that must be done in addition to the ongoing management of the operational risks that are found the moment 'the manager sits at his desk'. New operational risks can appear from a variety of sources:

"Centralised processing and telephone banking, these are all new operational risks"

Operational managers must be alert to these new threats and react accordingly. The research also identified the opportunities that exist with operational risk management, particularly the opportunity to challenge the amount of control that is being exercised in relation to the risk involved. Control processes, which have been in place for some time, need to be checked to make sure they are still valid and appropriate. Operational risks can be over-controlled (control inefficiency) as well as being under-controlled (control deficiency). The challenge for the operational manager is balancing the two control elements.

Operational managers also need to understand that they have a vested interest in creating an operational risk environment with a low level of residual risk. One of the emerging drivers behind this will be the capital charge that Business Units are likely to suffer when operational risk measurement becomes firmly embedded in the bank. The allocation of capital should, in theory, reflect the riskiness of the Business Unit and the higher the charge the greater the expected return will be.

Finally, in focusing their attention on their operational risks the managers must recognise the importance of working within a defined frame of reference. Specifically, this is likely to be the Business Unit objectives. Their efforts to manage operational risk need to begin with an assessment of their objectives from a risk perspective and a clear understanding of how those risks are currently being managed.

By responding positively to the benefits offered by the risk-mapping framework, operational managers can help protect themselves from the dangers that ineffective management of operational risk can bring. The critical incidents reported in Appendix D bear witness to some of the problems that can be caused when management are unable to effectively mitigate operational risk.

6.3.2 Operational Risk Mitigation

The focus of this research has been in the area of operational risk mitigation and a number of findings have implications for operational managers. Firstly, recognising that there are a number of different ways to mitigate an operational risk, although the most common, treating the risk, is likely to be the most appropriate given that most operational risks are embedded in the internal control environment. Secondly, their decision to mitigate will be constrained by a number of factors inherent in the way the organisation works and their own perception of the risk and knowledge of what can be done. Thirdly, mitigation is one area where other specialist units can have an important role to play in advising and implementing on the most appropriate course of action. Fourthly, the

decision taken on how the risk will be mitigated should include an agreed action plan, which is capable of being monitored, as a basis for ensuring the desired level of residual risk is being achieved.

A checklist for mitigating operational risks has been drawn up by the author. This is shown in Appendix F. The reader should note that this checklist is based on the data analysis undertaken by the author and may be seen a practical roadmap that may be used by managers when faced with an operational risk mitigation situation.

This checklist is seen as an important contribution since it offers practical recommendations to improve existing practice and is of use not only to the banks in the study but to others who wish to enhance their risk mitigation process. The regulators have indicated that they intend to begin (qualitatively) reviewing the operational risk management approaches of banks (Basle 2001) and the checklist should provide an important contribution to this process.

6.3.3 Training

The author considers that training in operational risk management is an important challenge for banks[64]. The research indicated that the managers felt that there was still work to do in this area. The current 'informal' training that is given via the risk-mapping exercise is only half of the story:

[64] The problem of training in risk management is not just confined to banks. There is anecdotal evidence to suggest that there is a lack of generic risk management training in many management development programs.

"They (the managers in the Business Unit) are all risk aware when we all sit around and have a discussion but they don't think it necessary when they are doing their plans and budgets and that kind of thing"

The development of a formal training program with the emphasis on operational risk awareness could be an important part of the bank's armoury in defending themselves against operational risk. The regulators are planning to introduce 'independent evaluation of operational risk' (Basle 2001) via, inter alia, 'the effectiveness of the bank's risk management processes with respect to operational risk exposures'. The author would, therefore, argue that demonstrating a formal training program would be a great asset for the banks when dealing with the regulators. The risk-mapping process relies on people throughout and it is their knowledge, skills and experience, which will determine the robustness of the results. Training in risk management should not, therefore, be seen as an 'optional extra' in the development of staff, but as a 'standard feature'.

Training may be focused and specific to the needs of the management and staff within the bank. An important part of the process would be to ensure that new starters are given sufficient training as part of their induction program. The development of a training strategy in the area of operational risk would be a key factor in helping to:

"increase the hurdle rate of risk management knowledge"

6.4 Implications for the Operational Risk function

6.4.1 Risk-mapping framework

"what we have got to be careful in putting any process in place for operational risk is that you don't switch off the common sense. We have seen it in dealing. You give dealers....derivative traders hedge funds, you give them sexy software to become a mathematical genius but they will still lose money because they forgot to think"

The above comment from an operational manager has an important message behind it. The risk-mapping process that the banks in this study are installing, or have installed, is not designed to be used as a 'checklist' for managing operational risks. All staff who contribute to the process must think 'outside the circle' particularly in the first phase of operational risk management where risks are being identified. Where workshops are used the selection of a range of people will help to remove risk bias and the skill of the facilitator in extracting the data from participants will be key to the success of the process.

The study found that the risk-mapping process itself is still relatively new within the banks studied. Once the risk map becomes a complete compendium of the operational risks faced by the bank, then the emphasis on the risk mapping process will move towards updating the risk profiles and capturing any new risks arising from, for example, major developments in the Business Unit. As the operational risk management process matures, there is likely to be more emphasis placed on internal and external monitoring of key risks and the development of the operational risk incident database. It is unlikely that a generic operational risk management framework will develop given the bespoke nature of the ones used in the banks studied and also the increasing developments in software applications for operational risk management[65]. That said, there are common features to all of them and there are certainly opportunities for say the Regulators to develop a best practice model based on their reviews of the operational risk management techniques

[65] The author is personally aware of two such packages and the practioner magazines have advertisements for others

being employed in the banks. Of particular interest is the approach at Gamma bank and Delta bank which request the risk to be documented in terms of event and causes (of the event).

"what we are trying to do is give them (the Business Unit managers) a structure where they can break it down and understand it more"

It is outside the scope of this research to establish whether the Business Unit managers do indeed understand it better but it would be an interesting area for future research as it could help in the development of a best practice model.

The author was unable to establish if the risk mapping process had been applied carte blanche across the banks being studied. For example, have the operational risks within the Corporate operational risk function been mapped? Is there a role for Internal Audit to play in completing this task (see section 6.5.1)? Have the operational risks in Internal Audit been mapped? The evidence in this study suggests that these two areas play a pivotal role in assisting operational management in managing their operational risks. If their work cannot be relied upon, and Internal Audit has come in for criticism in the past[66], then a question mark must hang over the whole process.

6.4.2 The role of the operational risk function

The operational risk managers, whether they operate at the corporate or the Business Unit level, have an important role to play in maintaining an acceptable level of operational risk in the bank. The study found that the primary vehicle for arriving at this desired level was

[66] Internal Audit were criticised over the Barings fiasco for not being resilient enough and Basle (1998b) found that Internal Audit was ineffective in many problem banking organisations

the implementation of an agreed action plan to mitigate a risk. If this is to be effective then a tracking procedure must be implemented. The Regulators have previously criticised Internal Audit for having an 'inadequate follow-up when problems were noted' (Basle 1998b) and of the four banks studied, Gamma bank appeared to have the most comprehensive procedure:

The tracking procedure is essentially through the operational risk manager being alert to action plans and delivery dates on these action plans and prompting business areas where they may have passed these dates with nothing happening or not enough happening. We here at the centre are also able to take an overview of how these plans are being progressed and are in a position to escalate them where necessary to Executive level.

Operational risk managers must recognise the growing importance that will be placed on managing this follow-up process.

The role of the operational risk function appears to be well defined in the banks studied and there is a degree of commonality in the functions they undertake. In the future, it may be that working in partnership with Internal Audit so as to avoid duplication of effort will be an important part of their role. This will necessitate good open communication channels to be maintained on both parts.

6.4.3 Quantification

As is evidenced by this study and the literature review, the measurement of operational risk remains the biggest challenge for banks. Basle (2001) has proposed three methodologies in their consultative paper, and these are likely to be the subject of debate over the coming months as the proposals are discussed. The Heads of Operational Risk from four of the leading UK retail banks interviewed in this study are likely to assume responsibility for developing and installing an appropriate methodology. Whether the

benefits of quantification will be seen further down the lines within the Business Unit are open to question. There is evidence in this study that those at the 'sharp-end' of operational risk management see the quantification debate as irrelevant to them. If the Regulators are expecting quantification to influence the behaviour of managers in the way they manage operational risk then there is no evidence in this study to support that assumption and it would be a fruitful area for further research.

The implications, both from the research and the literature, for the operational risk function is that they are likely to have to bridge the gap between the expectations of the Regulators and the expectations of the bank. One issue, for example, is the quantification of operational risk in insurance subsidiaries where the 'jury appears to be out' on what best to do. If quantification goes ahead and banks have to put capital aside, then they could placed at a competitive disadvantage to independent insurance operations who are currently not required to set aside capital[67] in the same way[68]. If quantification in this area is relaxed and there is no requirement to set aside capital, then by definition the banks will not be covering all their operational risks in areas where particular problems have been found in the past[69].

[67] Insurance companies are required to maintain a certain solvency margin which represents free capital set aside to ensure they can meet their liabilities to policyholders. It is not related to operational risk.
[68] The argument here is that the cost of capital for the banks will increase and shareholders will demand a greater return to reflect this
[69] See Blacker (2000) for a discussion of the pensions mis-selling scandal

6.5 Implications for Internal Audit

6.5.1 The role of Internal Audit

"People take this comfort factor from saying Internal Audit are happy with the proposals"

The evidence from this study indicates that the Internal Audit function has an important role to play in the management of operational risk. As a function, it is charged with providing an independent opinion on the adequacy of the internal control environment, which is designed to mitigate all risks. It is not just interested in operational risk mitigation but in all forms of risk mitigation. Much of its focus will be on operational risks and as well as assessing the adequacy of internal controls it will also perform tests on them to ensure that they are working correctly.

One of Internal Audit's primary responsibilities in the management of operational risk is assessing the work of all the operational risk managers and how effectively they do their job:

"if you can't rely on Operational Risk doing its job, all the reports that they produce for you are next to useless"

It could be argued that one of the most important risks that a bank faces is having an inadequate operational risk management system. The most logical unit who is in a position to form an opinion on this, is Internal Audit. Through its reporting line to the Audit committee, it provides comfort to the Board that the operational risk management system that is in place is adequate and is appropriate for the needs of the bank. Basle (2001) makes specific reference to the role of Internal Audit as being 'to conduct regular reviews of the operational risk management process and measurement methodology'.

Whilst regular is not defined, it suggests that Internal Audit should plan to review the work of the Operational Risk function on an ongoing basis in order to help satisfy regulatory requirements. Equally, if it is to rely on the work of the Operational Risk function in developing its own plan of activities then the aforementioned review takes on even more importance (see section 6.5.2 on risk-based auditing). Based upon the work undertaken in this study, the author has drawn up a checklist for use by Internal Audit when it reviews the work of the Operational Risk function. This can be found in Appendix E.

The identical reporting lines of both the Corporate operational risk function and Internal Audit found in three of the banks in this study are a potential source of difficulty. There are two reasons for this. Firstly, it could easily lead to confusion in the eyes of auditees about the precise roles and responsibilities of the two functions, a point not helped when operational risk managers previously worked in Internal Audit. This confusion may also be driven by evidence in the practitioner's literature of the two roles being combined in other financial services organisations (Cunnington 1999). Secondly, it compromises the independence of Internal Audit when it is reviewing the work of other functions in their division, specifically, of course, the operational risk function. This is a matter that senior management should consider carefully, particularly in the light of Turnbull (1999), which requires the Board to 'annually review its (Internal Audit) scope of work, authority and resources'.

Aside from the review of the Corporate operational risk function, Internal Audit also has a role to play in assisting with the management of operational risk. The evidence in this study points to its contribution at various stages in the operational risk management process:

1. Identification – through a regular review of operations where the focus of its work is on identifying risks followed by assessing and testing the mitigating actions in place;
2. Appraisal – acting as a 'long stop' control over the correct assessment of the impact/probability of the identified operational risks;
3. Mitigation – assessing the completeness of follow up action plans and acting as an advisor on mitigation tactics related to improving the internal control environment.

It would appear, therefore, that Internal Audit has an important role to play in the management of operational risk. Providing it adopts appropriate audit techniques, such as risk-based auditing (see section 6.5.2), there is every reason to believe that it is a key element in ensuring that management is achieving its desired level of residual operational risk.

6.5.2 Risk-based auditing

The need for a paradigm shift in the way that Internal Audit approach its work has been well articulated by McNamee and Selim (1998). Risk-based auditing to use the terminology in the literature (see Paul 1994), is now recognised by practitioners as being the most efficient and effective way that a 'modern' Internal Audit function should

operate. Whilst this study did not concentrate in this area, it was established that the Internal Audit departments of the banks in question all adopted a risk-based audit approach. The development of explicit operational risk management with its risk-mapping framework and well-documented results is an important input into the risk-based audit approach. It provides the internal auditor with a starting point from which audit work may be planned both at (1) the macro level – which are the 'riskiest' business units where internal audit effort should be concentrated, and (2) the micro level – where are the main risks within the business units where internal audit effort should be concentrated.

The author believes that it is incumbent upon Internal Audit departments to recognise that the focus of risk management is changing. Responding to these changes will be an important challenge for internal Auditors if they are to maintain their relevance and value to their 'customers' (operational management and their staff) and their 'stakeholders' (Board and the Audit Committee).

6.6 Conclusions about the Research Problem

The main research question that the study set out to answer was:

"How do UK retail banks mitigate their operational risk exposures?"

In formulating this question, the author was interested to see how the 'core model' of operational risk mitigation compared to theoretical models and the expectations of the Regulator. No regulatory models were found and indeed the Regulators have recently stated (Basle 2001) that they 'intend to work with the industry on risk mitigation concepts

over the coming months'. The author had some early discussions with one of the UK regulators, the Financial Services Authority, but it was apparent that their focus was on providing guidance on the definition of operational risk and how it may be measured.

