OPERATIONAL RISK MANAGEMENT

香 港 銀 行 學 會
The Hong Kong Institute of Bankers

Operational Risk Management

Operational Risk Management

The Hong Kong Institute of Bankers

WILEY

Published in 2013 by John Wiley & Sons Singapore Pte. Ltd.
1 Fusionopolis Walk, #07-01, Solaris South
Tower, Singapore 138628

Other Wiley Editorial Offices
John Wiley & Sons, 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons, The Atrium, Southern Gate, Chichester, West Sussex, P019 8SQ, United Kingdom
John Wiley & Sons (Canada) Ltd., 5353 Dundas Street West, Suite 400, Toronto, Ontario, M9B 6HB, Canada
John Wiley & Sons Australia Ltd., 42 McDougall Street, Milton, Queensland 4064, Australia
Wiley-VCH, Boschstrasse 12, D-69469 Weinheim, Germany

ISBN 978-0-470-82765-9 (Paperback)
ISBN 978-0-470-82767-3 (ePDF)
ISBN 978-0-470-82766-6 (Mobi)
ISBN 978-0-470-82768-0 (ePub)

Typeset in 11/14 pt. ArnoPro Regular by MPS Limited, Chennai, India.
Printed in Singapore by Markono Print Media.

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The management of operational risk is one of the broadest functions of any bank or financial institution and one of the hardest to compartmentalise. Over the past two decades, understanding of operational risk has grown rapidly. Alongside this understanding, however, the realisation has emerged that only limited data is available. As a whole, the banking industry often has to deal with operational risk by trial and error. This book continues the discussion of bank operations. It examines how banks deal with operational risk, considers some case studies and lessons from the past and discusses how regulators approach operational risk.

This book is divided into four parts and eleven chapters that delve deeply into the subject matter. Despite the depth, the discussion here is unlikely to be enough to fully grasp the challenges of operational risk that have been high up on the list of considerations for the Basel Committee on Banking Supervision (BCBS) since the late 1990s. Further reading is encouraged and suggestions are provided at the end of each chapter.

Every effort has been made to ensure that policies and regulations discussed in this book are up to date and current. Most regulations on operational risk in use around the world are based on Basel II, which this book discusses at length.

The first part of this book starts with a background discussion of what operational risk is in the banking industry as differentiated from other types of risk commonly addressed such as credit risk, market risk, and operations risk. It also discusses how operational risk considerations in the banking industry may differ from other industries. With a broad definition at hand, this part goes on to discuss operational risk frameworks and best practice principles. The part ends with a series of real life cases that give a practical relief to theoretical discussions of operational risk management.

The second part of this book, which starts in Chapter 4, looks at how banks can and should undertake operational risk planning. The first chapter in this part considers the various

methods and tools available to banks and other financial institutions. The second goes on to discuss how best to identify risk, and carry out risk and control self-assessment (RCSA). The final chapter in this part looks at how to measure and assess risk to determine the probable potential loss.

The third part of this book launches in Chapter 7 with an in-depth look of operational risk management. It starts out with considerations of risk control and mitigation followed by Chapter 8, which considers issues of escalation, key risk indicators (KRIs), and risk reporting at some length. This part ends in Chapter 9 with a discussion of associated techniques such as scenario analysis and how various operational risk models work and fit in within the greater framework of operational risk management. Some top-down and bottom-up models are considered.

The last part of this book encompasses the last two chapters, both of which consider how regulators look at operational risk and how regulatory approaches affect banks. The first considers regulatory requirements, particularly those set out by the Hong Kong Monetary Authority and its relationship to Basel II. The final chapter in this book looks at risk governance, outlines and discusses the principles for sound risk management developed by the BCBS and brings the book to an end with a brief discussion of how the various techniques help identify and manage potential events, thus, minimise losses.

This book includes detailed explanations, summaries, tables and charts to help industry professionals develop a sound theoretical framework for their work in the field. Both students and working professionals can benefit from this detailed work produced in collaboration with some of Hong Kong's most prominent professionals. Aimed at banking practitioners and designed as an essential tool to achieve learning outcomes, this book includes recommendations for additional readings. A list of further readings at the end of each chapter will help readers expand their knowledge of each subject while supplementary readings can help readers dig deeper into specific areas. Essential readings will occasionally be highlighted and these are important for students preparing for the examinations leading to the Associate of the Hong Kong Institute of Bankers designation (AHKIB).

