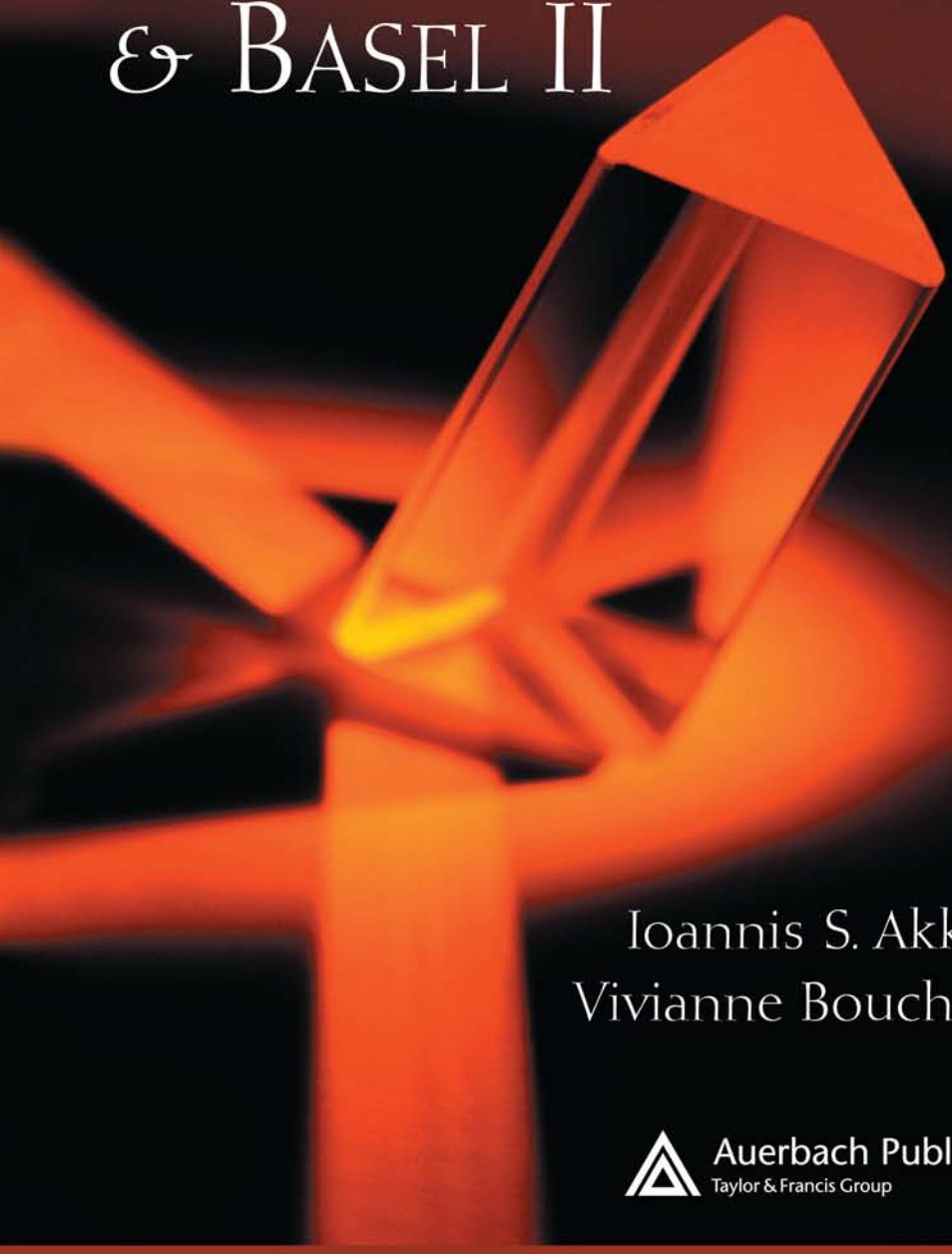
Guide to Optimal Operational Risk & Basel II



Ioannis S. Akkizidis
Vivianne Bouchereau

Auerbach Publications
Taylor & Francis Group

A Downloadable Complete Operational Risk Software Tool is Available for You

Guide to Optimal Operational Risk & Basel II

OTHER AUERBACH PUBLICATIONS

Agent-Based Manufacturing and Control Systems: New Agile Manufacturing Solutions for Achieving Peak Performance
Massimo Paolucci and Roberto Sacile
ISBN: 1574443364

Curing the Patch Management Headache
Felicia M. Nicastro
ISBN: 0849328543

Cyber Crime Investigator's Field Guide, Second Edition
Bruce Middleton
ISBN: 0849327687

Disassembly Modeling for Assembly, Maintenance, Reuse and Recycling
A. J. D. Lambert and Surendra M. Gupta
ISBN: 1574443348

The Ethical Hack: A Framework for Business Value Penetration Testing
James S. Tiller
ISBN: 084931609X

Fundamentals of DSL Technology
Philip Golden, Herve Dedieu, and Krista Jacobsen
ISBN: 0849319137

The HIPAA Program Reference Handbook
Ross Leo
ISBN: 0849322111

Implementing the IT Balanced Scorecard: Aligning IT with Corporate Strategy
Jessica Keyes
ISBN: 0849326214

Information Security Fundamentals
Thomas R. Peltier, Justin Peltier, and John A. Blackley
ISBN: 0849319579

Information Security Management Handbook, Fifth Edition, Volume 2
Harold F. Tipton and Micki Krause
ISBN: 0849332109

Introduction to Management of Reverse Logistics and Closed Loop Supply Chain Processes
Donald F. Blumberg
ISBN: 1574443607

Maximizing ROI on Software Development
Vijay Sikka
ISBN: 0849323126

Mobile Computing Handbook
Imad Mahgoub and Mohammad Ilyas
ISBN: 0849319714

MPLS for Metropolitan Area Networks
Nam-Kee Tan
ISBN: 084932212X

Multimedia Security Handbook
Borko Furht and Darko Kirovski
ISBN: 0849327733

Network Design: Management and Technical Perspectives, Second Edition
Teresa C. Piliouras
ISBN: 0849316081