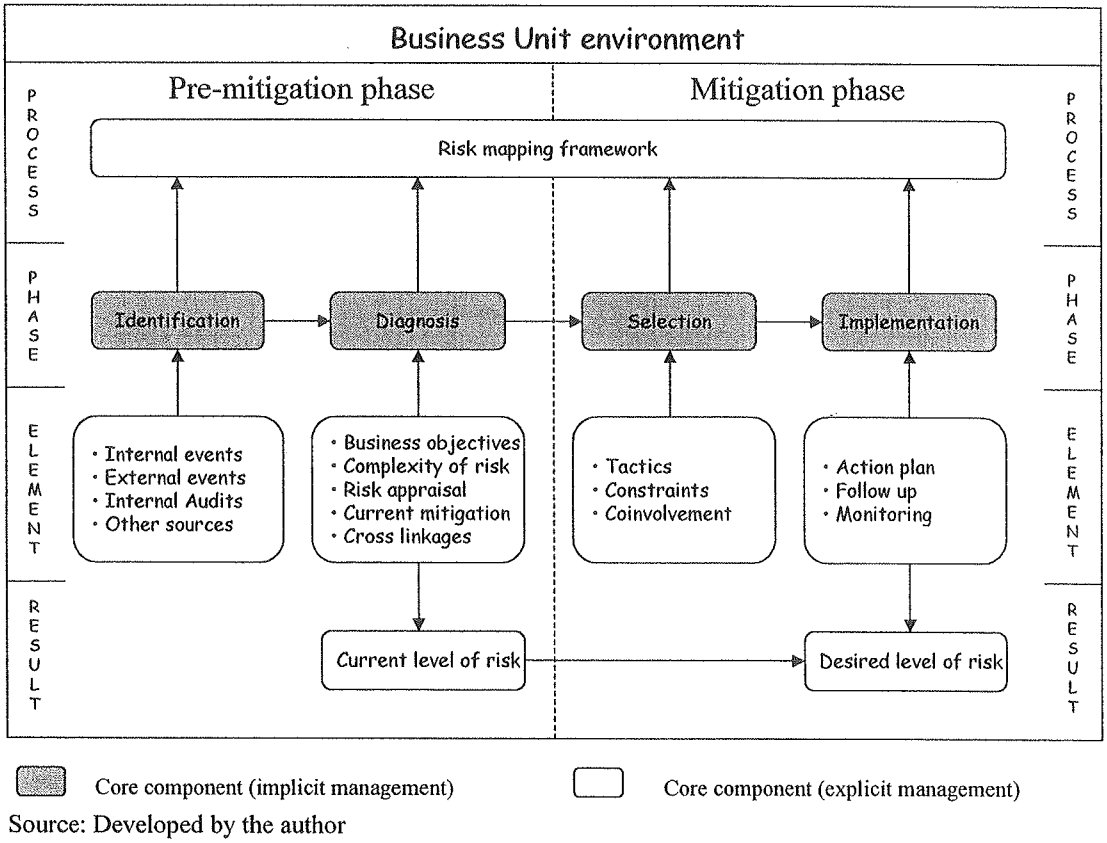
Against this background, the remainder of this section discusses a proposed theory on operational risk mitigation, how the move from implicit to explicit operational management has affected the pre-mitigation and mitigation phases of the risk management model and what problems exist in mitigating operational risks.

Based on the evidence from this study, the proposed theory of operational risk mitigation offered by the author has the following characteristics:

1. There is no single best way to mitigate an operational risk (*based on contingency theory*);
2. Managers mitigate operational risk by diagnosing the risk and selecting an appropriate mitigation tactic based on their internal environment (*based on the theory of bounded rationality*) and their own perception/knowledge of risk (*based on risk perception theory*);
3. The implementation of a mitigation tactic should lead to improvements to the internal control environment and a reduction in the level of operational risk;
4. The action managers take to establish the correct implementation of a mitigation tactic enables the organisation to guarantee its residual level of operational risk (*based on control theory*).

The author has argued that the management of operational risk has moved from being implicit to explicit. This change in emphasis is important in developing a model to illustrate the above theoretical propositions because, whilst there are a number of key phases with implicit operational risk management, additional 'components' may be added to demonstrate explicit operational risk management. The study has found that these components, however, are not just limited to the mitigation phase of operational risk management but are also found in the 'pre-mitigation' phases. Looking at the mitigation phase in isolation would not give the whole picture and the author has, therefore, proposed a model, which considers all the phases and components. This is shown in Figure 19.

Figure 19 Proposed Operational Risk Management model



Source: Developed by the author

The core components of implicit/informal operational risk management are shown as shaded boxes along the horizontal line marked 'Phase'. These equate to the phases in the simple risk management model (see Figure 1) as per Table 29.

Table 29 Phases of the risk management models compared

Proposed Risk Management Model phase	Simple Risk Management Model phase
Identification	Identification
Diagnosis	Evaluation, Estimation
Selection	Mitigation
Implementation	Mitigation

Source: Developed by the author

With the arrival of explicit/formal operational risk management, the core components have been augmented by a number of additional components which are represented by a further three horizontal lines:

- Process – the risk-mapping framework is now the driver behind the whole of the operational risk management effort and the phases are embedded within it;
- Elements – each of the phases has a number of distinct elements which act as the main drivers for that phase;
- Result – there is an explicitly stated current level of operational risk and desired level of operational risk.

Turning to the two pre-mitigation phases:

1. Identification – the evidence from the study indicates that there is a combination of elements which support this phase. Operational risks are identified through the examination of internal and external events (incidents/losses), by the Internal

Audit function and via a number of other sources (workshops, questionnaires, and so on) specific to the bank;

2. Diagnosis – the diagnosis of the risk is a crucial input into the mitigation phase and represents the qualitative assessment, which provides management with the current level of the risk. Evidence from the study point to a number of elements being used to arrive at the diagnosis: the objectives of the Business Unit, the complexity of the risk, the risk appraisal (probability/impact), the current mitigants in place and the cross linkages that the risk may have to other risks.

Turning to the mitigation phases:

1. Selection – the decision phase when the manager examines the risk diagnosis and selects, from the options available to him, what action to take. The evidence from the study suggests that the elements that will influence his decision are the tactics available to him, the constraints imposed upon him by the bank and his own knowledge of operational risk management, and his knowledge of who may be able to help him to mitigate the risk;
2. Implementation – the evidence from the study indicates that this final phase, the one that guarantees the desired level of operational risk, is driven by the establishment of an action plan (based on the mitigation tactic selected), the use of adequate follow-up procedures and the ongoing monitoring of operational risk indicators.

The reader will note that the model is similar to other decision-making models and is, therefore, well-rooted in existing theory.

It is the opinion of the author that the development of an implicit/formal system to manage and, therefore, mitigate operational risk should be based on a model of this type. The reader is again reminded that operational risk is a large and complex area and to reduce its management down to a few boxes in a model is not intended to trivialise the task ahead but merely to identify the building blocks from which a tailored solution to the banks own particular circumstances may be constructed. The model represents core practice derived from four of the leading UK retail banks.

Even with such a process in place, it should not be assumed that the panacea to operational risk management has been found. Drawing on the evidence from the four banks in this study, a number of problems relating to operational risk mitigation were noted:

1. The diagnosis of an operational risk is not a straightforward process. In some cases there may be observed or historical information upon which the impact/probability appraisal may be carried out whilst in others there may be next to nothing, for example, the operational risks involved with Internet banking;
2. Any mitigating actions should address the cause of an operational risk and not the event itself. Taking a simple example, having insufficient stocks of marketing material for customers could be due to a lack of stock-checking procedures. In this

case the solution is not to order more marketing material but to introduce improved stock checking controls.

3. Undertaking the cost/benefit analysis that is used to help decide on whether or not to mitigate a risk, is not always an easy task. For example, should the risks associated with web-site security breaches consider the reputational losses that the bank could suffer? If so, how should they be quantified?
4. Ensuring that managers are alert to the possibility of using help in mitigating an operational risk relies heavily on the individual judgement of the manager and his willingness to call for help. These types of factors may be difficult to manage because they rely on individual behaviours and personal relationships.

6.7 Summary

This chapter discussed the implications of the findings of the research for bank management. Operational risk is a complex area and the problems inherent in managing it are spread across the whole of the bank's operational processes. The starting point is the Board who must set the risk appetite not just for operational risk, but for all risks that the bank has to face. The Board is ultimately accountable for the operational risk exposures that the bank faces and although it delegates this responsibility to operational managers, it must retain a firm grip and understanding of what is already a fast evolving area. Lessons learned from this study of four major UK retail banks have been used to illustrate some of the issues that senior management have to face in addressing how best to manage, and with it, mitigate operational risk. Implications for the organisation, operational management, the operational risk function and Internal Audit were discussed. Finally,

conclusions about the research problem were explored with some theoretical statements and a model of the operational risk management process being proposed. The final word in this section is left with one of the risk managers interviewed and his view on the value of operational risk management.

"The real value of what is emerging with operational risk management is the recognition that it is not wrong to have an operational risk exposure, as long as you understand it and can say it's not cost effective to the business to introduce controls"

7. SUMMARY

7.1 Summary of the Research

Operational risk is a new topic in the financial services industry and this research examined the management of operational risk specifically in UK retail banks. The study was focused on the mitigation phase of operational risk management where a number of key issues were reviewed: the responsibility for operational risk mitigation; the tactics that were used to mitigate an operational risk; the barriers that existed when deciding upon an appropriate operational risk mitigation strategy. The subject is highly topical in the banking industry because of the regulatory requirements vis-à-vis operational risk that are being proposed by Basle. The research looked at operational risk from the perspective of the risk manager, the internal auditor and the operational manager in the Business Unit and may thus be described as inter-disciplinary.

The literature review in Chapter 2, provided a high level overview of some of the theoretical propositions and current issues in the areas of Banking, Internal Auditing, Management and Organisation that are of relevance to operational risk management. Operational risk management has become an important issue both for regulators and the banks themselves and the literature review established the implications for operational risk management in each of these areas. The Basle (2001) accord and the regulatory regime were discussed in Chapter 2 along with a review of theory in the generic area of risk management, with a section dedicated to operational risk. An important distinction

was made between the management of operational risk and the measurement of operational risk, both of which are seen as important by the regulators.

One of the drivers for this research was the early discovery by the author that little academic research had been done in the area of operational risk for financial services organisations. On top of this, the regulators had begun to produce a number of papers on operational risk management and the internal audit profession were also moving their audit approach towards being 'risk based'. These were the initial impetuses for the research, and further endorsement was given with the recent publication of the Basle (2001) accord, which has moved operational risk towards the top of the agenda for bank management.

The research design is described in Chapter 3. A case study approach was adopted as offering the best opportunity to answer the research questions. The design is qualitative and is based upon well-established techniques for case study research, particularly when the topic is new, the area has had little prior research and the research aims to develop theoretical propositions. Four cases were selected for study. Each case represents an example of a major player in the UK retail banking arena, a point that was important in the selection criteria, as the research was targeted at establishing 'core practice' by looking at industry leaders. Chapter 4 provides a more detailed look at the case study techniques that have been used.

The major findings of the research, summarised in Chapter 5, are that all the banks in this study are developing their operational risk management frameworks in accordance with the requirements of the draft Basle (2001) accord. There remains much to be done, however, on the measurement side of operational risk with all of the banks being in the embryonic stages of development. The study found that a risk-mapping framework was present in all the banks albeit that the system was being piloted in one at the time the work was carried out. The phases within the frameworks were found to be consistent with the literature although there are a number of variations in the modus operandi and documentation produced reflecting the bespoke development of these frameworks and the individual preferences of the banks. All the frameworks were used to manage as opposed to measure operational risk.

Turning specifically to operational risk mitigation and the focus of this study, the findings indicate that the mitigation process for an operational risk varies from a simple improvement to an internal control procedure to the complexity of establishing a project team to resolve the matter. There was general agreement that the barriers or constraints to mitigating operational risk are driven by either cost or ignorance. Whilst the issue of cost is unsurprising, more worrying is 'ignorance' or lack of awareness of operational risk. One of the key ways to improve this is through training and the study found that whilst there was widespread support for the development of formal training, very little had actually taken place.

The study has made a number of important contributions, which may be summarised as follows:

- Operational risk is acknowledged as being under researched in the financial services sector and the study has helped to chart and clarify some of the practical applications of operational risk management processes as well as proposing theoretical propositions for the mitigation of operational risk;
- Whilst the study focused on the UK, the findings and implications of the research have international application because Basle, as the primary regulator in this area, is an international organisation responsible for setting, and ensuring compliance with, bank regulation;
- The results of the study suggest that in some areas of operational risk mitigation the process is still 'immature'. For example, the mitigation of operational risks which span business units had no well defined and accepted process. This is an important contribution and provides the impetus for carrying out further targeted research;
- Current core practice is defined in the research, and the checklist emerging from this core practice provides practical advice and prescriptive recommendations about 'what can be done' to mitigate an operational risk exposure;
- The evidence from the study suggests that the Internal Audit role, another area which is acknowledged as being under-researched, is a crucial element in the management of operational risk. The high level review document for auditing the Operational Risk function is based on the findings of the study and contributes to the independent appraisal of the function required by Basle (2001);

- Studying the operational risk management process should assist banks to reduce their exposures and help to promote a more risk aware climate, where losses are minimised and cash flow enhanced;
- The study contributes to a better understanding of the risk management processes required and demanded under reporting initiatives, particularly in the UK context with the Turnbull (ICAEW 1999) requirements.
- Methodologically, the study increases and contributes to the growing repository of case study research programs in the generic area of risk management.

Practising managers, whether they be in Internal Audit, Risk Management or Operational Management should benefit from a number of the implications arising from the research. This in turn should lead to improvements at the organisational level as the 'firm' becomes more aware of the causes of operational risk and the potential effects that they could have if adequate mitigation plans are not put into place.

7.2 Limitations of the Research

The study itself had several limitations. The use of an *a priori* model imposed a framework on the data collection work, which may have created an artificial sense of order during the interviews. The actual process of operational risk management and mitigation may have been far more chaotic than that described. At worst this could mean some messages were lost.

Qualitative studies themselves are difficult to repeat because they are subject to so many biases. Some of these have been mentioned in the limitations of the research design (see section 3.5), for example, interviewer's bias in developing the questions. Others, such as confidentiality of the subjects, make replication of the study more difficult although there is ample opportunity to look at the problem from a different perspective.

The broad nature of operational risk means that not all contextual factors have been considered in depth. For example, the use of IT support systems to manage and mitigate operational risk was not discussed directly with the interviewees. This is, however, seen as a fruitful area for further research.