A number of people were integral to the development of this work. Among them it is important to highlight Frederick Au. There are many others whose contributions have been of particular significance in the preparation of this essential reference for banking professionals. Among them are Dr. David Yiu Chau Lam and Amos Chan. The information provided in the collection of Hong Kong Monetary Authority publications were instrumental in developing the chapters on risk control and risk governance, we are grateful for the insightful comments from representatives of the Hong Kong Monetary Authority.

The preparation would not have been possible without the help, advice, support, and encouragement of all these people and dozens more. We would like to extend our sincere thanks to them all.

The Hong Kong Institute of Bankers

PART 1

1

OPERATIONAL RISK IN THE BANKING INDUSTRY

CHAPTER 1

1

Overview and Definition

Learning objectives

After studying this chapter, you should be able to:

1. Understand how operational risk is defined by banking regulators, including the Hong Kong Monetary Authority (HKMA), and under Basel II
2. Distinguish operational risk from other types of risk, including market risk and credit risk, and from operations risk
3. Describe how Basel I and II approached operational risk and its inclusion as a factor in determining capital adequacy
4. Define operational risk management and discuss its drivers, activities, and related disciplines
5. Understand the HKMA approach to operational risk

Introduction

Risk is an inherent part of the business of banking. It comes in various forms, each of which presents its own challenges to the proper functioning of a bank. One of the most all-encompassing of these risks is operational risk.

Operational risk in banks and other financial institutions did not become a focal point until the late 1990s and the work by the Bank for International Settlements' Basel Committee on Banking Supervision (BCBS) to define it, as well as develop frameworks to manage it and provide regulatory options. Through Basel I and the subsequent Basel II, operational risk moved from a position well behind the curtain to a role on the center stage of banking operations. Over the past decade, operational risk has taken on even greater importance. The BCBS principles on operational risk management were honed and streamlined.

This book seeks to define and explain operational risk, explore approaches to measure it, control it, and mitigate losses—in short, to explore operational risk management. It explores the sources of operational risk and the evolution of operational risk events. It seeks to offer readers and students the tools to determine bank exposures and develop strategies to mitigate it.

This first chapter lays the foundations for the rest of the book. It seeks to define operational risk, categorise it, and examine where it comes from. It outlines the approaches used in Basel II and by the Hong Kong Monetary Authority (HKMA). The broad outlines of important operational risk events will also be considered before trying to differentiate operational risk from other types of risk, including operations risk, which is an entirely different category.

Lastly, this chapter considers the interplay between the risk management practices of various functions of a bank and operational risk, including financial risk management, audit and internal controls, and reliability engineering.

What is Operational Risk?

For banks and other financial institutions, risk is the inherent potential, while conducting business, for losses or fluctuations in future income that are triggered by events or ongoing trends. The usual forms of risk to which banks are exposed include market risk, credit risk, strategic risk, and operational risk.

Operational risk arises not only from a company's operations, but also from any disturbance in its operational processes. The disruption may come from a one-off event, ranging from rogue trading to terrorist activities or a landmark legal settlement, or from a systems breakdown to sabotage, regulatory breaches, and even acts of God.

Because the triggers are so varied, it is difficult to come up with an exact definition of operational risk. The fuzziness of definition has led to two extreme categorisations. The "narrow" view sees operational risk as stemming from failure within a company's back office or operations area. The "wide" view, on the other end of the spectrum, sees operational risk

as a quantitative residual, that is, the variance in net earnings not explained by financial risks such as market risk and credit risk.

While simpler to understand, the "narrow" view is constraining because it does not take into account the many risks that can affect operations, for example, reputation or legal risks. The "wide" view, by contrast, is more encompassing, and separates risks that are relatively easy to measure from those that are not. The problem is that the wide view is too sweeping, and because it lacks specificity, is virtually impossible for use in managing operations.

Operational Risk in Financial Institutions

Most banking regulators adopt definitions that fall somewhere between these two views, focusing on the risk of failures in technology, controls, and staff. For example, the U.S. Federal Reserve Board's *Trading and Capital-Market Activities Manual* defines operations and systems risk as "the risk of human error or fraud or the risk that systems will fail to adequately record, monitor, and account for transactions or positions." The U.S. *Office of the Comptroller of the Currency (1989)* described operational risk as including system failure, system disruption, and system compromises.