Network Security Technologies, Second Edition
Kwok T. Fung
ISBN: 0849330270

Outsourcing Software Development Offshore: Making It Work
Tandy Gold
ISBN: 0849319439

Quality Management Systems: A Handbook for Product Development Organizations
Vivek Nanda
ISBN: 1574443526

A Practical Guide to Security Assessments
Sudhanshu Kairab
ISBN: 0849317061

The Real-Time Enterprise
Dimitris N. Chorafas
ISBN: 0849327776

Software Testing and Continuous Quality Improvement, Second Edition
William E. Lewis
ISBN: 0849325242

Supply Chain Architecture: A Blueprint for Networking the Flow of Material, Information, and Cash
William T. Walker
ISBN: 1574443577

The Windows Serial Port Programming Handbook
Ying Bai
ISBN: 0849322138

AUERBACH PUBLICATIONS

www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Guide to Optimal Operational Risk & Basel II

Ioannis S. Akkizidis
Vivianne Bouchereau

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Published in 2005 by
Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-3813-1 (Hardcover)
International Standard Book Number-13: 978-0-8493-3813-7 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Catalog record is available from the Library of Congress

T&F informa

Taylor & Francis Group
is the Academic Division of T&F Informa plc.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Publications Web site at
http://www.auerbach-publications.com

Dedication

This book is dedicated to

My father (Ioannis Akkizidis)

My family (Vivianne Bouchereau)

Contents

Preface

Risk creates value and profits come from taking risks.

—Ulrich Doerig

Businesses are becoming more and more competitive and managing risk continues to be at the heart of financial organizations' activities. Risk management was in its elementary stages until the 1980s. It was not recognized as part of business management processes, but only as a method of taking precautionary measures when business went wrong. In recent years, managerial practices are recognizing the importance of enterprisewide risk management and trying to strategically analyze corporate activities. Organizations are realizing the need to properly understand their risks due to various actions as well as interrelations of the risks within the organization.

New disciplines are emerging for risk management, as well as a new focus on operational risk management. Operational risks have existed as financial organizations evolved. However, as a separate discipline, operational risk management surfaced only in recent years. Compliance regulations, such as Basel II, mandate a focus on operational risks, and have forced the market to evaluate the implications these regulations will have on procedures and strategies in coming years. Of all the different types of risks that can affect financial organizations, operational risks can be among the most devastating and the most difficult to anticipate. Operational risk continues to receive heightened attention among market participants and regulators, prompting dialogues and debates on the best ways to identify, measure, evaluate, control, and manage this important type of risk. This recognition has led to an increased emphasis on the importance of sound operational risk management in financial organizations and, to a greater extent, operational risks in banks' internal capital assessment and allocation

processes. Operational risk management is one of the most complex and fastest growing areas in financial organizations today. As one of the most heavily regulated industries, financial organizations are often required to set the ball rolling with regard to rules and guidelines, while other industries follow suit.

As the pace of change inside and outside financial organizations continues to increase exponentially and as the marketplace becomes more and more complex due to technological advancement and innovations, the management of operational change and operational risks has become a critical success factor. For the first time, the Basel Committee has proposed to establish capital charges for operational risks, in exchange for lowering them on market and credit risk. This new accord, aiming for a closer correspondence between the capital that banks hold and the risks they take, should lead to more stable, efficiently run financial organizations. Thus operational risk management has been placed high on the agenda for financial organizations. Incentives to comply with Basel II allow banks that can prove they have effective and sophisticated operational risk management systems to reduce their level of protective capital buffer, freeing potentially millions of dollars for investment in profitable activities. Efficient operational risk management is a decisive competitive advantage. It helps to maintain stability and continuity and supports revenue and earnings, a process for which senior management and boards of directors are increasingly called upon to ensure. Business operations will need to be as efficient as possible to deliver reliable services to customers. Operational risk management frameworks and practices will need to mature to satisfy all stakeholders versus shareholders, employees, government, regulators, and society as a whole. The Basel II Capital Accord marks a significant shift in the philosophy of capital regulation and the supervision of banks. Although numerical minimum capital requirements remain, they are embedded deep within Basel II's mathematical structure, a structure that places much more emphasis on the range of capital that may be required for specific operational risks faced by each bank. Basel II clearly lays down that financial organizations need to focus on loss data collection of three to five years varying according to different lines of business. It also stresses more effective ways to track, monitor, analyze, and report operational risk data.

The Basel II Accord is all about bringing together the world's financial organizations under a common regulatory framework, although the way to manage operational risk is different for each financial organization. Financial organizations could improve their operational risk management in a way that would have a bottom-line impact even without Basel II. Still, there are important reasons to go all the way: financial organizations certified as Basel II compliant could benefit from lower capital charges

and the enhanced reputation that would come from the regulators' seal of approval. Applying the Basel II requirements will take financial organizations to, or close to, best practices in operational risk management.

Significant operational losses in recent years in the banking industry have highlighted that operational risks can arise from internal and external fraud, failure to comply with employment laws or meet workplace safety standards, policy breaches, compliance breaches, key personnel risks, damage to physical assets, business disruptions and system failures, transaction processing failures, information security breaches, and so on. Financial organizations such as banks, security companies, and insurance companies have particularly been adversely affected by operational risks in recent years. The list of cases involving catastrophic consequences of procedural and operational momentary failure is long and unfortunately growing. To see the implications of operational risk events, one need only look at the devastating $691 million rogue trading loss at Allfirst Financial, the $484 million settlement due to misleading sales practices at Household Finance, the $1.3 billion loss of Barings Bank as a result of rogue trading operation, and the loss arising from the September 11, 2001, terrorist attack on the World Trade Center, which is estimated to be about $16.9 billion. However, the terrorist attack that took place in Madrid on March 11, 2004 had significantly fewer losses, and the most recent in London on July 7, 2005 found financial organizations worldwide more mature, and thus their financial losses are expected to be respectively less. This is because financial organizations have more knowledge on such risks and are designing and implementing more effective operational risk management frameworks. Concerning the London attack, the market also expects that there will be a big investment for designing and implementing effective operational risk management systems for many operations supporting business sectors that will be part of the upcoming Olympic games in London in the year 2012. Losses such as those that were initiated from the natural disasters of an earthquake and its associated tsunamis that hit the Indian Ocean on December 26, 2004, was one of the most devastating operational risks that are classified in the group of 'external risks' in these last few years. The terrible loss of human lives is estimated at over 200,000. The financial loss is yet unknown. This event illustrates how external calamities can affect and disrupt organizations' normal day-to-day operational activities.