7.3 Suggestions for Further Research

There are a number of areas that the author has cited in the thesis that could usefully be examined by further research studies. The role of the operational risk manager is likely to develop as the regulatory environment becomes embedded and his relationship with the internal auditor are fruitful areas for understanding how any tensions in operational risk management are being resolved.

The use of qualitative techniques to develop the theoretical propositions concerning operational mitigation mean that further positivist research could be undertaken to generalise the findings. This generalisation could be done across the broad area of financial services in the UK and could utilise banks and building societies, which operate in similar markets, or alternatively could be done across a broader spectrum of banks. The

replication of the study in this way would provide valuable insights into how the financial service industry as a whole is tackling operational risk management and mitigation.

The establishment of operational risk units and the systems that support them are still in the early days but further work could usefully be carried out on the costs involved. How much are banks willing to spend? How was the spend thus far incurred justified? What do management perceive the expected benefits to be of their investment in operational risk management? Is the cost merely viewed as another regulatory cost?

There is an opportunity to explore further the relationship between operational risk management (the art) and operational risk measurement (the science). In theory there should be a high degree of correlation between the two, i.e. the better the management the lower the figure for quantified operational risk, and vice versa. This presents a particularly interesting opportunity for further research.

The relationship between operational risk and shareholder value presents an opportunity for further study. A capital charge for operational risk will clearly have an affect on the required rate of return and, by definition, the value that may be created or destroyed. The explicit nature of operational risk management should, in theory, improve an organisation's cash flow by reducing potential losses thus providing a direct benefit to shareholder value. Additionally, if more explicit disclosure on how operational risks are being managed are presented in the Annual Report and Accounts, then it would suggest

that the market is 'better informed' about the organisation, a fact that should be taken into account in setting the share price.

Finally, the use of IT and Decision Support Systems in operational risk management systems is an area still under development where an important contribution could be made. It is important to establish how these systems are developed in banks and other financial services organisations and to what use they are being put. The integration of a system, which is able to both 'manage' and in some way 'measure' the risks, would provide a significant step forward in the future management of operational risk.

APPENDICES

Appendix A Pensions mis-selling in the UK – a case study

(The data for this case study has been developed from three principal sources (ABI 1998, House of Commons 1998 and critical incident number 1 cited in Appendix D) and illustrates an operational risk that affected organisations which sold personal pension plans in the UK in the late 1980s/early 1990s. UK retails banks, with their insurance operations, were affected by this incident and it represents an operational risk, where the final cost has still to be identified.)

Introduction

In 1988, the personal pensions provisions of the Social Security Act 1986 came into force in the UK. This allowed employees to save for retirement themselves instead of joining either an employer sponsored or the Government sponsored pension scheme. Between 1988 and 1994, more than five million personal pensions were sold. By 1992 it had become clear that many people had bought a personal pension when this was likely to have been to their disadvantage. A fact that illustrates the 'financial ignorance' of many customers. The scale and complexity of the problem meant that the Government, the Regulators and the companies themselves all became involved in the actions that followed. These actions, which have fallen principally on the companies, have necessitated a complete review of all pension plans sold (around 650,000) since 1988 with compensation payments being made where the customer has been found to be worse off.

What were the operational risks involved?

With the benefit of hindsight, it is very easy to be wise about the operational risks that were either not identified or identified and ignored, i.e. no appropriate mitigating action was taken. From the data that has been collected on this case the following appear to be have been the key operational risks that ultimately led to the scandal being highlighted:

1. Companies involved did not comply with regulatory rules concerning the sales of these types of products;
2. The Regulator's own checks on these types of sales were ineffective;
3. Many of the salesmen involved relied heavily on commission-driven sales for their own income;
4. There was an emphasis on producing quantity of business as opposed to quality of business;
5. Supervisory controls within the organisations were ineffective in detecting inappropriate sales.

The introduction of personal pensions was widely publicised, although it was never made clear at the time, that a large proportion of those with existing pension arrangements would benefit from not transferring. This could certainly have contributed to the 'operational environment' in which these products were being sold.

Another important operational risk to emerge has been the reputational risk of the companies involved as well as the reputational risk of the whole industry sector. Only time will tell if public confidence in pension providers has been permanently dented by this debacle.

Mitigating the risks involved

Much of the work done on the pensions mis-selling review has been concerned with correcting the mistakes that were made and ensuring that no one customer is worse off now than he/she would have been had they not taken out a personal pension. Many companies have set up large Pension Review departments to tackle this task. In the meantime, business unit managers remain responsible for mitigating the operational risks involved in selling personal pension plans. The involvement of so many high profile players has meant that some mitigating actions are almost being imposed on the business unit managers. For example, the Treasury Select Committee strongly recommended giving increasing power to the Regulator, the Financial Services Authority (House of Commons 1998). This involves ensuring that the Financial Services Authority has the ability to enforce its regulation of the financial services sector (including banks) effectively and examining ways to reduce the excessive dependence on commission-based selling. These tactics are, therefore, aimed at risk reduction, specifically looking at reducing the probability of the event recurring.

The final piece of the jigsaw relates to the mitigating actions of the companies themselves. As well as being driven by the FSA, the author's research suggests that the companies are also using risk reduction as the main tactic. Steps include improving the sales training process for pensions products, enhancing monitoring procedures and providing more balanced information to the public on pensions. Given the current estimates of the likely cost of this review, £11 billion, it is one example of an operational risk that cannot be allowed to happen again.

Appendix B Case Study Protocol

1. Overview of the case study project

- ***Project objectives*** - The overall objective of the project was to examine one aspect of the risk management model, namely risk mitigation, in the context of one type of business risk, namely operational risk, within the UK retail banking industry. This led to the development of the following main research question:

  "How do UK retail banks mitigate their operational risk exposures?"

  There were a number of secondary questions to be explored:

  1. Who is responsible for operational risk mitigation?
  2. If more than one functional unit has responsibility, on what basis is the operational risk exposure assigned to the unit concerned?
  3. What tactics are considered before being used to mitigate operational risk exposures?
  4. How are those tactics established?
  5. What commonality exists across banks in their risk mitigation tactics, i.e. what may be viewed as "core" good practice?
  6. What is the process used for deciding upon the risk mitigation strategy to adopt?
  7. What is the process used to ensure that the risk mitigation decisions are adequately communicated and reported?
  8. How do banks' operational risk mitigation models compare to the theoretical models?

9. How do banks' operational risk mitigation models compare to the expectations of the Regulators?
10. What are the major barriers to implementing operational risk mitigation actions?

- ***Background information*** - A literature review of the operational risk area had been produced which, inter alia, highlighted the scarcity of previous academic research in the area of operational risk. One of the first difficulties encountered is defining the term operational risk. Other areas of risk management have been examined in more detail, for example, market risk and the application of value at risk methodologies to calculating market risk exposures, but operational risk (in the context of the financial services industry) has only recently attracted attention following some of the large scale losses that have occurred as a result of operational risk exposures. This presented some challenging opportunities to further develop theory in the operational risk area. The initial risk mitigation model proposed was drawn from decision-making theory which has been well researched and developed from an academic standpoint. The research program was self-funded by the author and there has been no sponsoring organisation.
- ***Summary of the substantive issues*** - the rationale for selecting UK retail banking was based on the literature review undertaken as a prelude to completing the research proposal. This highlighted the growth in operational risk exposures being experienced within the financial service sector generally resulting from factors such as globalisation, business climate and regulatory pressures. Whilst operational risk is a feature of many businesses there is increasing pressure on the banking sector to ensure

that adequate operational risk management procedures are in place. It was expected that UK retail banks, in particular, would have similar operational risk problems and, as such, represent a homogeneous group upon which to examine the research question. One of the expected outcomes of the research was the establishment of core practice within the selected population of UK retail banks. The risk mitigation phase of the risk management model was chosen as the focus of the research (although it was recognised that the other phases would need to be addressed) since it could be seen as representing one of the most important daily challenges facing management, i.e. how best to reduce the operational risk exposures identified by the risk management model. Risk identification, evaluation and estimation are all important phases of risk management, but unless conscious risk mitigation strategies are deployed it can all be to no avail. The research questions were examined by using a series of probing interviews with key players (see people interviewed) in operational risk management. These interviews were semi-structured and a 'template' of questions was developed to guide the process.

2. Structure of the field procedures

- ***Banks visited*** - the following UK retail banks were chosen:

Bank	Location	Contact for gaining access	Web site
Alpha	Confidential information	Confidential information	Confidential information
Beta	Confidential information	Confidential information	Confidential information
Gamma	Confidential information	Confidential information	Confidential information
Delta	Confidential information	Confidential information	Confidential information
Bank A (declined)	Confidential information	Confidential information	Confidential information
Bank B (reserve)	Confidential information	Confidential information	Confidential information
Bank C (reserve)	Confidential information	Confidential information	Confidential information
Bank D (reserve)	Confidential information	Confidential information	Confidential information
Bank E (reserve)	Confidential information	Confidential information	Confidential information

The initial list of banks was selected because they were known to represent "large" and "household" names in UK retail banking. They were, therefore, likely to have an Operational Risk Unit and an Internal Audit Department. The selected banks were approached directly (by telephone) by the author as the first step to gaining access. This was followed up by a letter enclosing a copy of the abridged research proposal and the working paper. A follow up call was made to arrange an interview when face-to-face discussions could begin, including, where necessary, a standard presentation on the research proposal.

- ***Determining the people interviewed*** - the literature review and pilot case study undertaken with Alpha bank highlighted that two of the key players in operational risk management are the Risk Management function and the Internal Audit Department. Managing operational risk is also an integral part of every operational manager's job and interviewees were, therefore, selected from these three sources. Typically the

interviewees were the Director of Audit, the Director of Risk Management, the Head of Operational Risk and two selected senior operational managers within the business units. The criteria for selecting the latter two was done in discussion with the Risk Management unit, but factors taken into account included managers from separate business, managers who have experienced recent operational risk problems (in order that critical incident techniques can be employed at the interviews), managers with above average audit ratings in the control of their operations and operational risk managers working in the business units. One of the key concerns with this type of research project is the need to ensure that absolute secrecy is maintained. This applies not only to the banks but also to the interviewees. As a result the letters of the Greek alphabet were used to disguise the names of the banks and generic titles for the interviewees were adopted, i.e. the most senior risk person has been called the Director of Risk Management throughout.

- ***Determining the other sources of information used and access problems*** - author can face difficulties of gaining access to organisations in research projects of this type. The author's personal contacts within the banking sector and the internal audit profession helped to mitigate this risk and only one of the original banks would not participate (due to impending organisational changes). A minor issue occurred with Gamma bank when the Head of Operational Risk left the organisation unexpectedly just as the interviews were being organised. Equally, the sensitivity of the information gathered during the study is recognised and all material has been personally controlled by the author, kept under lock and key and will be retained for 6 years following completion

of the work. All the information collected during the project has been maintained in a series of project files, which include data collected from the case studies.

- ***Contingency plans*** - in case of difficulties gaining access, the author made the a number of contingency arrangements to move the study forward. In the event none of these needed to be used.
- ***Resources used*** - the author carried out all the interview work in order to maintain a consistent approach throughout. Most of the transcribing of the taped interviews and all the subsequent data analysis was carried out by the author. Case study work was reviewed on an ongoing basis by the supervisors in order to ensure that the work carried out, met the high academic standards of professionalism demanded at doctoral level.

3. Case study questions

- ***The nature of the questions*** - case study questions can be classified in to 5 groupings as detailed below. It is important to structure the interview questions according to the sequence of risk mitigation events and the author utilised the risk management model to help structure the interview. In order to avoid the issue of bias, the questions were not shown to the interviewee. The principal reason for developing case study questions was to provide a tool for data collection and subsequent data analysis.
- ***Level 1 and 2 questions*** - these relate to questions to be asked of the specific interviewees (level 1) and questions about the bank itself (level 2). Some of the information relating to the bank was found in the Annual Report and Accounts, for example, policy statement on risk management. Attached as Appendix 1 is a list of the

questions discussed during the interview. Those in large type represented primary questions, whilst those in smaller type were likely to be answered during the discussion of the primary question and are, therefore, secondary questions. The text in italic represented prompts as to the sorts of answers that may be expected. The purpose of these questions was to help guide the interview and allow the interviewee to discuss openly his views on operational risk. It may, therefore, best be described as a "semi-structured interview sheet".

- ***Level 3 questions*** - these relate to the findings across the cases, i.e. banks. The starting point for these questions was the main research question together with the secondary questions. The important point was to establish emerging themes from across the case studies. (refer to section 5 for the study findings)
- ***Level 4 and 5 questions*** - the development of these questions took place once the study was nearing completion. They represent reflective questions relating to the entire study and normative questions about policy recommendations and conclusions. (refer to section 6 for the study conclusions and implications)

4. The analysis plan

- ***Outline of case study report*** - for each of the case studies undertaken a case study report was prepared (not included in this thesis document). Preparing an initial outline of the report before the field work began helped to focus the author onto the main

topics to be covered and also provided and aid to structuring the work. For composing the report, a Linear-Analytic structure[70] with the following headings was used:

1) Introduction
2) The Research Question
3) Operational Risk Management - The Theoretical Perspective
4) Research Methodology in α Bank
5) Operational Risk Management in α Bank
    - Background information on α Bank
    - Definition of Operational Risk
    - The Risk Management Framework
    - Operational Risk Mitigation
    - Examples of Operational Risk Problems
6) Relating the theory to the practice in α Bank
7) Conclusions
8) Database of accumulated evidence

A draft of the report was sent to the bank for comment and corroboration of the validity of the findings.

- ***Database of evidence*** - an important element of any case study work is the evidence that is accumulated during the field work. Such evidence was maintained in a "retrievable" database for subsequent use and analysis where appropriate. The transcripts of the interviews form a key part of this database as they are the main source of data. Other data collected both before, during and after the field work (for

[70] See "Case Study Research - Design and Methods" (1994) by Robert Yin, p.138

example relevant information from the Annual Report and Accounts and the web site) has been included in the database.