For its part, the BCBS defines operational risk in its Basel II guidelines "as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."

The HKMA closely follows the Basel II definition. In its *Supervisory Policy Manual* for *Operational Risk Management*, the HKMA defines operational risk as "risk of direct or indirect loss resulting from inadequate or failed internal processes, staff and systems or from external events."[1]

In evaluating operational risk, the HKMA requires authorised institutions (AIs) to take into account both product and AI-specific factors.

"The relevant product factors include the maturity of the product in the market, the need for significant fund movements, the impact of a breakdown in segregation of duties and the level of complexity and innovation in the market place," it explains. "AI-specific factors, which can significantly increase or decrease the basic level of operational risk, include the quality of the audit function and programme, the volume of transactions in relation to systems development and capacity, the complexity of the processing environment and the level of manual intervention required to process transactions."

Causal Factors

Determining the causes of operational risk is key to understanding and handling operational risk. In the last decade, understanding of operational risk has deepened considerably as has the

[1]HKMA Supervisory Policy Manual, *Risk-based Supervisory Approach* (HKMA, 11 October 2001), 20.

ability of practitioners to separate operational risk from other types of risk such as credit risk, market risk, risks from interest rates or liquidity risk, reputational risk, legal risk, or strategic risk.

Operational risk has emerged as a much more significant issue over the last couple of decades as banks rely on more complex technology and automate their processes, develop more complex products, become larger through mergers and acquisitions, consolidate and reorganize their operations, outsource some functions, and adopt measures to control other types of risk that create new operational concerns.[2]

In setting out its approach to handle operations risk, the HKMA lays out four general causal factors for operational risk:

- Process factors;
- People factors;
- System factors;
- External factors.

Each of these, in turn, creates different categories of risk that are explored further in the next section.

Categories

The four main causal factors of operational risk—processes, people, systems, and external factors—all create manageable but potentially significant risks to an organization. Like the HKMA, the BCBS also suggests that identifying these four causal factors is the first step towards defining operational risk and then creating a framework to address it that is uniform across financial institutions. Each of these causal factors is relatively general in its scope and each can lead to significant risk events.[3]

Process Factors

The first causal factor, process risk, focuses on the internal structures that an institution uses to carry out its business. These processes can, and often do, carry significant risks with them.

There are multiple categories of risks that can be associated with process:

- Inadequate or inappropriate guidelines and procedures;
- Inadequate communication or a failure in communication;
- Erroneous data entry;
- Inadequate reconciliation;
- Poor customer or legal documentation;
- Inadequate security controls;

---

[2]HKMA Supervisory Policy Manual, *Risk-based Supervisory Approach* (HKMA, 11 October 2001), 20.
[3]HKMA Supervisory Policy Manual, *Risk-based Supervisory Approach* (HKMA, 11 October 2001), 20.

- Breach of regulatory and statutory provisions or requirements;
- Inadequate change management process; and
- Inadequate back up or contingency planning.

People Factors

People, whether intentionally or otherwise, can also pose a significant operational risk. Intensive training and careful, multi-layered supervision can help but there are still several categories of operational risk that stem from this ever-present causal factor. These include:

- Breaches of internal guidelines, policies, or procedures;
- Breaches of delegated authority;
- International criminal acts;
- Inadequate segregation of duties or lack of dual controls;
- Lack of experience;
- Staff oversight; and
- Unclear roles and responsibilities.

System Factors

In recent years, there have been a number of high-profile institutional failures—sometimes but not always related to financial institutions—that were caused by systemic risk. New computer software models that help stock traders do high-intensity trading with hundreds of thousands of trades per minute based on complicated algorithms have been highly profitable but have, at times, caused massive losses in just a few minutes. Banks and other financial institutions have lost customer data due to system failures and networks have been known to break down.

System risk may be easier to identify than other causal factors and there are fewer categories of operational risk associated with systems. Nevertheless, experience shows that this type of risk can be potentially devastating for a financial institution. The HKMA gives an example of a systemic risk factor in its guidance on *Operational Risk Management* issued as part of its *Supervisory Policy Manual*: Inadequate hardware, networks, or sever maintenance. It is probably safe to include inadequate software in this category as well.