One highly visible operational risk event can suddenly end the life of a financial organization. Moreover, many, almost-invisible individual errors of persistent operational risk events over a period of time can strain the resources of the financial organization. Whereas a fundamentally strong organization can often recover from market risk and credit risk events, it may be almost impossible to recover from certain operational risk events. The extent of potential operational risk losses will increase in the future

as global financial organizations specialize in unpredictable new products and services, mergers and acquisitions, and outsourcing, to name just a few.

For effective operational risk assessment, control, and management, it is vital to identify, measure, model, monitor, evaluate, and determine the operational risk profile, but more important to optimize the implications of the operational risks in operational business performances. This ensures an alignment of these operational risks to the business/strategic objectives, planning process, decision making, practices, and quality initiatives. Moreover, strategic and planning policies on when and how to accept, avoid, or mitigate operational risks according to their actual probability, impact, and exposure should be defined. This definition must be consistent with the optimal levels of operational risks. Apart from the underlying approaches, the provision of sound practical tools is essential for efficient operational risk management.

This book presents all the key aspects of operational risk management that are also aligned with the Basel II requirements. More important, it gives detailed guidance for the design and implementation of efficient operational risk management systems. Thus, all the elements of the assessment analysis, including the operational risk identification analysis, measurement, modeling, and monitoring analysis, together with the evaluation analysis and the estimation of capital requirements, make up a great part of this book. Additionally, a significant part of this book addresses managing and controlling operational risks, which includes operational risk profiling, optimization, decision making, and design of optimal risk policies. Several novel approaches that combine aspects of advanced mathematical algorithmic modeling with business intelligent techniques together with total quality management are outlined in the book. Moreover, a forward-looking design of sound practical tools to drive optimal bottom-line results is highlighted. Practical examples of the approaches are presented to support the guidelines of the book. Because one picture is worth a thousand words, this book contains specially designed graphics to help readers visualize as many ideas and concepts as possible. The graphical output results for the case studies illustrated in the book originate from a software tool that the reader can access at www.crcpress.com/e_products/downloads/download.asap?cat_no=AU3813. The software tool supports the applicability of the material of the book. For more details about the software and any feedback related to the subject of this book, please contact the authors or visit http://www.riskoptimisation.com.

Audience

This book is intended for practitioners or those who have an interest in learning about operational risk management and its role in the Basel II

Accord. It is particularly suitable for those seeking to grasp the more advanced approaches of assessing, controlling, and managing operational risk in financial organizations. It also serves as a guide to understand the fundamentals of operational risk management and the Basel II operational risk management principles. More important, it serves as a guide for implementing optimal operational risk management systems. Potential readers of the book include but are not limited to:

- Operational risk managers/chief risk officers/risk analysts
- Operational risk consultants
- Operations and business line managers
- Chief security officers
- Financial risk managers
- Chief information officers
- Actuaries
- Auditors
- Compliance officers
- Insurers
- University lecturers in risk management subjects
- Postgraduate students in financial and banking undertaking subjects related to banking processes, management, and risks
- Financial project managers

Organization of This Book

The book is divided into four parts. The first part introduces the idea of operational risks and how they affect financial organizations. It also focuses on the main aspects of managing operational risks in financial organizations. Part II focuses on the requirements of an operational risk management framework according to the Basel II Accord. Part III and Part IV of this book give overview guidelines on how to design an efficient framework for operational risk management systems in accordance with Basel II requirements. Whereas Part III concentrates notably on the operational risk assessment phase, Part IV focuses on the controlling and managing of these operational risks. All these stages combine to implement efficient and optimal operational risk management systems. The book is organized as shown in Figure 0.1

Chapter 1: Operational Risks in Financial Organizations

This chapter introduces several topics that form the basis of the subsequent chapters. It attempts to show the multifaceted definition of operational risk and highlights some of its major concerns. Examples of operational

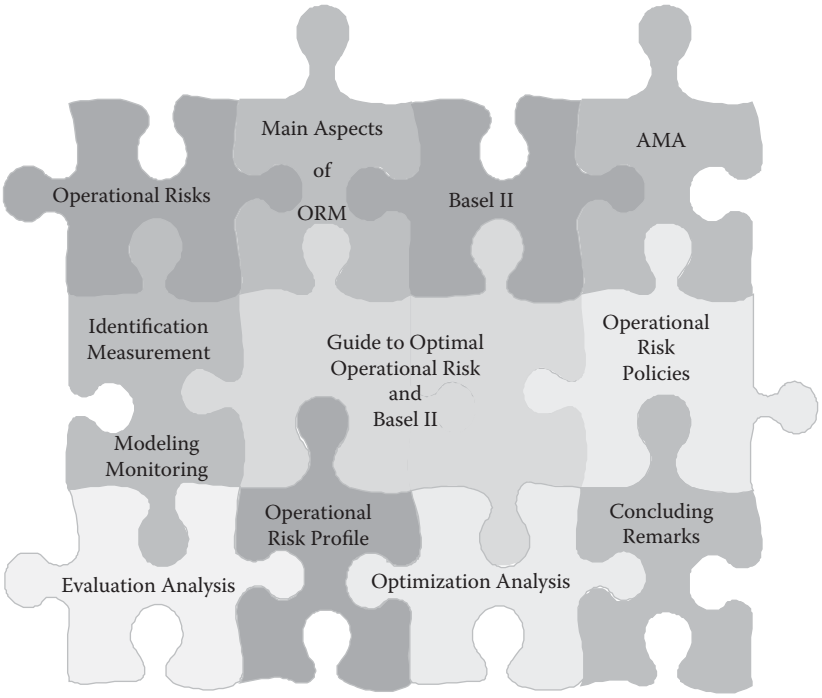


Figure 0.1 Organization of the book.

losses in various organizations around the globe are highlighted to put in perspective the need to manage these risks. The characteristics of operational risks are generally discussed, and then the chapter examines the effect of IT and IT security in the realism of operational risks.