- ***Transcription and codification of data*** - following the transcription of the interviews, a coding system was used to provide a first cut analysis of the data. The coding system used was based on the research questions, any known problem areas, the theoretical framework and was focused on the area of operational risk mitigation. A preliminary code list was prepared before detailed work began and amended in the light of the experience gained during the pilot case study. Appendix 2 illustrates the high level coding used.
- ***Statistical analysis of data*** – the software package, ATLASti was used to analyse the data. This is a well-developed qualitative data analysis tool which was used to draw meaningful conclusions and develop emerging themes from the fieldwork results.
- ***Interpretation of results*** - following the data analysis, the results were examined for consistency across case studies in order that valid overall conclusions could be drawn. At this stage in the process the results were subject to a "challenge" process where rival and alternative explanations were examined. This resulted in the development of the theoretical framework and proposed model (see section 6.6).

APPENDIX 1 to Case Study Protocol

NB.

1. The questions in normal type were the main questions, whilst those in small type were supplements to the main questions
2. The type in italics were 'triggers' drawn up by the author and were used as prompts, where necessary, to try and elicit a response.

PART 1

A. What is operational risk?	**B. The Risk Management Framework**
1.Do you have a definition of operational risk? 2.Is the definition documented? 3.Who approved the definition of operational risk? *(Board, Executive Committee, Audit Committee, Risk Management Committee, Other Committee – Which?, Individual – Who?)* 4.Which areas are included in your definition of operational risk (need to provide a definition of each type)? *(Project management risks, Legal risks, Environmental risks, Compliance risks, Personnel risks, Security risks, Information system risks, Business processing risks, Business relationship risks, Customer Service risks, Strategic Planning risks, Business Interruption, Fraud, Criminal act, Other)* 5. Do you know anything about the history of operational risk and how the term came about? 6. How do you consider operational risk has been managed in the past? 7. Do you have any idea how much your company spends on managing (operational) risk? Cost of the department, training, consultants, etc.. 8. What do you think about what the Regulators are trying to do with operational risk? *(valuing operational risk, liaison with them, etc..)* 9. Does your operational risk unit have terms of Reference? Could I have a copy? 10. Do major (in terms of impact) operational risks have an owner to focus management attention? 11. Why was the operational risk unit set up and how was the structure determined?	**Risk Identification – is the process of perceiving hazards, identifying failures and recognising adverse consequences** 1. Who is responsible for identifying operational risk exposures? 2.Is this responsibility clearly laid out in their job function? 3.Describe the process by which operational risks are identified *(Physical Inspection, Check Lists, Flow Charts, Audit Reporting, Management Reporting, Incident Reporting)* 4.How frequently are these processes used? **Risk Evaluation – is the process of estimating risk probabilities, describing the risk, quantifying the risk** 5.Does the Bank evaluate operational risk exposures? 6.Who is responsible for evaluating operational risk exposures? 7.Describe the process by which operational risks are evaluated 8.Are there set criteria used to assess the exposure? 9.What data is used to evaluate the risk? 10.Are the benefits of accepting the risk examined? 11.How is the risk judged as being acceptable or otherwise? **Risk Estimation – is the process of estimating the impact of the risk, judging acceptability of the risk, comparing risks against benefits** 12.Does the bank estimate the impact of operational risk exposures?

how was the structure determined?	13.Who is responsible for estimating the impact of operational risk exposures? 14.Describe the process by which operational risks are estimated 15.Are there set criteria used to assess the impact? 16.What data is used to estimate the impact?

PART 2

A. Who mitigates Operational risk? 1.What is the organisational structure of the bank? 2.Are there clearly identifiable business units? 3.What is the level of autonomy? 4.Within this structure who mitigates operational risk? 5.What is the structure of the Risk Management Unit? 6.Do they have approved Terms of Reference? 7.Do they mitigate operational risk? 8.What is the structure of the Internal Audit Unit? 9.Do they have approved Terms of Reference? 10.Do they mitigate operational risk? 11.Are External Consultants used to mitigate operational risk? 12.Why are external consultants used? 13.Are other Internal Units used to mitigate operational risk? 14.How do the areas included in the definition of operational risk relate to the Units responsible for mitigation – who mitigates what? 15. To what extent will the Business Unit Management call upon additional support given the pressures they are under? 16.When an operational risk exposure has been identified what tactics are used to mitigate the risk? ***Avoidance (i.e. making the occurrence of the event impossible)?*** a).Under what circumstances would risk avoidance	16.How are the mitigation tactics chosen and put into action? 17.Who decides the action to be taken? 18.Why is that person/function responsible for making the decision? 19.What procedures are in place to select a course of action? (Is VAR used as part of the data for making a decision?) 20.What procedures are in place to implement a course of action? 21.How do you ensure that the mitigation tactic is working? 22.What follow-up procedures are in place? 23.Who carries out the follow-up procedures? 24.Why is that person/function responsible for carrying out the follow-up procedure? 25.If the mitigation tactic is not deemed to be working satisfactorily, what procedures are in place to correct this? 26.Does that person/function carrying out the follow-up work have the authority to enforce changes? 27.How frequently are follow up reviews undertaken? 28.What are the barriers to mitigating operational risk? *(Political barriers – Organisational inertia, Culture, Risk maturity Economic – Lack of cash, Lack of other resources, Impact on the bottom line Ignorance – Staff training, Inadequate communication about risk exposures, "It will not happen to us" syndrome, Unaware of possible options, Other – Practicality of the tactic*

be used? b)Establish the type of risks that are/have been mitigated in this way (e.g. deliberately withdrawing from a market because the operational risks involved are considered to be too great) ***<u>Reduction/Suppression</u> (i.e. reducing the likelihood of the occurrence of the event and/or reducing the eventual loss?)*** a)Under what circumstances would risk reduction/suppression be used? b)Establish whether the following tactics are used: *(Improving internal control procedures, Redesigning the processes involved, Training, Separation of Personnel, Ongoing monitoring (audit/compliance reviews), Improved reporting systems, External advice, Improving quality standards)* ***<u>Assumption/Retention</u> (i.e. accepting the likelihood of the occurrence of the event and undertaking no mitigating actions)?*** a) Under what circumstances would risk assumption/retention be used? Is there a monetary limit used to guide the decision? b)Establish the type of risks that are/have been mitigated in this way (e.g. level of loss and probability of occurrence is considered to be low) ***<u>Insurance</u> (i.e. accepting the likelihood of the occurrence of the event but reducing the eventual loss by transferring the risk)?*** a)Under what circumstances would insurance be used? b)Establish the type of risks that are/have been mitigated in this way (e.g. business interruption risks frequently are insured) ***Combinations (of the above techniques)?*** a)Under what circumstances would a combination of techniques be used? b)Establish the type of risks that are/have been mitigated in this way (e.g. risks mitigated through the establishment of a captive insurance company) ***Other?*** a)Under what circumstances would a other techniques be used?	*involved, Effect on the internal organisation – resistance to changing practices, Effect on the external environment – reputation could be harmed, Government regulations, Monitorability of the required action, Required action not deemed to be effective in the timescale involved, for example, because of changing environmental circumstances)* **<u>B. Discuss a recent example of an operational risk problem</u>** 1.Who was involved in the discussions about how to solve it? 2.What actions were considered to mitigate the risk? 3.Who decided on what action to take? 4.Why did that person decide? 5.Why were certain items rejected? 6.How successful has the mitigation action been? 7.How was it followed up? 8.How representative is this incident of the risk mitigation process within the business? 9.Do you have any other examples of where the risk mitigation action was different? 10.Why was a different action chosen? NB. Discuss pensions review as a fallback example

b)Establish the type of risks that are/have been mitigated in this way	

APPENDIX 2 to case study protocol

Operational Risk Case Studies - Coding System

AREA	CODE	NOTES
Internal Organisation	**IO**	
IO: Operational Risk Definition	IO-ORD	Definitions of operational risk that are used by the Banks
IO: Operational Risk Areas	IO-ORA	Areas that are included within the definition
IO: Risk Management Structure	IO-RMS	Comments/perceptions relating to the Bank's risk management structure
IO: Risk Management Policy	IO-RMP	Comments/perceptions relating to the Bank's risk management policy
IO: Organisational Structure	IO-OS	Comments/perceptions relating to the Bank's organisational structure
IO: General Information	IO-GI	General information about the Bank/risk management that helps to put the study into context
IO: Training	IO-TRAIN	Comments related to risk management training within the organisation
IO: Risk Strategies	IO-STRAT	Current strategies for dealing with risk management within the organisation
IO: Database	IO-DBASE	Information relating to the use of a risk management (incident) database within the organisation
Operational Risk Identification	**RI**	
RI: Responsibility	RI-RESP	Comments on responsibility for operational risk identification
RI: Process	RI-PRO	Information on the sequence of events that lead to operational risks

		being identified
Operational Risk Evaluation	**REV**	
REV: Responsibility	REV-RESP	Comments on responsibility for operational risk evaluation
REV: Process	REV-PRO	Information on the sequence of events that lead to operational risks being evaluated
REV: Data	REV-DATA	Types of data used in the operational risk evaluation process
REV: Quantification	REV-QUAN	Information on the use of quantitative risk measurement techniques
REV: Judgement	REV-JUDGE	Indications of the ways of thinking that caused a decision on operational risk evaluation to be made
Operational Risk Estimation	**RES**	
RES: Responsibility	RES-RESP	Comments on responsibility for operational risk estimation
RES: Process	RES-PRO	Information on the sequence of events that lead to the impact of the operational risks being estimated
RES: Data	RES-DATA	Types of data used in the operational risk estimation process
RES: Judgement	RES-JUDGE	Indications of the ways of thinking that caused a decision on operational risk estimation to be made
Operational Risk Mitigation	**RM**	
RM: Business Units	RM-BU	Comments on the Business Unit role in operational risk mitigation
RM: Internal Audit	RM-IA	Comments on Internal Audit role in operational risk mitigation
RM: Risk Management	RM-RM	Comments on Risk Management role in operational risk mitigation
RM: External Consultants	RM-EC	Comments on External Consultants role in operational risk mitigation
RM: Other Units	RM-OU	Comments on role of other internal units in operational risk mitigation
RM: Interfaces	RM-INTER	Information describing the collective way in which operational risk is

		mitigated
RM: Barriers	RM-BAR	Information on the barriers to mitigating operational risk
RM: Critical Incidents	RM-CRI	Reported incidents on operational risk

Operational Risk Mitigation Tactics	**TAC**	
TAC: Avoidance	TAC-AVOID	Evidence to support avoidance being used as an operational risk mitigation tactic
TAC: Reduction/Suppression	TAC-RED	Evidence to support reduction/ suppression being used as an operational risk mitigation tactic
TAC: Assumption/Retention	TAC-ASS	Evidence to support assumption/ retention being used as an operational risk mitigation tactic
TAC: Insurance	TAC-INS	Evidence to support insurance being used as an operational risk mitigation tactic
TAC: Combination	TAC-COMB	Evidence to support a combination of the above being used as an operational risk mitigation tactic
TAC: Other	TAC-OTHER	Evidence to support other techniques being used as an operational risk mitigation tactic

Operational Risk Mitigation Procedures	**PROC**	
PROC: Decision Maker	PROC-DM	Comments on who decides on the course of action to be taken when an operational risk is being mitigated
PROC: Selection process	PROC-PRO	Information relating to the process of selecting a suitable mitigation tactic
PROC: Implementation	PROC-IMP	Information relating to the process used in implementing a selected mitigation tactic
PROC: Corrective Action Tracking	PROC-CAT	Information related to the subsequent follow-up of implemented operational risk mitigation decisions

General	**GEN**	
GEN: Quotations	GEN-QUO	Noteworthy quotations for possible use in the report

GEN: Regulators	GEN-REG	Comments related to the Regulators including their role in operational risk management
GEN: Report	GEN-REP	Items for possible inclusion in the report

Critical Incidents	**CI**	
DEC: Decision Maker	CI - DEC	Information about the decision maker in the critical incident
ACT: Action	CI -ACT	Information concerning the action taken in the critical incident

Appendix C Example of Operational Risk Assessment form

The form below has been adapted from one given to the author by Gamma bank. It illustrates the data that is captured as part of the overall assessment of the operational risk, and is, therefore, and integral part of the operational risk mapping process The phases proposed in the research model (see section 6.6) have been related to the form and it may be noted that there is a close fit in terms of information collected. Comments have been made against each phase to highlight any issues.

Business Unit		*Location*	

IDENTIFICATION – source of risk not specified

Process	
Risk Description *Top 10 risks*	
Risk Category *Risk Sub-category*	
Risk Definition	(1) The risk includes…….. (2) The defined level at which the risk will have a significant impact is…….

DIAGNOSIS – cross linkage to other business units not specified

Potential effect	
Previous examples of risk	
Potential financial impact	(using scale)
Likelihood of risk occurring	(using scale)
Factors contributing to risk	
Preventative controls in place	
Detective controls in place	
Control Assessment	Fully adequate? Adequate?

	Inadequate?