External Factors

External factors can also pose significant operational risk to a banking institution. Here again, processes can be put in place to control or mitigate events associated with external risks, even if these are often harder to control. Among the categories of external risk are:

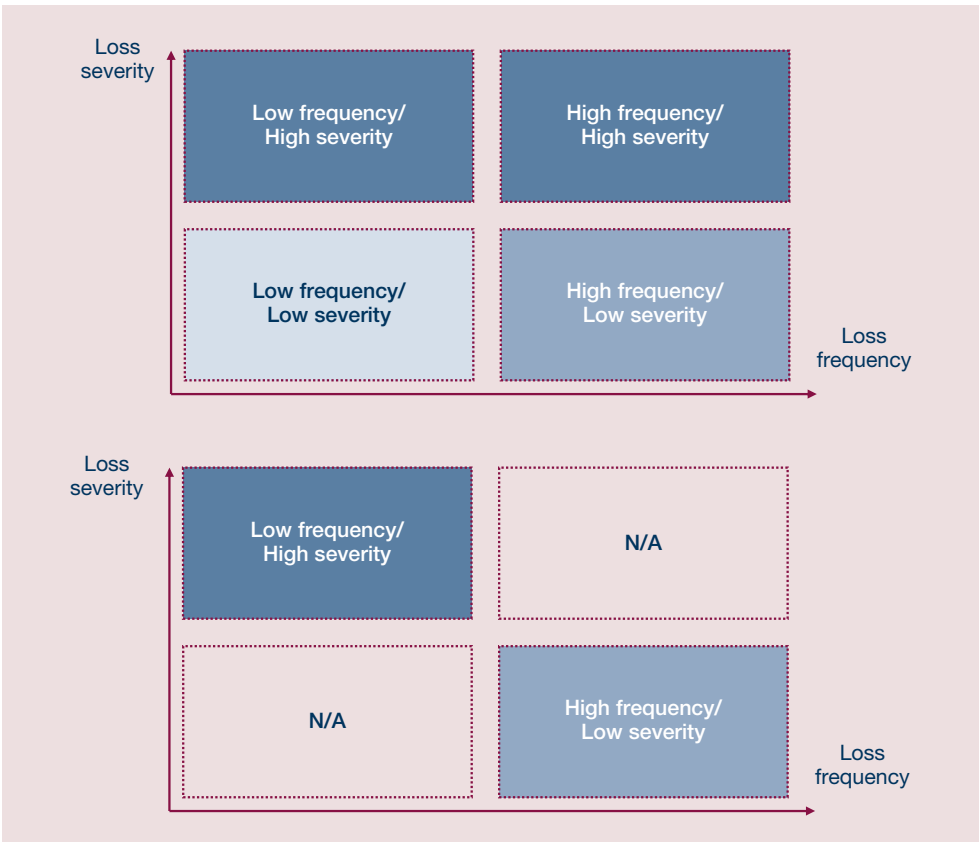
- Criminal acts;
- Vendor misperformance;
- Man-made disasters;
- Natural disasters; and
- Political, legislative, and regulatory causes.

Important Operational Risk Events

With broad operational risk causal factors broken down into somewhat narrower risk categories, the next step is to determine how categories translate into actual events and the potential losses that stem from those events. Operational risk management is fundamentally about managing risk to prevent operational losses, particularly large ones. The major operational risks are primarily driven by events such as fraud, sales practice violations, and unauthorised activities. The goal of operational risk management is to lower the frequency and severity of large-loss events.

We can draw a four-section grid that depicts low frequency and high frequency loss events against small losses and large losses (see Exhibit 1.1).

EXHIBIT 1.1 Classification of operational risk by frequency and severity: unrealistic view (top) and realistic view (bottom)



Anna S. Chernobai, Svetlozar T. Rachev, Frank J. Fabozzi, *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis* (New Jersey: John Wiley & Sons, Inc., 2007), 25.

The key challenge for operational risk management is to ensure a low frequency of major events that lead to large losses. Large losses from major events can destroy a bank. Perhaps the most famous example of such a destructive event is what happened at Barings Bank in the United Kingdom, which declared bankruptcy in 1995.