Chapter 2: Main Aspects of Operational Risk Management

This chapter contains a discussion of the main aspects of operational risk management (ORM). Furthermore, effective operational risk management frameworks are outlined. The quantification of operational risks and the testing and verification of the operational risk management framework are then discussed. Enterprisewide risk management, which aims to integrate the management of the different types of risks faced by financial organizations, is introduced, together with some main operational risk management concerns. Finally some key players for implementing effectively operational risk management frameworks are listed.

Chapter 3: Operational Risk in Basel II

This chapter introduces the Basel II Accord, briefly comparing it with its predecessor. The chapter then highlights the meaning of operational risk in Basel II and lists some of the main objectives and targets of the Basel II Accord. A discussion of the three pillars of the accord is also included. The calculation of the minimum capital requirements is subsequently discussed in relation to which of the three proposed Basel II approaches is implemented. The qualifying criteria for operational risk capital calculation are then highlighted with reference to the main factors in selecting an appropriate approach. Finally, Chapter 3 introduces the ten principles of the accord with some action points concerning the three pillars of Basel II, to consider in preparation for an efficient operational risk management framework.

Chapter 4: Advanced Measurement Approach

Chapter 4 focuses on the advanced measurement approach (AMA) proposed by Basel II. It discusses the quantitative standards of the AMA, including the three broad AMA approaches proposed by Basel II. It then discusses the qualifying criteria for operational risk capital calculation using the AMA. In addition, this chapter introduces the supervisory standards for the AMA. Finally, it discusses the use of insurance as an operational risk mitigation strategy under the AMA.

Chapter 5: Operational Risk Identification, Measurement, Modeling, and Monitoring Analysis

This chapter deals with the framework of methodologies for operational risk identification, measurement, modeling, and monitoring analysis. The chapter gives guidelines on when and how to define key performance and risk indicators and how to measure these indicators, for the information data extraction process related to operational risk causes, events, and consequences. It also shows how to model and monitor efficiently both operational risks and affected operations based on correlation analysis defined from multidimensional operational risk parameters. Results that illustrate the mapping of the pattern or contour topography of the operational risks and affected operations are presented. Advanced graphical representation using three-dimensional surface illustrations shows the correlation models for both operational risk and affected operations.

Chapter 6: Operational Risk Assessment via Evaluation Analysis

This chapter focuses on the evaluation process for both operational risks and affected operations. The evaluation is based on significance analysis referring to cause, events, and consequences. Clustering approaches based on fuzzy logic theory are presented to show their implementation for the operational risk evaluation analysis. The identification of the equilibrium points referring to operational risk and affected operations based on two different methods are presented in this chapter. A method called "mountain surface evaluation," which is based on advanced algorithmic analysis and graphical representation, is also discussed extensively in this chapter. Finally, the estimation and evaluation of the economical capital reserves using the operational VaR and the application of extreme value theory are described in this chapter.

Chapter 7: Operational Risk Profiling

This chapter gives guidance on how to estimate the probability and impact based on the analysis of the operational risk causes, events, and consequences. This analysis is mainly focused on the correlations, significances, actual, and loss values of operational risks. Furthermore, the modeling and monitoring of the operational risk profile, based on fuzzy clustering and fuzzy logic techniques and methodologies, are discussed. These advanced approaches for decision making are applied to different case studies of operational risks in banking organizations. Advanced graphical representation of the results are presented and discussed extensively to show the applicability of the approaches.

Chapter 8: Operational Risk Optimization

This chapter presents operational risk optimization by means of optimizing the levels of operational risk parameters to minimize the overall value of risks and their effect on the operations. Moreover, techniques of optimizing the resources that should be allocated to manage these risks are also discussed in this chapter. Different optimization techniques and methodologies that can be used for designing effective and optimal operational risk management systems are introduced with a focus on significance–exposure– correlation optimization. Results coming from the optimization analysis are also presented and discussed.

Chapter 9: Framework for Decision Making and Designing Optimal Risk Policies

This chapter provides guidance on how financial organizations should plan their actions and policies for designing efficient operational risk management frameworks. This includes the policies of when to accept, avoid, or transfer/mitigate operational risks. Scenarios used for risk analysis are also presented. Business impact analysis for designing the "worst-case scenario" is also discussed. Moreover, this chapter gives guidelines for designing business continuity plans to deal with operational risks that are severe. The main guidelines for undertaking internal control, in relation to Basel II's requirements, are also presented. Finally, the importance of reporting tools that banking organizations must have in place to manage the vast amount of information data gathered from operational risk management systems is discussed. All these analyses present a solid platform for effective decision making concerning the assessment, control, and management of operational risks.

Chapter 10: Concluding Remarks

This chapter offers some concluding remarks and discusses future directions of operational risk management.

References are given at the end of every chapter for those interested in strengthening their knowledge beyond the scope of this book. All referenced documents written by the Basel Committee on Banking Supervision are available free of charge from their Web site at http://www.bis.org/bcbs/publ.htm. A list of acronyms is given in the appendix to ease understanding of the terms used throughout the book.

Acknowledgments

The authors would like to especially thank all those who supported them in various ways to enable them to complete this book. These include, first of all, their individual families, Athena Akkizidou and Nikos Akkizidis. Special thanks go to Vasilios Masmanidis and Christos Ventiadis for their support, Helen Sjöberg for her inspiration, and Maja Kotzmuth-Clarke and Stelios Apostolopoulos for their constant encouraging words. They would also like to thank Dr. Lampros Kalyvas for the valuable participation in discussions, feedback, and small contributions for the material of this book. Finally, the authors would like to mention the country of Sweden, always open to new ideas, which gave them the opportunity to first implement their ideas. They would also like to thank CRC Press and Auerbach Publications, members of The Taylor & Francis Group, for giving them the opportunity to publish their work.