MITIGATION

SELECTION and IMPLEMENTATION – action plan should detail who is involved, when follow-up should take place and any monitoring of the action/risk that should take place

Action plans for increased mitigation	
Responsibility	

Appendix D Critical Incidents

This Appendix provides a summarised analysis of the critical incidents discussed during the interviews. A brief description of the columns is given below:

Description of incident – the name of the incident together with a short sentence describing what happened
Type of operational risk – the category of operational risks that are involved
Incident sensitivity – private indicates that the incident has remained within the confines of the bank whereas public means the has appeared at some time in the public domain
Supporting information – supporting information relates either to the incident or to the subsequent action. The type of supporting information available is quoted although this has not always been seen (mainly due to the sensitivity of what is involved), and for the most part the incident has been analysed using the interview material
How identified – answers the question how was the incident picked up
Mitigation tactic – identifies which of the four mitigation tactics, take, terminate, transfer and treat were used to mitigate against future occurrences of the risk
Notes on mitigation – additional information related to the mitigation action

No.	Description of incident	Type of operational risk	Incident sensitivity	Supporting information	How identified	Mitigation tactic	Notes on mitigation
1	**Pensions mis-selling** – bad advice given to customers persuaded to buy a personal pension (see also Appendix A)	Compliance, sales practices	In public domain (industry event)	Press reports, Government reports, Industry reports, internal documents	Customer	Treat	Mitigation took place at industry and company level
2	**Foreign exchange dealer** – trader ran up sizeable book and withheld information	Rogue trader, segregation of duties	Private to the bank	Not known	Informal networking	Treat	Undisclosed steps taken to improve the control system
3	**Telephone banking operation** – identification of lack of contingency planning	Business continuity	Private to the bank	Location of second operation	Recognised by Management	Treat	Service is switched between the two operations on a regular basis

	arrangements						
4	**EMU** – payments were being mis-routed by correspondents in the old national currency	Payment, HR performance	Private to the bank	Internal documents believed to be available	Internal control procedures	Treat	Mitigation of this risk has provided important lessons for possible UK entry into EMU
5	**Book of transaction transferred** – errors in trades discovered following transfer of book	Transaction error	Private to the bank	Internal documents believed to be available	Internal control procedures	Take or treat	A cost benefit analysis was being undertaken to decide whether assume the risk (and do no further work) or correct all the deals
6	**Joint venture finance company** – systems was unable to cope with (underestimated) business volumes	Systems adequacy, customer service	In public domain	Press reports	Customer complaints	Treat	Competetitors were able to learn from this incident and avoid making the same mistake
7	**Electronic payments system** – clerks/managers had the ability to input instructions and release funds	Segregation of duties, coercion	Private to the bank	Not known	Risk review	Treat and take	Whilst segregation of duties was introduced, the coercion risk was accepted as a low probability
8	**Insurance operation** – a catalogue of 'bad management' practices was found	Compliance, sales practice	Initially private then in public domain	Press reports	Regulators	Treat	A complete recovery program was set up as well as regulatory fines being imposed
9	**Uncleared effects** – cash being drawn on cheques which have not cleared	External Fraud	Private to the bank	Not known	Management information - losses began to rise	Treat	Mitigation was an iterative process as those involved continued to find more ways to beat the system
10	**Office fire** – fire occurred but the business continuity plan did not work.	Physical security, business continuity	Private to the bank	Internal documents believed to be available	Member of staff	Treat	Mitigation now involves testing the business continuity arrangements
11	**Incorrect payment remittance** – despite supervisory controls in place to prevent this happening, poor training and communication caused large payment error	Payment error, HR skills	Private to the bank	Internal documents believed to be available	Customer contact	Treat and take	Training risk had been identified and assumed for a short period but manifestation of payment risk brought forward the action plan

12	**Mainframe unavailability** – several instances of hardware/software being unavailable	Systems availability	Private to the bank	Internal documents believed to be available	Mainframe malfunction	Treat	Ongoing incidents are investigated and the risk and risk mitigants re-assessed
13	**Money laundering** – breakdown in the control environment enabled money to be laundered	Money laundering	Private to the bank and the banking industry	Not known	Industry process	Treat	Controls had to be improved to protect the bank against any further incidents
14	**Account limit excess** – series of controls had lapsed enabling member of staff to set a large excess on his account	Internal fraud	Private to the bank	Internal documents believed to be available	Not known	Treat	Control framework had to be re-established
15	**Pension fund administration** - unable to provide adequate service following large increase in volumes resulting from ambitious strategy	Systems adequacy, customer service	Private to the bank	Not known	Customer complaints	Terminate and treat	Risk initially avoided by stopping new business whilst more robust infrastructure was put in place
16	**PBX voice switch** – phone network was hacked as a result of (intentional) changes made to voice switch which left the system exposed	External fraud, systems security	Private to the bank (but believed to occur elsewhere)	Internal documents, Internet material on switch hacking	Management information – call charges increased	Treat	Project team was established to resolve this issue as a number of external parties were involved.
17	**PEP launch** - unable to cope with (underestimated) business volumes	Systems adequacy, customer service	Private to the bank	Not known	Customer complaint	Treat	A number of mechanisms have been put in place to reduce the impact but a residual risk still remains
18	**Deed store** – halon gas fire prevention system found to be inoperative	Physical security	Private to the bank	Location of problem	Competitor suffered a deed fire	Treat	Lack of communication meant that this risk had been unwittingly assumed. Major work now in place to install new system
19	**Call centre** - identification of lack of contingency planning arrangements	Business continuity	Private to the bank	Internal documents believed to be available	Management concern	Treat (being considered)	Risk still exists and a number of options are being considered

Appendix E High level review document for auditing the Operational Risk function

Audit objectives: To evaluate and assess the effectiveness of the Operational Risk Function (ORF)

1. *Organisation*
   - 1.1 Establish the nature of the organisational arrangements (e.g. organisational chart) for the ORF?
   - 1.2 Does the (corporate) ORF have a clear reporting line into the Risk Director?
   - 1.3 Does the (Business Unit) ORF have a clear reporting line into senior management in the Business Unit?
   - 1.4 Describe the organisational links between the corporate ORF and the Business Unit ORFs? How does the relationship guarantee that the corporate ORF is made aware of all important operational risk matters?
   - 1.5 Are the ORFs adequately staffed? – review the experience and qualifications of those involved.
   - 1.6 Are Operational Risk committees used to monitor the operations of the ORFs? Review the minutes for completeness and ensure that action points are followed.

2. *Objectives*
   - 2.1 Are the objectives of the (corporate) ORF clearly defined and documented?
   - 2.2 Do they cover the main functions of an ORF? – policy making, risk-mapping, reporting arrangement, quantification, training, and so on
   - 2.3 Have the objectives been formally approved by the Risk Committee/Board?

3. *Planning*
   - 3.1 How is the work of the ORF planned in order to achieve their stated objectives?
   - 3.2 Are there adequate resources in place to achieve the plan?
   - 3.3 Is there a process is in place to review the achievement of the plan?
   - 3.4 Describe the action taken when changes to the plan are required – how are priorities established?
   - 3.5 How successful has the ORF been in achieving the plan?

4. *Processes*
   - 4.1 Does the ORF use a (documented) risk-mapping approach?
   - 4.2 Describe the risk-mapping approach and, in particular, the methods used to capture data on risks – do they appear sufficient?
   - 4.3 Does the risk-mapping approach cover the main phases of the risk management process – identification, appraisal (probability/impact) and mitigation?
   - 4.4 Does the risk-mapping approach extend to all areas of the bank?
   - 4.5 How is the documentation maintained up-to-date?

4.6 Are there sufficient controls within the framework to ensure the resultant output is robust (particularly management controls – this is a particularly important point as the process is subjective)?
4.7 Is a loss/incident database maintained?
4.8 How is the data collected?
4.9 Has a methodology for quantifying operational risk been adopted? Describe the methodology used and ensure it is in line with the requirements of the Regulators?
4.10 How robust is the quantification methodology and do the results appear consistent with the views of management?

5. ***Reporting***
5.1 Does the ORF produce reports on a regular basis?
5.2 Do the reports include a summary of key risks and key risks indicators for monitoring levels of operational risk?
5.3 Describe the action management take on the reports where there is an unsatisfactory situation noted – does it appear sufficient?

Appendix F Checklist for mitigating operational risks

Proactive risk management (risk has not materialised)

1. Has the risk been adequately diagnosed?
   - Related to business unit objectives?
   - Adequately described
     a) Risk category
     b) Scale of risk
     c) Cross linkage to other risks
   - Probability assessed?
   - Impact assessed?
   - Current mitigants noted?

2. Assess whether it is feasible to implement any mitigation actions
   - Should the risk be accepted? If so, why?
   - Should the risk be accepted in the short term? If so, why?
   - If the risk is to be accepted should the risk be re-reviewed at a later date? If so, when?
   - Should the risk be avoided completely? If so, why?

3. Assess the action that may be taken to reduce the impact and/or probability
   - Has a draft cost/benefit analysis been completed and checked for accuracy? If not, why not? Who needs to authorise the expenditure?
   - For operational risks where the impact is high but the probability is low establish whether transferring part of the impact via insurance is feasible. If not, why not?
   - Establish the desired level of risk that the organisation wishes to accept and the current level that has been established though the probability/impact appraisal. How much work is likely to be involved in removing the 'gap' between the two? Can the work involved to close the 'gap' be managed within the business unit (see point 4 below)? Is a project team required to complete the work (see point 5 below)?

4. Assess whether the mitigation work can be managed within the Business Unit
   - Should additional 'expertise' be used to help mitigate the risk? If not, why not?
   - Establish the action required to reduce the impact/probability (typically this would involve improving the internal control system)? For example, is more documentation required, are more resources required, is more training required, are more supervisory checks required, is a better segregation of

duties required, does management reporting need to be enhanced, can other units be involved to share the risk and so on?
- Establish and document an action plan to effect the necessary changes. Who will be responsible for ensuring the action is carried out?

5. Assess whether the mitigation work needs to be managed by establishing a project team
   - Establish the project team and appoint the project manager
   - Agree the terms of reference and develop the project plan
   - Establish a reporting mechanism to keep Business Unit management informed of the progress of the mitigation actions

6. Monitor the progress of the action plans
   - Ensure regular progress reports vis-à-vis the achievement of the action/project plans are in place. If they aren't, what is the justification for this?
   - Ensure follow up procedures are in place to take action when progress is considered to be unsatisfactory. Implement procedures as appropriate.
   - When the work is complete, re-appraise the impact/probability in the light of the improvements made and ensure the residual risk is acceptable.
   - Update the risk map accordingly.

Reactive risk management (risk has materialised)

1. Examine the diagnosis of the risk – had it been identified? If so, review:
   - Relationship to business unit objectives?
   - Adequacy of description
     a) Risk category
     b) Scale of risk
     c) Cross linkage to other risks
   - Adequacy of probability assessment?
   - Adequacy of impact assessment?
   - Adequacy of current mitigants?

2. Update the loss database with details of the incident that took place.
   - What event(s) caused the risk to materialise?
   - How much direct and indirect loss is involved?
   - What are the key lessons to be learned?
   - Who needs to know about the incident? Prepare a report as necessary.

3. Assess whether it is feasible to implement any additional mitigation actions
   - Should the risk be accepted and no further action taken? If so, why?

- If the risk is to be accepted should the risk be re-reviewed at a later date? If so, when?
- Given the reasons why the incident happened, is it feasible to avoid the risk completely in the future? If so, why?

4. Assess the action that may be taken to reduce the impact and/or probability and prevent future occurrences
   - Has a draft cost/benefit analysis been completed and checked for accuracy? If not, why not? Who needs to authorise the expenditure?
   - Is there scope for using insurance to transfer part of the impact. If not, why not?
   - Review the causes of the incident and assess the additional work required to mitigate the risk down to an acceptable level. How much work is likely to be involved? Can the work involved be managed within the business unit (see point 5 below)? Is a project team required to complete the work (see point 6 below)?

5. Assess whether the mitigation work can be managed within the Business Unit
   - Should additional 'expertise' be used to help mitigate the risk? If not, why not?
   - Establish the action required to reduce the impact/probability (typically this would involve improving the internal control system)? For example, is more documentation required, are more resources required, is more training required, are more supervisory checks required, is a better segregation of duties required, does management reporting need to be enhanced, can other units be involved to share the risk and so on?
   - Establish and document an action plan to effect the necessary changes. Who will be responsible for ensuring the action is carried out?

6. Assess whether the mitigation work needs to be managed by establishing a project team
   - Establish the project team and appoint the project manager
   - Agree the terms of reference and develop the project plan
   - Establish a reporting mechanism to keep Business Init management of the progress of the mitigation actions

7. Monitor the progress of the action plans
   - Ensure regular progress reports vis-à-vis the achievement of the action/project plans are in place. If they aren't, what is the justification for this?
   - Ensure follow up procedures are in place to take action when progress is considered to be unsatisfactory. Implement procedures as appropriate.
   - When the work is complete, re-appraise the impact/probability in the light of the improvements made and ensure the residual risk is acceptable.
   - Update the risk map accordingly

BIBLIOGRAPHY

Acs, J. (1985): "A Comparison of Models for Strategic Planning, Risk Analysis and Risk Management", *Theory and Decision*, 19, pp 205 - 248

Adams, J. (1998): "Risk Management is a Balancing Act," *Association for Project Management*, February, pp 18 - 19

Adams, M.B. (1994): "Agency Theory and Internal Audit", *Managerial Auditing Journal*, Vol 9, No 8, pp 8 – 12

Allott, A. (1996): "The Emerging Role of the Internal Audit," *Management Accounting*, January Vol.74 No.1, pp 60 - 62

Anghern, A.A. and Jelassi, T. (1994): "DSS Research and Practice in Perspective", *Decision Support System*, Vol 12, pp 267 – 275

Arlington (1998): *History of Decisions Making*, Arlington Software, available http://benli.bcc.bilkent.edu.tr/~omer/downloads/dec_analy/history.html

Asif, S. and Sargeant, A. (2000): "Modelling internal communications in the financial services sector", *European Journal of Marketing*, Vol 34, No 3/4, pp 299 – 317

Association of British Insurers – ABI (1998): Parliamentary Briefing on Pensions Mis-selling, available http://www.abi.org.uk/INDUSTRY/market/PboPMs//PboPMs.asp

Augustine, N.R. (1995): "Managing the Crisis you Tried to Prevent", *Harvard Business Review*, March-April, pp 147 - 158

Bacharach, S.B. (1989): "Organisational Theories: some criteria for evaluation", *Academy of Management Review*, Vol 14, No 4, pp 496 – 515

Bailey, A.D., Preston McAfee, R. and Whinston, A.B. (1981): "An Application of Complexity Theory to the Analysis of Internal Control Systems", *Auditing: A Journal of Practice and Theory*, Vol 1 No 1, pp 38 – 52

Baird, I.S. and Thomas, H. (1985): "Toward a contingency model of strategic risk taking", *Academy of Management Review*, Vol 10, No 2, pp 230 – 243

Bandyopadhyay, K., Myktyn, P.P. and Myktyn, K. (1999): "A framework for integrated risk management in information technology", *Management Decision*, Vol 37, No 5, pp 437 – 444

Bank of England (1983): "Revised Presentation of Banking Statistics", *Bank of England Quarterly Bulletin*, December, pp 562 - 563

Bank of England (1991): "Bank Groupings in statistical presentations", *Bank of England Quarterly Bulletin*, February, pp 99 - 100

Barnard, J. (1992): "Successful CEOs talk about decision making", *Business Horizons*, September-October, pp 70 – 74

Basi, R.S. (1998): "Administrative decision making: a contextual analysis", *Management Decision*, Vol 36, No 4, pp 232 – 240

Basle (2001): "New Basle Capital Accord – Consultative Document", *Basle Committee on Banking Supervision*, January