Barings was the oldest merchant bank in the UK, a venerable institution founded in 1762 that operated profitably for more than two centuries until one man with unchecked powers brought it all down. In 1993, Nick Leeson was appointed general manager of the Barings Futures subsidiary in Singapore. His job was to take advantage of low-risk arbitrage opportunities and leverage differences in price in similar equity derivatives on the Singapore Money Exchange (SIMEX) and exchange markets in Osaka, Japan. With little consideration for operational risk, Leeson was given control of both trading and back-office functions.

Leeson's losses started to accumulate when the markets became much more volatile through 1993 and 1994 and he hid those losses in a special account (numbered 88888). The earth opened up under his (and the bank's) feet when a massive earthquake struck Kobe on January 17, 1995. Leeson's losses topped US$1 billion. His fraudulent practices did not become apparent until February, when he did not show up to work at his office in Singapore and tried to flee to England. In his own book, *Rogue Trader*, Leeson says he had built up an exposure in Japanese shares of more than GBP11 billion, which amounted to about 40% of the Singapore market. In March 1995, ING bought Barings for GBP1 and, before the year was out, Leeson was sentenced to six and a half years in a Singapore jail.[4]

All this could have been avoided through better internal controls and consideration of operational risks. What happened at Barings was monumental, a large loss, low frequency event that is not necessarily unique to the banking industry. Industries such as aviation, healthcare, chemical-processing, and railway also face similar dangers.

A secondary challenge for operational risk management is to stem the high frequency of small losses, although these usually are not a serious threat to the company. Often these minor losses can be incorporated into the cost of doing business (for example, credit-card fraud loss). Over time, operational risk management can spot the problem areas and find appropriate solutions to minimise or avert the occurrence of these minor but frequent losses.

What happens when operational risk management fails? Exhibit 1.2 lists examples of highly severe but fortunately low-frequency events and operational shortcomings that resulted in big bank losses over two decades.

These events are not always associated with operational risk but they can be directly linked to failures in operational risk management.

---

[4]Anna S. Chernobai, Svetlozar T. Rachev, Frank J. Fabozzi, *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis* (New Jersey: John Wiley & Sons, Inc., 2007).

EXHIBIT 1.2 Examples of operational risks

Institution	Activity	Year	Loss $ million*
Daiwa Bank, New York	Unauthorised bond trading caused by poor management controls	1984–95	1,100
Sumitomo Corp, London	Unauthorised copper trading, fraud, and forgery	1986–96	1,700
UK life-insurance industry	Pensions mis-selling and non-compliance	1988–94	18,000
Standard Chartered, India	Irregularities on Bombay Stock Exchange	1992	400
Credit Lyonnais	Poor lending control	1980s, 1990s	29,000
U.S. banks, corporations, retailers	Check fraud	1993	12,000
London Stock Exchange and members	TRURUS system cancellation	1993	700
Kidder Peabody	Bond trading, lack of internal controls	1994	200
Proctor & Gamble	Lack of management understanding	1994	157
Morgan Grenfell	Misrepresentation	1990s	640
Orange County	Bond trading, lack of management oversight	1994	1,700
Barings, Singapore	Inadequate control of futures trading—in particular poor segregation of duties	1995	1,600
Deutsche Bank (Morgan Grenfell), London	Investment outside authority	1996	600
eBay	Internet auction house, technology failure	1999	5,000 wiped off market value

Christopher Marshall, *Measuring and Managing Operational Risks in Financial Institutions* (Singapore: John Wiley & Sons, 2001), 27.
*Approximate US$ cost as cited on at least one occasion in the press.

Linked Events

An example of failures linked to operational risk can be found in hedge fund failures in recent years, failures that amount to about US$600 billion invested in some 6,000 funds.[5] Hedge funds typically associate operational risk with the operating environment of the fund, including middle and back office functions, trade processing, accounting, administration, valuation, and reporting. It is a wide definition that makes it possible to link myriad events to operational risk management.

In *Measuring and Managing Operational Risks in Financial Institutions*, Anna Chernobai, Svetlozar Rachev, and Frank Fabozzi quote a 2002 study by the Capital Markets Company (Capco) that linked about half of all hedge fund failures to operational risk. The most common failures include misrepresentation of fund investments, misappropriation of investor funds, often by investment managers, unauthorised trading, and inadequate resources. All these could feasibly be linked with operational risk.[6]

Legal Events

The definition of operational risk adopted by the HKMA (and by the BCBS) excludes strategic or reputational risk but includes legal risk. By defining operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and system or from external events,"[7] the HKMA takes into consideration that accounting for legal events is a key function for operational risk managers.