About the Authors

Ioannis Akkizidis, Ph.D. is a business and risk analyst and the main architect of the approaches presented in this book. He has been developing and applying advanced mathematical algorithmic theories and practices to identify, model, map, evaluate, and optimize complex operational risks for banking organizations and big enterprises. He has extensive academic knowledge through his master's (M.Sc.) in control systems analysis and Ph.D. in artificial intelligence and applied mathematics. He has published several scientific and working papers from journals to newspapers, has presented at several international conferences, and has given ample talks on the subject of operational risk optimization and management. He has worked worldwide for many years in business and risk analysis and has designed and implemented advanced software tools for large organizations and financial organizations.

Vivianne Boucher eau, Ph.D. is a business and risk analyst. She has undertaken projects in the field of business performance, operational risk analysis, and optimization, as well as quality management. She has contributed to the design of the various methodologies on operational risk assessment, control, and management presented in this book. She has given seminars and talks on operational risk management and Basel II and has several years of working experience in the quality engineering field. She is also a qualified lead quality auditor for ISO 9001: 2000, has written numerous papers on the subject of total quality management, and has been a presenter at numerous international seminars and conferences. She has extensive academic background and working knowledge in this field. She obtained her combined bachelor's and master's degree (M.Eng.) in electronic and electrical engineering and her Ph.D. in quality engineering.

Contacting the Authors

The authors are pleased to have any feedback and are open to any discussion referring to the subject and material presented in this book. Please contact them via e-mail at:

- i.akkizidis@optimisation4business.com (Ioannis S. Akkizidis)
- v.bouchereau@optimisation4business.com (Vivianne Bouchereau)

I

OPERATIONAL RISK AND ITS MANAGEMENT

Chapter 1, Operational Risks in Financial Organizations

Chapter 2, Main Aspects of Operational Risk Management

This first part of this book, which consists of Chapters 1 and 2, introduces the idea of operational risks and how they affect financial organizations. It also focuses on the main aspects of managing operational risks in financial organizations.

Chapter 1

Operational Risks in Financial Organizations

Where there is money, there is risk.

—Paul Getty

Introduction

Managing risk is an old habit of human beings. In their day-to-day lives, people always seem to be worried about future risks. As a result, they end up investing in insurance or other investment methods to secure themselves against unforeseen risks. Accidents, environmental disasters, bankruptcy, and loss of business are risks that have plagued the human race since time began. Generally, no complete protection exists against every potential risk, but appropriate proactive measures to mitigate certain risks can be adopted. The same concept also applies to financial organizations. Understanding risks has always been a fundamental, if only implicit, management process in financial organizations. What is new is the following:

- The increased explicit awareness and consciousness of managers and senior management of risk issues
- The explicit and analytical approaches

- The greater awareness to direct an organization's risk profile toward those risks for which it has a comparative advantage in managing
- The pressure to allocate resources more consciously

Risk management was in its elementary stages until the 1980s. It was not recognized as part of the business management process but only as a method of taking precautionary measures when business went wrong. The concept was, "Do business and then measure the risks," whereas in today's economy, the concept is, "Measure the risk first, then do business." Thus, during the late 1980s and early 1990s, apart from profit-making goals, organizations were faced with other goals, such as accountability, transparency, and performance, as demanded by their investors. Risk management has always been a fundamental management process in financial organizations. It is a well-known fact that where there is money, a certain amount of risk must be involved. In the realm of the financial domain today, the term "risk" is being used more frequently. It is recommended that operations integrate risk management into decision making in the same way it has already integrated such critical factors as time, money, and labor. Managing risks effectively has become the duty of everyone involved in financial organizations. Nowadays, however, there is more pressure to avoid things going wrong while continuing to improve corporate performance. By monitoring risk more closely, financial organizations can minimize the required amount of reserve capital and maximize their profitability.

Good risk management is a decisive competitive advantage. It helps to maintain stability and continuity, and it supports revenue and earnings, a process for which senior management and boards of directors are increasingly called upon to ensure. The Basel Committee on Banking Supervision created the first Basel Accord in 1988 (as discussed in Chapter 3) to ensure capital allocation by examining market risk and credit risk within banking organizations. The new version, Basel II, finalized in June 2004, is set to modify its evaluation of credit risk and, more importantly, seeks to assess operational risk, an area previously not clearly defined in the financial services marketplace. It will give banks more flexibility in weighing those risks by providing several new options for calculating credit and operational risks. The bottom-line, less-risky loans should require less capital. The Basel Committee itself does not actually have any authority to impose capital-reserve requirements on the world's banks; instead, it formulates broad supervisory standards and recommends best practices, which it then turns over to regulatory authorities in its 13 member countries for implementation. The 13 members include the G10 plus Luxembourg and Spain (G10: Canada, Belgium, Germany, Italy, Japan, the Netherlands,

Sweden, Switzerland, United Kingdom, United States). Many nonmember countries are also seeking to comply with its recommendations.

Operational risk has existed as financial organizations evolved. Operational risk management in financial organizations as discussed throughout this book is preventive rather than reactive. It is based on the philosophy that it is irresponsible and wasteful to wait for an accident to happen and then figure out how to prevent it from happening again. Over the past several years, financial organizations have focused on developing sophisticated tools to measure market risk and credit risk. Today, operational risk has become another critical aspect in risk capital allocation. Unlike with market risk and credit risk, which mainly involve only risks associated with trading and lending, everyone in the organization can be a source of operational risk. The new Basel II Accord instigated by the Bank of International Settlement is undertaking a major effort to fundamentally increase the quantification of operational risk. Operational risk as the most recent area of risk management is therefore all set to face formal quantification through the regulatory process. The Basel Committee has observed through various surveys[1] that the current measurement of operational risk by banks is relatively undefined and qualitative in nature. Comprehensive, enterprisewide strategy and tactics toward risk can no longer be achieved by applying common sense only — although common sense remains crucial. There is a need for credible and relevant methodologies to define, identify, assess, measure, analyze, control, and manage risks. Operational risks are highly multifaceted, complex, and often interlinked. Although not avoidable, operational risks are manageable. Financial organizations and regulators and supervisors should be aware of the cost-benefit relationship of setting in place the quantification of operational risk, which involves data gathering, models, procedures, systems, and staff. The value of financial organizations increasingly lies in its intangible assets, such as data, knowledge, skills, people, network, reputation, and brand. These assets are bundled together in the organization and can also reflect in operational risks.