Basle (1998a): "Operational Risk Management", *Basle Committee on Banking Supervision*, September

Basle (1998b): "Framework for Internal Control Systems in Banking Organisations", *Basle Committee on Banking Supervision*, September

Beck, U. (1992): "From Industrial Society to Risk Society", *Theory, Culture and Society*, Vol 9, No 1, pp 97 – 123

Bell, D.E. and Onillon, P.A.(1992): "Don't Put Your Competitive Advantage at Risk", *Risk Management Reports*, May/June (Vol.19, No.3), pp 13 - 24

Benjamin, C.O., Lu, C. and de Neufville, R. (1995): "Classifying risks on Information Technology Projects," *Engineering Management Journal*, December Vol 7 No 4 pp 45 – 54

Benbasat, I, Goldstein, D.K. and Mead, M. (1987): (The Case Research Strategy in Studies of Information Systems," *MIS Quarterly*, September, pp 369 – 386

Bernstein, P.L. (1996): "The New Religion of Risk Management", *Harvard Business Review*, March-April, pp 47 - 51

Beroggi, G.E.G. and Wallace, W.A. (1994): "Operational Risk Management: A new paradigm for decision making", IEEE Transactions on Systems, Management and Cybernetics, Vol 24, No 10, October, pp 1450 - 1457

Betts, A., Meadows, M. and Walley, P. (2000): "Call centre capacity management", *International Journal of Service Industry Management*, Vol 11, No 2, pp 185 – 196

Blacker, K. (1998): "Operational Risk for Financial Services – A review of the Literature", *The International Journal of Project and Business Risk Management*, Vol.2 Issue 3, pp 291 - 306

Blacker, K. (2000): "Mitigating Operational Risk in British Banks", *Risk Management: An International Journal*, Vol 2, No 3, pp 23 – 33

Bonoma, T.V. (1985): "Case Research in Marketing", *Journal of Marketing Research*, Vol XXII, May, pp 199 – 208

Boyle, E.J. (1993): "A Framework for the Modern Internal Audit Function", *Advances in Management Accounting*, pp 227 – 254

Brigley, S. (1995): "Business Ethics in Context: Researching with Case Studies", *Journal of Business Ethics*, Vol 14, pp 219 – 226

Brindle, M. (1999): "Games decision makers play", *Management Decision*, Vol 37, No 8, pp 604 – 612

British Banking Association and PriceWaterhouseCoopers – BBA (1999a): *Operational Risk Management: The New Frontier*, October 1999

British Banking Association - BBA (1999b): Statistics – Branches and ATMs, available http://www.bba.org.uk/html/1773.html

British Banking Association - BBA (1999c): *Operational Risk Data Pooling*, available http://www.bba.org.uk/asp/docShow.asp?docID=1179

British Banking Association and Coopers and Lybrand - BBA (1997): *Survey of Operational Risk*, May 1997

Broadbent, M. (1999): *Measuring Business Performance*, London: The Chartered Institute of Management Accountants

Brown, B.M.J. (1992): *Allfinanz without limits*, Dublin: Lafferty Publications

Buchanan, M., Iyer, R. and Karl, C.A. (1999): *The Case Study in Business Research*, available http://www.ozemail.com.au/~bechervaise/DBAR3.htm

Burton, P. (2000): "Antecedents and Consequences of Corporate Governance Structures", *Corporate Governance: An International Review*, Vol 8, No 3, July, pp 194 - 203

Cadbury Report (1992): *Financial Aspects of Corporate Governance*, The Committee on Financial Aspects of Corporate Governance, London: Gee
Cade, E.C. (1997): *Managing Banking Risks*, Cambridge: Woodhead

Cavaye, A.L.M. (1996): "Case study research: a multi-faceted research approach for IS,"

Information Systems Journal, Vol 6 pp 227 – 242

Caruana, A. and Calleya, P. (1998): "The effect of internal marketing on organisational commitment among retail bank managers", *International Journal of Bank Marketing*, Vol 16, No 3, pp 108 – 116

Chapman, C. and Ward, S. (1996): *Project Risk Management*, London: Wiley

Cheaney, N. (2000): "The Practicalities of Implementing an Operational Risk Model", *Presentation to the Operational Risk Research Forum*, July, London

Chell, E. (1998): "Critical Incident Technique", in Symon, G. and Cassell, C. (eds) *Qualitative Methods and Analysis in Organisational Research*: A Practical Guide, London : Sage

Chenail, R.J. (2000): "Navigating the Seven C's: Curiosity, Confirmation, Comparison, Changing, Collaborating, Critiquing and Combinations," *The Qualitative Report*, March Vol 4, Nos 3 and 4, available http://www.nova.edu/ssss/QR/QR4-3/sevencs.html

Coffey, A. and Atkinson, P. (1996): *"Making Sense of Qualitative Data"*, California: Sage

Colbert, J.L. and Alderman, C.W. (1995): "A risk-driven approach to the internal audit", *Managerial Auditing Journal*, Vol 10, N0 2, pp 38 – 44

Committee of Sponsoring Organisations of the Treadway Commission – COSO (1992): *Internal Control – Integrated Framework*, September

Comptroller of the Currency (1997): *Remarks by Eugene A. Ludwig, Comptroller of the Currency before the FFIEC Conference on Regulatory Capital, Washington, D.C.,* News Release dated 12/12/97

Comptroller of the Currency (1998a): *Technology Risk Management,* OCC Bulletin dated 4/2/98

Comptroller of the Currency (1998b): *Technology Risk Management: PC Banking,* OCC Bulletin dated 24/8/98

Comptroller of the Currency (1998c): *Interpretive Letter #845 to Ms. Karol K. Sparks, November 1998, 12 U.S.C. 24(7),* letter dated 20/10/98

Covello, V.T., Von Winterfeldt, D. and Slovic, P. (1987): *"Communicating Scientific Information About Health and Environmental Risks: Problems and Opportunities from a Social and Behavioural Perspective"*, pp 221 – 240 in Covello, V.T. et al, *Uncertainty in Risk Assessment, Risk Management and Decision Making*, New York: Plenum Press

Cox, S.J. and Tait, N.R.S. (1991): *Reliability, Safety and Risk Management – an Integrated Approach*, Oxford: Butterworth-Heinemann

Crawford, D.B. (2000): "Levels of Control", *Internal Auditor*, Vol 57, No 5, October pp 42 –45

Crick, W.F. and Wadsworth, J.E. (1958): *A Hundred Years of Joint Stock Banking*, London: Hodder and Stoughton

Crook, D. (2000): "Whistleblowing Update", *Presentation to the Institute of Internal Auditors South West District*, Yatton, Bristol (October)

Cruickshank, D. (1999): *Competition in UK Banking: A report to the Chancellor of the Exchequer*, Norwich: The Stationery Office

Cunnington, T. (1999): "Moving Internal Audit to the forefront of risk management as part of a corporate risk management strategy", *Proceedings of the Internal Audit and Business Risk Conference 1999*, Amsterdam (November)

Dale R. (1994): "Regulating Investment Business in the Single Market," *Bank of England Quarterly Bulletin*, November pp 333 - 340

Darke, P., Shanks, G. and Broadbent, M. (1998): "Successfully completing case study research: combining rigour, relevance and pragmatism," *Information Systems Journal*, Vol. 8 pp 273 – 289

Dembo, R.S. and Freeman, A. (1998), *Seeing Tomorrow- Rewriting the Rules of Risk*, New York: Wiley

Denzin, N.K. and Lincoln, Y.S. (1998): *"Entering the Field of Qualitative Research"* pp 1 – 45 in Denzin, N.K. and Lincoln, Y.S. Ed, *Collecting and Interpreting Qualitative Materials*, California: Sage

Devlin, J.F. (1995): "Technology and innovation in retail banking distribution", *International Journal of Bank Marketing*, Vol 13, No 4, pp 19 – 25

Dey, I. (1993): *Qualitative Data Analysis*, London: Routledge

DiMaggio, P.J. (1995): "Comments on 'What Theory is *Not*'", *Administrative Science Quarterly*, Vol 40, pp 391 – 397

Dowd, K. (1998): *Beyond Value at Risk*, Chichester: Wiley

Drucker, P. (1997): "Looking Ahead: Implications of the Present", *Harvard Business*

Review, September – October 1997, pp 18 – 24

Drummond, H. (1992): "Another Fine Mess: Time for Quality in Decision-Making", *Journal of General Management*, Vol 18, No 1 pp 1 - 14

Ealy T.V. (1993): "Bringing Risk Management into the Boardroom", *Risk Management*, April pp 30 -37

Easterby-Smith, M., Thorpe, R. and Lowe, A. (1991): *Management Research - an Introduction*, London: Sage

Economist (2001): "Stronger foundations", available http://www.economist.com/displayStory.cfm?Story_ID=478861

Eierman, M.A. et al (1995): "DSS Theory: A model of constructs and relationships", *Decision Support Systems*, Vol 14, No 1, pp 1 - 26

Eisenhardt, K.M. (1989): "Building Theories from Case Study Research", *Academy of Management Review*, 989, Vol 14, No 4, pp 532 - 550

Eisner, E. (1991): *The Enlightened Eye*, New York: Macmillan

Engemann, K.J. and Miller, H.J. (1992): "Operations Risk Management at a Major Bank", *Interfaces*, Vol 22/6, November - December 1992, pp 140 – 149

Erlandson, D.A., Harris, E.L., Skipper, B.L. and Allen, S.D. (1993): *Doing Naturalistic Inquriy: a guide to methods*, California: Sage

European Confederation of Institutes of Internal Auditors – ECIIA (1999): *The Internal Auditor's Role in the Prevention of Fraud*

Fayol, H. (1949): *General and Industrial Management*, London: Pitman

Felix Jr, W.L., Gramling, A.A., and Maletta, M.J. (1999): "Internal vs External Audit", *Internal Auditing*, July

Fenlon, A. (1999): "How management can learn from chaos", *Financial Focus* (published by the Faculty of Finance and Management of the Institute of Chartered Accountants in England and Wales), Issue 48, February, pp 1 – 2

Fiegenbaum, A. and Thomas, H. (1988): "Attitudes towards risk and the risk-return paradox: prospect theory explanations", *Academy of Management Journal*, Vol 31, No 1, pp 85 – 106

Flint, D. (1998): *Philosophy and Principles of Auditing*, Basingstoke: MacMillan

Fontana, A. and Frey, J.H. (1998): *Interviewing: The Art of Science,* pp 47 – 78 in Denzin, N.K. and Lincoln, Y.S. Ed, *Collecting and Interpreting Qualitative Materials*, California: Sage

Friedlob, G.T. and Scheifer, L.L.F. (1999): "Fuzzy logic: application for audit risk and uncertainty", *Managerial Auditing Journal*, Vol 14, No 3, pp 127 – 135

Froot, K.A., Scharfstein, D.S. and Stein, J.C. (1994): "A Framework for Risk Management", *Harvard Business Review*, November - December, pp 91 -102

Gable, G.G. (1994): "Integrating Case Study and Survey Research Methods: An example in Information Systems", *European Journal of Information Systems*, Vol 3 No 2 pp 112 – 126

Gall, M.G., Borg, W.R. and Gall, J.P. (1966): *Educational Research: An Introduction (6^{th} edition)*, White Plains, NY: Longman

Gandy A. (1997): "Balancing Act: High Tech Solutions to Operational Risk", *Chartered Banker*, January, pp 14 -15

German, P. and Robinson, R. (1998): "Assessment of Operational Risk for North Atlantic Pipeline", *Offshore*, February, Vol. 58, no. 2, pp 50 - 52

Gill, J. and Johnson, P. (1997): *Research Methods for Managers (2^{nd} edition)*, London: Paul Chapman

Giglioni, G. and Bedeian, A. (1974): "A Conspectus of Management Control", *Academy of Management Journal*, Vol 17 No 2, pp 292 - 305

Glazer, R., Steckel, J.H. and Winer, R.S. (1992): "Locally Rational Decision Making: The Distracting Effect of Information on Managerial Performance", *Management Science*, Vol 38, No 2, pp 212 - 226

Gordon, L.A., Miller, D. and Mintzberg, H. (1975): *Normative Models in Managerial Decision-Making, New York*: National Association of Accountants and Ontario: The Society of Industrial Accountants of Canada

Gordon, P.J. (1997): "Ten Strategic Audit Questions", *Business Horizons*, Vol 40, No 5, pp 7-14

Gray, I. (1984): *General and Industrial Management - Revised edition Henri Fayol*, London: Pitman

Gray, I. and Manson, S. (1989): *The Audit Process*, London: Van Nostrand Reinhold (International) Co. Ltd.