New techniques to mitigate other types of risk such as those associated with collateralisation, credit derivatives, or asset securitization, may open the door for more legal risk that would fall under the broad umbrella of operational risk. These risks are included in the operational risk framework despite the fact that the HKMA's risk-based supervisory approach suggests that AIs are subject to eight major types of risk: credit, market, interest rate, liquidity, operational, reputational, legal, and strategic. The old silo approach to managing risk is no longer seen as sufficient. Risks are often interlinked, as is the case with operational and legal risks. A bank may, for example, have operational processes to handle issues of security associated with mortgages or loans but if these processes lead to outcomes that do not conform with local laws or regulations then the process is intrinsically flawed and the resulting legal event may ultimately be the result of poor operational risk management.

At the same time, Hong Kong's *Banking Ordinance* requires AIs to carry out their business with "integrity, prudence, competence and in a manner which is not detrimental to the interests of depositors or potential depositors." In assessing a bank's compliance with these

---

[5]Anna S. Chernobai, Svetlozar T. Rachev, Frank J. Fabozzi, *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis* (New Jersey: John Wiley & Sons, Inc., 2007).

[6]Anna S. Chernobai, Svetlozar T. Rachev, Frank J. Fabozzi, *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis* (New Jersey: John Wiley & Sons, Inc., 2007).

[7]Hong Kong Monetary Authority, *Supervisory Policy Manual: Operational Risk Management*; 28 November 2005. Pg. 3.

requirements, the HKMA takes into account operational risk issues like the bank's ability to deal with external shocks or unexpected contingencies, its ability to deal with fraud, the likelihood of operational errors, and the quality of systems and staff. At the same time, the *Banking Ordinance* calls for a capital adequacy ratio of 8% or more, which takes into account operational risk, credit risk, and market risk. Failures in any of these can lead to significant legal events.

There are other areas in which operational risk factors can result in legal events. For example, poor legal documentation can lead to risk events associated with process. Banks generate an enormous amount of paperwork and documentation. Inaccurate or inappropriate information in any of these documents can increase both legal risk and operational risk.[8]

The HKMA says banks should review all external documentation before issuing them. This includes considering the following:

- Compliance with regulatory and legal requirements;
- The use of standard and non-standard terms;
- Channels or ways in which documentation is issued; and
- Whether confirmation of acceptance is required.

Another important and potentially costly legal event is a change in the legal system of laws of a country or changes to a particular code, such as the tax code.[9] The advent of a slew of new regulations to deal with the perceived failures of the financial industry in the past two decades (and particularly since 2008) have led to a series of such risks. At times, new laws and regulations have impact across borders. In the U.S. for example, the *Bank Secrecy Act*, the *USA PATRIOT Act* and anti-money laundering regulations all can generate risks for banks that operational risk managers should monitor carefully to avoid significant penalties and fines.

A case involving HSBC bank in 2012 highlights these risks. After a probe of several years, authorities in the U.S. linked the giant global bank to allegations of money laundering in connection to the bank's acquisition in 2002 of Grupo Financiero Bital, a Mexican bank with a poor compliance system. U.S. authorities believe HSBC failed to improve procedures and that failure may have permitted some transactions to happen that exposed the bank to considerable legal risk. As of June 2012, the bank had set aside US$700 million for potential liabilities.[10]

Tax Events

Operational risk-related events that, in terms of the potential magnitude of associated losses, can be quite significant are associated with tax non-compliance or evasion, at times

---

[8]Hong Kong Monetary Authority, *Supervisory Policy Manual: Operational Risk Management*; 28 November 2005. Pg. 28.

[9]Anna S. Chernobai, Svetlozar T. Rachev, Frank J. Fabozzi, *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis* (New Jersey: John Wiley & Sons, Inc., 2007).

[10]Shahien Nasiripour, Caroline Binham, Patrick Jenkins; *HSBC faces probe on money laundering claims;* Financial Times; online; 15 July 2012.