Although operational risk is not a new risk, deregulation and globalization of financial services, together with the growing sophistication of financial technologies, new business activities, and delivery channels, are making organizations' operational risk profiles (i.e., the level of operational risk's probability, impact, and exposure across an organization's activities and risk categories) more complex.

Regulators are currently examining operational and compliance risks under the Bank Secrecy Act,[2] USA Patriot Act,[3] Gramm–Leach–Bliley Act,[4] Basel II Accord,[27] Sarbanes–Oxley,[31] and Federal Financial Institutions Examination Council (FFIEC) guidelines.[5] The Bank Secrecy Act and the

USA Patriot Act require programs to be in place for anti-money-laundering, reporting of suspicious activity, large cash transactions, customer identification, and more. The Gramm–Leach–Bliley Act requires safeguards for customer information, privacy, and information security. The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) and Sarbanes–Oxley both require internal controls review across most departments, which are a subset of the bankwide risk assessment process. FFIEC information technology (IT) handbooks direct senior management and the board of directors to manage IT risks, including information security, business continuity, and disaster recovery.

Three excellent reasons for a banking organization to advance its operational risk program are as follows:

1. Regulators are going to require the organization to do so over time.
2. Taking a proactive attitude means doing it according to the organization's own timelines and on its own terms.
3. The organization's shareholders expect the organization to add value to its bank.

Financial organizations should not accept operational risks simply as fate but should deal with them intentionally. Financial organizations are thus challenged to do the following:

- Meet their compliance commitment.
- Employ best practices such as Basel II.
- Build an appropriate and effective operational risk management system.
- Assess, measure, analyze, and report operational risks.
- Design strategies to align and manage operational risks across the organization.
- Have timely and accurate reporting, tracking, and control of operational risks.
- Maximize the potential benefits of freeing up capital charge.

This chapter introduces several topics that form a basis for subsequent chapters. It begins by defining operational risks and why financial organizations should be concerned about them. This leads to a presentation of where operational risks exist in financial organizations, with concrete examples of where operational risks have caused major catastrophes in financial organizations in the past. Next, causes of operational risks in financial organizations are examined. The characteristics of operational risks are generally discussed; then further details are presented of how operational risk affects, or is affected by, IT. Finally, this chapter looks briefly at IT security. The layout of this chapter is presented pictorially in Figure 1.1.

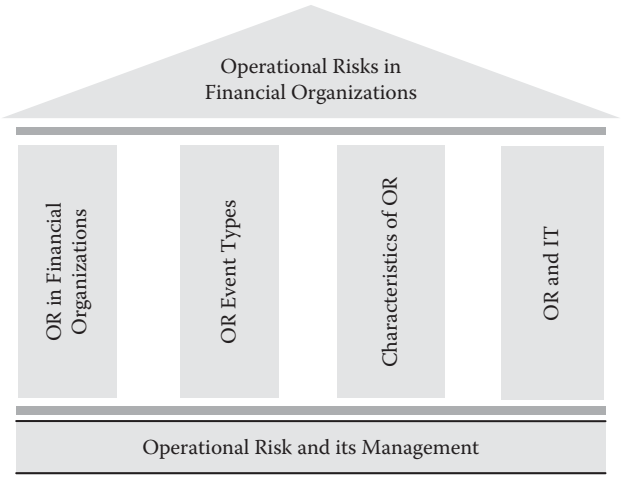


Figure 1.1 Layout of Chapter 1.

Operational Risks in Financial Organizations

Of all the different types of risks that affect financial organizations, operational risks can be among the most destructive and most difficult to foresee. Operational risks continue to receive keen attention among market participants and regulators, triggering dialogues and debates on the best ways to identify, measure, and manage this important risk. This recognition has led to an increased prominence of the importance of sound operational risk management in financial organizations and, to a greater degree, operational risk in banks' internal capital assessment and allocation processes. In fact, the banking industry is currently undergoing a surge of innovation and development in these areas. The extraordinary demands of setting up a robust yet sensible and practical operational risk management system are puzzling risk professionals in every industry, and even more in financial organizations, where the regulators set out very detailed requirements.

The Basel II Accord focuses on bringing together the world's financial organizations under a common regulatory framework, although the way to manage operational risk is different for each financial organization; after all, there are over 30,000 banks and an estimated 20,000 insurance companies worldwide. Basel II will enable banks to align regulatory requirements more closely with their internal risk measurement and to improve operational processes. Forward-thinking organizations recognize that the accord also provides a unique opportunity to modernize and upgrade their overall risk practices and risk infrastructure, specifically for credit and operational risk. For these banks, Basel II means more than

compliance; rather, it denotes the opportunity to achieve distinct competitive advantage in a tight global market. Some banking organizations have begun developing processes required by Basel II, but few if any organizations have made the operational risk framework a practical tool to drive bottom-line results by enhancing operational and performance effectiveness.

Management of risk in operations is not a new practice in banking; it has always been essential to prevent fraud, maintain internal controls, and reduce errors in transaction processing. In the past, however, banks relied on internal controls within business lines, supplemented by the audit function, to manage operational risk. By supplementing internal control with monitoring and managing operational risks more closely, financial organizations can minimize the required amount of capital reserve and maximize their profitability.

Defining Operational Risks

So far, this chapter has discussed operational risk without actually defining what it means. A definition of operational risk is thus needed. A common definition of operational risk has to be understood, accepted, and identical across a financial organization. A common practical definition of operational risk does not exist in literature or in the industry. Operational risk encompasses various risks inherent in business activities across an organization, and consequently, its losses have the potential to be of much greater magnitude. Operational risk is a broader risk discipline and recognizes that there are components of operational risks that underlie all other risks.