Greenland, S.J. (1995): "Network management and the branch distribution channel", *International Journal of Bank Marketing*, Vol 13, No 4, pp 12 – 18

Gregory, R. and Lichtenstein, S. (1994): "A Hint of Risk: Tradeoffs Between Quantitative and Qualitative Risk Factors", *Risk Analysis*, Vol 14, No 2, pp 199 – 206

Grobstein, M. and Craig, P.W. (1984): "A Risk Analysis Approach to Auditing", *Auditing: A Journal of Practice and Theory*, Vol 3 No 2, pp 1 – 16

Groth, J.C. (1992): "Common-sense Risk Assessment", *Management Decision*, Vol. 30, No 5, pp 10 - 16

Guba, E.G.. and Lincoln, Y.S. (1994): "*Competing Paradigms in Qualitative Research*" pp 105 – 117 in Denzin, N.K. and Lincoln, Y.S. (Eds), *Handbook of Qualitative Research*, California: Sage

Guerrier, G.L. (1997): "Challenging the Transaction Costs Theory in the Distribution of Complex Industrial Products: an Exploratory Research", DBA Thesis, Brunel University, February

Gummesson, E. (2000): *Qualitative Methods in Management Research*, California: Sage

Hair, J.F. (1998): "Research Techniques", *Doctoral Programmes - Henley Management College*, 29/11/98 - 4/12/98

Hamel, J., Dufour, S. and Fortin, D. (1993), *Case Study Methods*, Sage University Paper on Qualitative Research Methods (Vol 32), California: Sage

Hammond, J.S., Keeney, R.L. and Raiffa, H. (1998): "The Hidden Traps in Decision Making", *Harvard Business Review*, September-October 1998, pp 47 - 58

Harris-Jones, J. (1998): *The Management of Corporate Risk*, London: The Association of Corporate Treasurers

Hatch, M.J. (1997): *Organization Theory*, New York: Oxford University Press

Heffernan, S. (1996): *Modern Banking in Theory and Practice*, Chichester: Wiley

Hemaida, R. (1997): "A zero-one programming model fro internal audit planning", *Managerial Auditing Journal*, Vol 12, No 7, pp 331 – 335

Hendrickx, L. and Vlek, C. (1991): "Perceived Control, Nature of Risk Information and

Risk Taking", *Journal of Behavioural Decision Making*, Vol 4, pp 235 - 247

Hickson, C. and Turner, J. (1996): "*Banking regulation's impact on industry monopoly and risk*", Vol 96, No 5, pp 34 – 42

Hillson, D.A. (1997): "Towards a Risk Maturity Model", *International Journal of Project and Business Risk Management*, Vol 1, No 1, pp 35 - 45

Hoffman, D. And Johnson, M.(1996): "Operating Procedures", *Risk*, Vol. 9/No.10/ October, pp 60 - 63

Hommel, U. (2000): *"Managing Catastrophic Risk with Financial Instruments"*, pp 39 – 60 in Frenkel, M., Hommel, U. and Rudolf, M.: *"Risk Management: Challenge and Opportunity"*, Berlin: Springer

Horrigan, W. (1967): *Risk, Risk Management and Insurance*, The Withdean Papers No 1

House of Commons (1998): Treasury Select Committee Ninth Report dated 12/11/98, available http://www.parliament.the-stationery-office.co.uk/pa/cm199798/cmselect/cmtreasy/712/71202.htm

Humphrey, C. and Scapens, R. (1992): *Theories and Case Studies*, Working Paper 92/4, Centre for Empirical Research in Accounting and Finance, University of Manchester

Independent (2000): "Online Fraud Risk was greater than Barclays admitted", August 2 2000

Institute of Chartered Accountants in England and Wales - ICAEW (1999*): Internal Control – Guidance for Directors on the Combined Code (The Turnbull Report)*

Institute of Chartered Accountants in England and Wales - ICAEW (1998): *Financial Reporting of Risk (Proposals for a Statement of Business Risk)*

Institute of Internal Auditors Exposure Draft – IIA (1999a): *Definition of Internal Auditing*

Institute of Internal Auditors – IIA (1999b): *Control and Risk Self Assessment (Professional Briefing Note 14)*

Institute of Internal Auditors – IIA (1999c): *Effective Governance*

Institute of Internal Auditors – IIA (1998a): *Managing Risk (Professional Briefing Note 13)*

Institute of Internal Auditors – IIA (1998b): *Standards and Guidelines for the Professional Practice of Internal Auditing*, Altamonte Springs, Florida: IIA

International Organisation of Securities Commissions - IOSCO (1998): *Risk Management Control Guidance for Securities Firms and their Supervisors*

International Organisation of Securities Commissions - IOSCO (1994): "*Operational and Financial Risk Management Control Mechanisms for Over-the-Counter Derivatives of Regulated Securities Firms*", available http://www.iosco.org/docs-public/1994-operational_and_financial_risk-document02.html

Jameson, R. (1998): "Operational Risk – Playing the name game", *Risk*, October , pp 38 – 43

Janesick, V.J. (1998): *Stretching Exercises for Qualitative Researchers*, California: Sage

Jauch, L.R. and Kraft, K.L. (1986): "Strategic Management of Uncertainty", *Academy of Management Review*, Vol 11, No 4, pp 777 - 790

Jayawardhena, C. and Foley, P. (2000): "Changes in the banking sector – the case of internet banking in the UK", *Internet Research: Electronic Networking Applications and Policy*, Vol 10, No 1, pp 19 – 30

Jensen, M.C. and Meckling, W.H. (1976): "Theory of the Firm: Managerial Behaviour, Agency Costs and Ownership Structure"., Journal of Financial Economics, Vol 3, pp 305 – 360

Jick, T.D. (1979): "Mixing Qualitative and Quantitative Methods: Triangulation in action", *Administrative Science Quarterly*, Vol 24, December, pp 602 - 611

Kaen, F.R.. (2000): "*Risk Management, Corporate Governance and the Modern Corporation*", pp 247 – 262 in Frenkel, M., Hommel, U. and Rudolf, M.: "*Risk Management: Challenge and Opportunity*", Berlin: Springer

Kahneman, D. and Lovallo, D. (1993): "Timid Choices and Bold Forecasts: A Cognitive Perspective on Risk Taking", *Management Science*, Vol 39, No. 1 January, pp 17 – 31

Kahneman, D. and Tversky, A. (1979): "Prospect Theory: An Analysis of Decision Under Risk", *Econometrica*, Vol 47, No. 2 March, pp 263 – 291

Kaminsky, S.W. (1989): *Beyond Retail Banking*, London: Lafferty Publications

Keeney, R.L. (1996): "The Role of Values in Risk Management", *The Annals of the American Academy*, May, pp 126 - 134

Kerlinger, F.N. (1986): *Foundations of Behavioural Research 3rd edn*, New York: Holt, Rinehart and Winston

Kersten, G.E. and Michalowski, W. (1996): *"The DSS Phenomenon: Design, Functions and Management Support"* paper presented at the International Conference on Decision Support Systems for Sustainable Development: Software Technology for Agenda 21, International Institute for Software Technology and IDRC, Ottawa, 24/2 – 8/3

Kharbanda, O.P. and Stallworthy, E.A. (1990): "Managerial Decision Making – Part 2: The Newer Techniques", *Management Decision*, Vol 28, No 4, pp 29 - 35

Kimber, M. and Hoffman, D.G. (1999): *"Operational Risk Management and capital adequacy: a frontal assault on capital"* in *"Operational Risk"*, London: Risk Professional/Informa Business Publishing

Kinsella, R. (1995a): *"Internal Controls in Banking"*, pp 1 – 8 in Kinsella, R. Ed., *Internal Controls in Banking*, Chichester: Wiley

Kinsella, R. (1995b): *"Internal Bank Controls: An Agenda for Dialogue"*, pp 101 – 105 in Kinsella, R. Ed., *Internal Controls in Banking*, Chichester: Wiley

Kirk, J. and Miller, M.L. (1986), *Reliability and Validity in Qualitative Research*, Sage University Paper on Qualitative Research Methods (Vol 1), California: Sage

Klein, J.H. (1996): *Modelling Organisational Cognition of Risk Management*, Discussion Paper 96-109, Department of Accounting and Management Science, University of Southampton

Krebs, J.R. and Kacelnik, A. (1997): *"Risk: a scientific view"* in the Royal Society: *Risk: Science, Policy and Risk, A Discussion Meeting held at the Royal Society on 18/3/97*, London: The Royal Society

Kupiec, P.H.(1995): "Techniques for Verifying the Accuracy of Risk Measurement", *The Journal of Derivatives*, Winter, pp 73 - 84

Kurland, O. M. (1992): "Risk Communication, Mitigation and Uncertainty", *Risk Management*, December, Vol. 39, no. 12, p 60

Kurland, O. M. (1993): "Risk Mitigation in the Atomic Age", *Risk Management*, June, Vol. 40, no. 6, p 34 - 40

Landsdowne, Z.F. (1999): "Risk Matrix: An Approach for prioritising Risks and Tracking Risk Mitigation Progress", *Proceedings of the 30th Annual Project Management Institute Seminars and Symposium*, Philadelphia USA (October)

Lavington, F. (1925): "An approach to the theory of business risks", Economics Journal, XXXV, June, pp 186 - 199

Lee, A.S. (1989): "A Scientific Methodology for MIS Case Studies", *MIS Quarterly*, March, pp 33 – 50

Leeson, N. (1996): *Rogue Trader*, London: Warner

Lowe, A. and Kuusisto, J. (1999): "The institutional stature of the retail bank: the neglected asset", *International Journal of Bank Marketing*, Vol 17, No 4, pp 171 – 181

MacCrimmon, K.R., and Wehrung, D.A.(1986): *Taking Risks,* New York: The Free Press

McCarthy, M.J. (1991): *Mastering the Information Age*, Los Angeles: J.P.Tarcher

McGoldrick, P.J. and Greenland, S.J. (1992): "Competition between banks and building societies in the retailing of financial services", British Journal of Management, Vol 3, No 2, pp 169 – 179

McConnell, P.J. (1998): "Barings: the Development of a Disaster", *International Journal of Project and Business Risk Management*, Vol 2, Issue 1, pp 59 - 74

McConnell, P.J. (1996): *Information Technology for Market Risk Management in International Banks*, DBA Thesis, Brunel University, July

McConnell, P.J. and Blacker, K. (1999): "An Approach to Modelling Operational Risk in Banks", *Henley Working Paper Series,* Ref. HWP 9926

McCutcheon, D.M. and Meredith, J.R. (1993): "Conducting case study research in operations management," *Journal of Operations Management*, Vol 11, pp 239 256

McGrath, J.E. (1982): "Dilemmatics: The Study of Research Choices and Dilemmas", In: *Judgement Calls in Research*, J.E.McGrath, J.Martin and R.A.Kulka (eds.), California: Sage

McKechnie, G. and Howell, N. (1998): *Million-Dollar Frauds*, Florida: Institute of Internal Auditors

McKinnon, J. (1988): "Reliability and Validity in Field Research: Some Strategies and Tactics", *Accounting, Auditing and Accountability Journal*, Vol 1, No 1, pp 34 – 54

McNamee, D. (1997): "Risk-based Auditing", *Internal Auditor*, August, pp 23 - 27

McNamee, D. (1995): "Towards a general theory of Internal Audit", *Internal Auditing*, April, pp 17 - 20

McNamee, D and Selim, G.M. (1998): *Risk Management: Changing the Internal Auditor's Paradigm*, Florida: Institute of Internal Auditors

Martin, H. (1998): "Balancing Risk with Reward", *Accounting and Business*, February, pp 8-9

Menkes, J. and Lave, L.B. (1987): *"Value and Function of Information in Risk Management"*, pp 213 – 220 in Covello, V.T. et al, *Uncertainty in Risk Assessment, Risk Management and Decision Making*, New York: Plenum Press

Merchant, K.A. (1982): "The Control Function of Management", *Sloan Management Review*, Summer, pp 43 - 55

Merriam, S.B. (1988): *Case Study Research in Education: A Qualitative Approach*, San Francisco, CA: Jossey-Bass

Merton, R.C. (1995): "Financial Innovation and the Management and Regulation of Financial Institutions", *The Journal of Banking and Finance*, Vol 19 pp 461 - 481

Miccolis, J.A. (1996): "Toward a Universal Language of Risk", *Risk Management*, July, pp 45 - 48

Miles, B.M. (1979): "Qualitative Data as an attractive nuisance", *Administrative Science Quarterly*, Vol 24, December, pp 590 - 601

Miles, M and Huberman, A (1994): *Qualitative Data Analysis*, California: Sage

Mills, R.W. (1998): *The Dynamics of Shareholder Value,* Lechlade: Mars Business Associates

Mills, R.W. (1997): *"Internal Control Practices within Large UK Companies"*, pp 121 – 143 in Keasey, K. and Wright, M., *Corporate Governance – Responsibilities, Risks and Remuneration*, Chichester: Wiley

Mintzberg, H. (1989): *Mintzberg on Management*, New York: Free Press

Mintzberg, H. (1979): *The Structuring of Organisations: A Synthesis of the Research*, Prentice Hall

Mintzberg, H. (1973): *The Nature of Managerial Work*, New York: Harper and Row

Mols, N.P. (1998): "The Internet and the bank's strategic distribution channel decisions", *Internet Research: Electronic Networking Applications and Policy*, Vol 8, No 4, pp 331 – 337

Nellis, J.G. (1998): "Strategies for staying ahead", *Chartered Banker*, June, pp 28 – 31

Nellis, J.G., McCaffrey, K.M. and Hutchinson, R.W. (2000): "Strategic challenges for the European banking industry in the new millennium", *International Journal of Bank Marketing*, Vol 18, No 2, pp 53 – 63

NHS (1999): *Governance in the new NHS: Controls Assurance Statements 1999/2000 – Risk Management and Organisational Controls*, dated 21/5/99, available http://tap.ccta.gov.uk/doh/coin4.nsf

Nicholson, B.R.I. (2000): *"Fraud Against Banks: A Practical Perspective"*, pp 49– 60 in Norton, J.J. and Walker, G.: *"Banks: Fraud and Crime (2nd edition)"*, London: LLP Professional Publishing

Nutt, P.C. (1984): "Types of Organisational Decision Processes", *Administrative Science Quarterly*, Vol. 29, pp 414 - 450

Oldman, A. (1997): "The Development of a Model for Strategic Cost Reduction as a Managerial Response to Market Orientation", DBA Thesis, Brunel University, November

Oldfield, G.S. and Santamero, A.M. (1997): "Risk Management in Financial Institutions", *Sloan Management Review*, Autumn, pp 33 - 46

Olive, C.D. (2000): *"Operational Risk in Banking Institutions"*, pp 135 – 171 in Norton, J.J. and Walker, G.: *"Banks: Fraud and Crime (2nd edition)"*, London: LLP Professional Publishing

Ong, M.K. (1998): "On the Quantification of Operational Risk: A Short Polemic", in Arthur Andersen: *Operational Risk and Financial Institutions,* London: Risk Publications

Organisation for Economic Co-operation and Development – OECD (1999): "*OECD Principles of Corporate Governance*", dated 19/4/99

Otley, D.T. and Berry, A.J. (1994): "Case Study Research in Management Accounting and Control", *Management Accounting Research*, No 5, pp 45 - 65

Ouchi, W.G. (1979): "A Conceptual Framework for the Design of Organisational Control Mechanisms," *Management Science*, Vol 25, No 9, pp 833 – 848

Pablo, A. L. (1999): "Managerial risk interpretations: does industry make a difference?", *Journal of Managerial Psychology*, Vol 14, No 2, pp 92 – 107

Parsley, M. (1996): "Risk Management's Final Frontier", *Euromoney*, September, pp 74 - 79

Paul, R. (1994): "Say Yes to a Risk Based Audit Approach," *Internal Auditing*, February, pp 15 - 17

Peters, J.M. (1990): "A Cognitive Computational Model of Risk Hypothesis Generation", *Journal of Accounting Research*, Vol 28 pp 83 - 103

Petit, T.A. (1967): "A Behavioural Theory of Management", *Academy of Management Journal*, Vol 10, No 4, pp 341 – 350

Porter, M.E. (1985): *"Competitive Advantage"*, New York: Free Press

Powell, D. (1996): An Introduction to Risk Communication and the Perception of Risk, available http://www.plant.uoguelph.ca/safefood/risk-anal/risk-review/risk-review.htm

PriceWaterhouseCoopers (1999): *"Creating Tomorrow's Leading Retail Bank"*, London: Economist Intelligence Unit and PriceWaterhouseCoopers

PriceWaterhouseCoopers (1998): "Risk Management - A survey of Middle Market companies with turnover £5m - £200m", *PriceWaterhouseCoopers - Barometer No. 9* (Summer)

Preston, T.J. (1993): "*A Risk Management Approach to Control*", MSc dissertation, Southampton University

Pyle, D.H. (1997): "Bank Risk Management: Theory", *Proceedings of the Risk Management and Regulation in Banking Conference*, Jerusalem, May

Quick, J. (2000): "A Regulator's View of Managing Other Risks in Banking", *Risk Management: An International Journal*, Vol 2, No 3, pp 15 – 21

Rahman, M.A. (1998): "A Participatory DSS to Incorporate Local Knowledge for Resources and Environment Management in Developing Countries" available http://www.fes.uwaterloo.ca/u/marahman/PhD_Comprehensive.html

Rayner, S. (1987): *"Learning from the Blind Men and the Elephant, or Seeing Things Whole in Risk Management"*, pp 207 – 212 in Covello, V.T. et al, *Uncertainty in Risk Assessment, Risk Management and Decision Making*, New York: Plenum Press

Raz, T. and Michael, E. (2001): "Use and benefits of tools for project risk management", *International Journal of Project Management*, Vol 19, pp 9 – 17

Reed, N. (1997): "Variations on a Theme", in *Value at Risk*, Risk Publications

Reid, C., Thomson, J. and Wallace-Smith, J. (1998): "Impact of information on corporate decision making: the UK banking sector", *Library management*, Vol 19, No 2, pp 86 –109

Rezaee, Z (1995): "What the COSO report means for internal auditors", *Managerial Auditing Journal*, Vol 10, No 6, pp 5 – 9

Richardson, K.A. and Bartley, R. (1998): "Managing Organisational Complexity Case Studies in Military Use of Decision Support Analysis", available http://www.concentric.net/~kurtar/Berty2/Comp/RAE/rae1.htm

Ritchie, R., and Marshall, D.(1994): *Business Risk Management*, London: Chapman and Hall

Roberts, K.H. and Libuser, C. (1993): "From Bohpal to banking: organisational design can mitigate risk", *Organisational Dynamics*, Vol 21, No 4, pp 15 – 27

Robson, S. and Foster, A. (1989): *Qualitative Research in Action*, London: Edward Arnold

Rodgers, F.W. (1986) with R.L. Shook: *The IBM Way*, New York: Harper and Row

Rotberg, E.H. (1992): *Risk Taking in the Financial Services Industry*, Paris: Organisation for Economic Co-operation and Development

Royal Society, The (1997): *Science, Policy and Risk, A Discussion Meeting held at the Royal Society on 18/3/97*, London: The Royal Society

Royal Society, The (1992): *Risk: Analysis, Perception and Management, Report of a Royal Society Study Group*, London: The Royal Society

Ruffini, F.A.J., Boer, H. and Van Riemsdijk, M.J. (2000): "Organisation design in operations management", *International Journal of Operations and Production Management*, Vol 20, No 7, pp 860 – 879

Ryan, R., Scapens, R.W. and Theobold, M. (1992): *Research Method and Methodology in Finance and Accounting*, London: Academic Press

Sadgrove, K. (1996): *The Complete Guide to Business Risk Management*, London: Gower

Salancik, G.R. and Meindl, J.R. (1984): "Corporate Attributions as Strategic Illusions Of Management Control", *Administrative Science Quarterly*, Vol 29, pp 238 – 254

San Miguel, J.G. and Govindarajan, V. (1984): "The Contingent Relationship Between the Controller and Internal Audit Functions in Large Organisations", *Accounting, Organisations and Society*, Vol 9, No 2, pp 179 – 188

Santamero, A.M. (1997): "Commercial Risk Management; An Analysis of the Process", *Journal of Financial Services Research*, Vol 12:2/3, pp 83 - 115

Santos, J.A.C. (2000): "Bank Capital Regulation in Contemporary Banking Theory: A Review of the Literature", *Bank for International Settlements Working Paper No. 30*, September

Schwab, B, and Schwab, H. (1997): "Better Risk Management: A key to Improved Performance", *Journal of General Management*, Vol 22, No 4, Summer, pp 65 – 75

Schwandt, T.A. (1997): "*Qualitative Inquiry: A Dictionary of Terms*", California: Sage

Senior, A. (1999): "A Modern Approach to Operational Risk", *Risk Professional*, Issue 3/1, May, pp 24 – 27

Shackleton, J.(1997): "*Business Risk Management*", Technical Focus issued by the Institute of Chartered Accountants in England and Wales

Sheedy, E. (1999): "Applying an Agency Framework to Operational Risk Management", available http://www.mafc.mq.edu.au/MAFCpapers/paper22.pdf

Simon, H. (1972): *"Theories of Bounded Rationality"* in Radner, C.B. and Radner, R. *"Decision and Organisation"*, North Holland, Amsterdam

Simon, H. (1977): *The New Science of Management Decision*, New Jersey: Prentice Hall

Simons, K. (1997): "Value at Risk - New Approaches to Risk Management", in *Value at Risk*, Risk Publications

Simons, R. (1999): "How Risky is your Company?", *Harvard Business Review*, May-June, pp 85 - 94

Skyttner, L. (1999): "Praxeology – a cybernetic application", *Kybernetics*, Vol 28, No 2, pp 141 – 163

Slagmulder, R. (1997): "Using Management Control Systems to achieve alignment between strategic investment decisions and strategy", *Management Accounting Research*, Vol 8 pp. 103 - 139

Smallman, C. (2000): "What is operational risk and why is it important?", *Risk Management, An International Journal*, Vol 2, No 3, pp 7 – 14

Smallman, C. (1996): "Risk and organisational behaviour: a research model", *Disaster Prevention and Management*, Vol 5, No 2, pp 12 – 26

Smithson, C. and Minton, L. (1997): "How to Calculate Value at Risk", in *Value at Risk*, Risk Publications

Sohal, A., Simon, A. and Lu, E. (1996): "Practical Examples: Generative and case study research in quality management", *International Journal of Quality and Reliability Management*, Vol 13, No 2, pp 75 – 88

Spraakman, G. (1997): "Transaction cost economics: a theory for internal audit", *Managerial Auditing Journal*, Vol 12, No 7, pp 323 – 330

Stake, R.E. (1995): *The Art of Case Study Research*, California: Sage

Straub, D.W. and Welke, R.J. (1998): "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, December, pp 441 – 469

Sunday Times (2001a): "Banks drag feet on cheque clearance", 29th April

Sunday Times (2001b): "Beware banks bearing gifts", 8th April

Sunday Times (2001c): "Banks ignore calls to clean up their act", 18th March

Sunday Times (2001d): "Banks break rules to hang on to unhappy customers", 7th January

Sutton, R.I. and Staw, B.M. (1995): "What Theory is *Not*", *Administrative Science Quarterly*, Vol 40, pp 371 – 384

Talmor, S. (1998): "Regulators unite on Risk", *The Banker*, February, Vol. 148, no. 864, pp 69 - 70

Tarter, C.J. and Hoy, W.K. (1998): "Toward a contingency theory of decision making", *Journal of Education Administration*, Vol 36, No 3, pp 212 – 228

Taylor, F.W. (1911): *"The Principles of Scientific Management"* in Taylor, F.W. (1947), *"Scientific Management"*, London: Harper and Row

Tellis, W. (1997): "Application of a Case Study Methodology," *The Qualitative Report*, September, Vol 3, No 3, available http://www.nova.edu/ssss/QR/QR3-3/tellis2.html

Teuber, A. (1990): "Justifying Risk", Daedalus, Vol 119, No 4, pp 235 – 254

Thompson, J. And Frost, C. (1997): "Operational Risk Management: Where to Start", Reproduced from the *Bank of England's Financial Stability Review*, p 23 - 31

Thompson, P. (1983): The Nature of Work: *"An Introduction to Debates on the Labour Process"*, Basingstoke: MacMillan

Thompson, P. (1998): "Assessing the environmental risk exposure of UK banks", *International Journal of Bank Marketing*, Vol 16, No 3, pp 129 – 139

Titus, M.E. and Lewis, D. (1997): "Understanding and Applying Value at Risk", in *Value at Risk*, Risk Publications

Toft, B. and Reynolds, S. (1997): *Learning from Disasters: A Management Approach: 2nd edition*, Leicester: Perpetuity Press

Treasury Management Association of Canada (1998), "*Glossary of Risk Management Terms*"

Tschoegl, A.E.. (2000): *"The Key to Risk Management: Management"*, pp 103 – 120 in Frenkel, M., Hommel, U. and Rudolf, M.: "*Risk Management: Challenge and Opportunity*", Berlin: Springer

Tsoukas, H. (1994): "What is Management? An Outline Metatheory", *British Journal of Management*, Vol. 5, pp 289 – 301

Tufano, P. (1996): "Who Manages Risk?", *Journal of Finance*, September, pp 1097 - 1137

Van Maanen, J. (1979): *"Introduction"* pp 11 - 29 in *Varieties of Qualitative Research* Dabbs Jr, J.M. and Faulkner, R.R. (Eds), Beverley Hills, CA: Sage

Van Maanen, J. (1982): "Reclaiming Qualitative Methods for Organisational Research", *Administrative Science Quarterly*, December 1979, Vol. 24, pp 520 – 526

Vinten, G. (1995): "The whistleblowers' charter", *Executive Development*, Vol 8, No 2, pp 25 – 28

Vinten, G. (1996): *Internal Audit Research: The First Half Century*, London: Certified Accountants Educational Trust

Walden, I. (2000): *"Internet Payment Services and Crime in Cyberspace"*, pp 391– 404 in Norton, J.J. and Walker, G.: *"Banks: Fraud and Crime (2nd edition)"*, London: LLP Professional Publishing

Walsh, A. (1995): *"Internal Control in the Computerised Banking Environment"*, pp 9 – 23 in Kinsella, R. Ed., *Internal Controls in Banking*, Chichester: Wiley

Walsh, J.P. and Seward, J.K. (1990): "On the Efficiency of Internal And External Corporate Control Mechanisms," *Academy of Management Review*, Vol 15, No 3, pp 421 – 458

Walsham, G. (1995): "Interpretive Case studies in IS Research: Nature and Method," *European Journal of Information Systems*, Vol 4 pp 74 – 81

Weber, J.A. (1998): *"Merging the Metaphysical and Epistemological Aspects of Uncertainty: A Theoretical Vision"*, available http://www.hbg.psu.edu/Faculty/jxr11/weber.html

Weick, K.E. (1995): "What Theory is *Not,* Theorising *is*", *Administrative Science Quarterly*, Vol 40, pp 385 – 390

White, D. (1995): "Application of Systems Thinking to Risk Management: A Review of the Literature", *Management Decisions*, Vol.33 No.10, pp 35 - 45

Whitley, R. (1989): "On the Nature of Managerial Tasks and Skills: Their Distinguishing Characteristics and Organisation", *Journal Of Management Studies*, May, pp 209 – 224

Wildavsky, A. and Dake, K. (1990): "Theories of risk perception: who fears what and why?", *Daedalus*, Vol 119, No 4, pp 41 – 60

Willcocks, L. and Griffiths, C. (1994): "Predicting Risk of Failure in Large-Scale Information Technology Projects", *Technological Forecast and Social Change*, Vol 47, pp 205 – 228

Williams, T.L. (1996): "An Integrated Approach to Risk Management", *Risk Management*, July, pp 22 - 27

Wilson, A. (1997): "The culture of the branch team and its impact on service delivery and corporate identity", *International Journal of Bank Marketing*, Vol 15, No 5, pp 163 – 168

Winegardner, K.E. (1998): "The Case Study Method of Scholarly Research", available http://www.tgsa.edu/online/cybrary/case1.html

Wiseman, R.M. and Catanach, A.H. (1997): "A longitudinal disaggregation of operational risk under changing regulations: evidence from the savings and loan industry", *Academy of Management Journal*, August, Vol. 40, no. 4, pp 799 - 831

Wiseman, R.M. and Gomez-Mejia, L.R. (1998): "A behavioural agency model of managerial risk taking", *Academy of Management Review*, Vol. 23, no. 1, pp 133 - 153

Withey, D. (1998): "*Operational Risk - A proposed operational and technical framework*" Unpublished paper by Amelia Financial Systems Limited, London, September

Wolcott, F.H. (1992): *"Posturing in qualitative research"* pp 3 – 52 in LeCompte, M.D., Millroy, J. and Preissle (Eds), *The Handbook of Qualitative Research in Education*, New York: Academic Press

Worren, N.A.M., Moore, K. and Collett, P. (1997): "When Theories become Tools: The Pragmatic Validity of Conceptual Models", *Oxford University Templeton College*, Working Paper

Yin, R.K. (1981): "The Case Study Crisis: Some Answers", *Administrative Science Quarterly*, Vol 26, March, pp 58 – 65

Yin, R.K. (1994): *Case Study Research - Design and Methods (second edition)*, California: Sage

Young, B. Ed (1999): "Understanding Operational Risk: A consideration of main issues and underlying assumptions", *Unpublished paper by the Operational Risk Research Forum*

Zeckhauser, R. and Viscusi, W. K. (1996): "The Risk Management Dilemma", *The Annals of the American Academy of Political and Social Sciences*, May, pp 144 – 155

Zeigenfuss, D. E. (1995): "The State of the Art in Internal Auditing Risk Assessment Techniques", *Managerial Auditing Journal*, Vol 10, No 4, pp 3 – 11

Zinalden, M. (1996): "Bank strategic positioning and some determinants of bank selection", *International Journal of Bank Marketing*, Vol 14, No 6, pp 12 – 22