The term "operational risk" itself has been defined only in the past few years, although this type of risk has been around for hundreds of years. As opposed to the definitions of "market risk" and "credit risk," which are relatively clear, the definition of operational risk has evolved rapidly over the past few years. At first, it was commonly defined as every type of nonquantifiable risk faced by a bank. However, further analysis has refined the definition considerably. Theoretically, there are as many definitions as there are financial organizations. The British Bankers' Association (BBA) survey in 1999[6] showed that, although there is a broad agreement on the general concept of operational risk, diversity in some detailed aspects will continue to exist. Some definitions of operational risks are reproduced here:

- "Operational Risk is the risk of everything other than credit and market risk." (This is the definition of 15 percent of the 55 organizations surveyed.)[6]
- "Operational Risks are events, activities, or circumstances that can affect an organization and the achievement of business/quality objectives."

- "Operational Risk is 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 or controls" (Bank for International Settlements [BIS]).[7]
- "Operational Risk is the risk of losses resulting from inadequate or failed processes, people, and system or from external events."[8]

A survey conducted in June 2000 by the Risk Management Group (RMG) of the Basel Committee, through its Other Risks Technical Working Group (ORTWG),[9] indicated that although a range of definitions is presently used, there has been a high degree of convergence during the past one to two years. The following definition of operational risk, or close variants of it, is used by a large number of banks: "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events." Although some banks included legal risk in their definitions, almost all organizations reject the idea of including strategic and business risk in a regulatory capital charge (although many allocate economic capital for this).

Operational risks are only eliminated if a bank ceases to exist; and although market and credit risks are revenue driven, operational risks are not. Credit and market risks originate from outside the bank. In contrast, operational risks originate primarily from within the specific bank, except risks in the category "external" as discussed in the subsequent section. Losses from external events, such as a natural disaster that damages an organization's physical assets or electrical or telecommunications failures that disrupt the business, are somewhat easier to define than losses from internal problems, such as employees' fraud and product flaws. Because the risks from internal problems will be closely tied to a bank's specific products and business lines, they should be more organization specific than the risks due to external events.

Because operational risks exist in the natural course of corporate activity, there is a great emphasis on process orientation in the operational risk concept, which positions the definition of operational risk management closer to "total quality management." In the banking sector, operational risk resembles similar risks in industry more closely than it resembles market or credit risks in a bank. Operational risk should be managed whenever the way something is usually done is modified, to make the chances of success as great as possible, while making the chances of failure, injury, or loss as small as possible. It is a common-sense approach to balancing the risks against the benefits to be gained in a situation and then choosing the most effective course of action.

To further understand operational risks, it is important to view this type of risk in the context of the other risks that affect financial organizations. These risks are generally defined as follows:

- Credit risk
- Market risk
- Business risk, which is the risk of losses from business volume changes
- Insurance underwriting risk, which is the risk of losses from unexpected insurance claims volume
- Reputation risk, which is the risk of losses by not meeting stakeholders' expectations
- Strategy risk, which is the risk of losses from not choosing "to do the right thing"

The characteristics of operational risks are clearly different from other risks: market and credit risks are — with relatively objective market prices or ratings — willingly taken for revenue's sake. Operational risks are usually not willingly incurred and not priced in the market. Checks and controls of the market and reputation aspects cause every bank not to sustain operational losses because they increase expenses or affect the share prices.

Operational risk, simply put, is the risk associated with everyday activities of an organization, which involves the management of the performance of its processes, its people, and its systems to reach the expected business performance, targets, and objectives. Banks can tune their processes to reduce human errors and operational failures, and develop contingency plans for problems such as system breakdowns.

Under new regulatory rules, each bank will be allowed to adopt its own definition of operational risk. These individual definitions are subject to the requirement that they provide a clear understanding of what is meant by operational risk, consider the full range of operational risks facing the bank, and capture the most significant causes of severe operational losses. In arriving at the definition, the regulators recognize that the exact approach for operational risk management that a bank chooses "will depend on a range of factors, including its size and sophistication and the nature and complexity of its activities." Notwithstanding individual differences, the new Basel II Accord demands clearly documented strategies and oversight by the board and senior management, a strong operational risk culture, and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal escalation, reporting, and contingency planning.

Existence of Operational Risks in Financial Organizations

In the financial world, operational risks have always been present, and a newly established bank is confronted with operational risks even before

it decides on its first credit transaction or market position. Operational risks are primarily internal risks or "bank made." External risks must be handled differently and are largely insurable, or will increasingly become insurable. Operational risks include breakdowns in internal controls and corporate governance. These kinds of breakdowns can lead to financial losses through slip-ups, frauds, or failure to carry out operations in a timely manner. It might lead to a situation where the interests of the bank are compromised in some ways; for example, its dealers, lending officers, or other staff exceeding their authority or conducting business in an unscrupulous or hazardous manner. Other aspects of operational risks include major failure of IT systems or events such as natural mishaps, major fires, or other disasters. Operational risk surfaced in financial organizations since the 1990s as a chain of operational catastrophes affecting numerous financial organizations around the globe. The entire last decade of the twentieth century and the early part of the twenty-first century witnessed news of banking failures as front-page headlines all around the world.

One such event took place in late January 2003, when a computer worm called Sapphire spread quickly throughout the Internet and overwhelmed business computers with data. It was a nightmare for business operations, shutting down automatic teller machines (ATMs), congesting online ticketing systems, and blacking out an emergency call center in Seattle, Washington. It highlighted a fear of corporate managers and directors everywhere of operational risk. Operational failures such as those caused by Sapphire can result in huge financial losses and a damaged reputation. In 2001, Deutsche Bank and JPMorgan Chase disclosed large economic capital in insurance premiums for operational risks.[10,11] Table 1.4, later in this chapter, highlights further some operational risks that financial organizations have suffered in the past.

The increasing number of high-profile operational risk cases has left no doubt in the minds of bank managers and regulators that risk systems and risk-adjusted performance measures are potentially unreliable if they ignore operational risk. Shareholders, employees, rating agencies, equity analysts, and other stakeholders are demanding more focused operational risk information.

Each financial organization has its own individual and unique operational settings. Thus, being able to manage operational risk might require tailoring its definition to the organization's specific settings. Operational risks may tangibly reveal themselves in the likes of business disruption, control failures, errors, misdeeds, or external events and can be captured in five major operational risk categories, which are depicted in Figure 1.2:

1. Organization
2. Processes and Policies

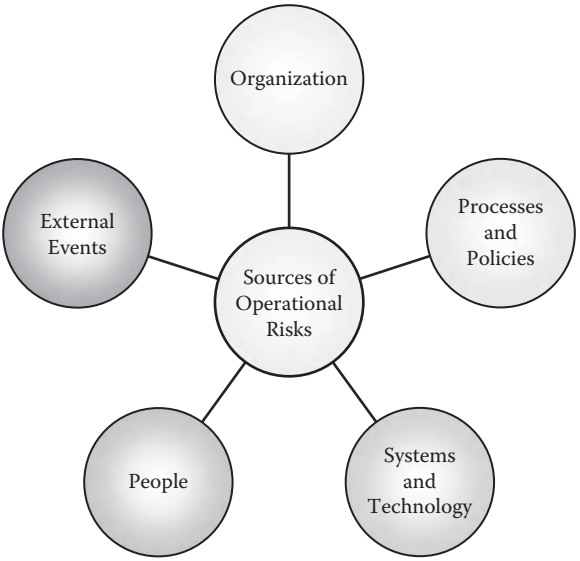


Figure 1.2 Sources of operational risk in financial organizations.

3. Systems and Technology
4. People
5. External Events

These five categories can be further expanded.

1. Organization

Whatever the reason for a change in business strategy, most major operational risk incidents happen during a period of change in the organization of the business. This could result in a change in staffing levels, a significant change in volumes of transactions as a result of a merger, new product or service launches, or the introduction of new computer programs. The banking history is littered with cases where merger strategies have gone horribly wrong and integration problems far exceeded the expected benefits of integration. In the 1980s and early 1990s many European banks sought their fortunes by buying into the U.S. market only to find that the crisis in the residential real estate market and the economy generally forced them to reverse their strategies. These types of risks also arise from such issues as project management, corporate culture and communication, responsibilities, allocation of resources, and business continuity planning. Furthermore, operational risks brought on by the risks embedded in the

governance and structure, outsourcing, and security of the organization form part of this type of risk.

2. Processes and Policies

Financial organizations use a huge number of processes to deliver their products and services to their customers. Process and policy risks can arise at any stage in the value chain. For example, marketing material can be mailed to the wrong customers; account opening and transactions can be processed incorrectly. Changes in legislation can render processes that were previously compliant out of compliance. Pension legislation changes in the United Kingdom caused a number of companies to mis-sell pension funds due to a lack of training in new procedures. The total cost to the financial services sector in the United Kingdom to rectify the problem was estimated in excess of £10bn.[13] Unexpected volumes of new businesses can also be a source of operational risk. There are numerous examples of new product and service launches that either failed or were seriously compromised due to the bank not being able to cope with the demands for its new product and services. In the urgency to get to market, key processing requirements can be overlooked. In brief, process and policy risks are related to the execution and maintenance of transactions, and to the various aspects of running a business. This includes risks such as mergers and acquisitions, new products and services risks, errors and omissions, inadequate or problematic security, inadequate quality control, and so forth. These stem from risks arising from such issues as model or methodology errors, design errors, and workflows with ambiguously defined process steps. It also includes risks arising from weaknesses in processes such as settlement and payment, noncompliance with internal policies or external regulations, or failures in products or in dealing with clients. Inconsistent or badly documented processes can put the business at risk even if they are followed perfectly. There are three organizational dimensions of internal processes where operational risks should be assessed, controlled, and managed. These dimensions are interrelated:

1. Business-line processes, including their functions
2. Corporate functions (IT, Human Resources, Finance, Legal, etc.)
3. General management

3. Systems and Technology

The growing dependency of financial organizations on IT systems is a key source of operational risk. Data corruption problems, whether accidental

or deliberate, are regular sources of embarrassing and costly operational mistakes. One bank made payments in excess of $150 million before a computer program patch involving a change in decimal points was found to have been incorrectly tested.[13] Another example of a system risk failure was discovered in February 2003 by staff at Provident Financial Group when they were testing the installation of a new financial model. As a result, Provident was forced to subtract $70.3 million from earnings statements released in the previous six years.[13] On November 20, 1985, the clearing operation of the Bank of New York (BNY) handled more than 32,000 Treasury security trades for the first time. This record volume triggered a software problem, preventing the organization from delivering Treasuries to buyers. The next morning was settlement day, and BNY began accumulating undelivered securities, which had to be financed by borrowings at the discount window of the New York Federal Reserve. BNY had to borrow a staggering $23 billion by the end of the day.[13] The following morning, with the software still malfunctioning, dealers were told not to deliver more Treasuries through the affected clearer, which led to a broadening of the disruption. Fortunately, the software was corrected later that day and clearing normalized. Because of a high concentration in the market for clearing services, a single malfunction in a single organization's system led to an expensive crisis.

General technology problems (operational errors that are technology related, unauthorized use or misuse of technology, etc.); hardware (equipment failure, inadequate or unavailable hardware, etc.); security (hacking, firewall failure, external disruption, etc.); software (computer viruses, programming bugs, etc.); systems (system failures, system maintenance, etc.); and telecommunications (telephone, fax, e-mails, etc.) are increasingly great sources of operational risks. The IT staff may precisely follow a perfectly designed process, yet fail to meet business goals because of problems with the hardware or software. Only IT people (who are sometimes far removed from the banking business) understand the technologies behind many new banking systems.

4. People

Risks arising from people are the most dynamic of all sources of operational risks. Internal controls are often blamed for operational breakdowns, whereas the true causes of many operational losses can be traced back to human failure. Every chief executive officer (CEO) has argued that people are the most important resource in their banks, yet the difficulty in measuring and modeling people risks has often led management to shy away from the problem when it comes to evaluating this aspect of

operational risk. Operational risk losses can occur due to workers' compensation claims, violation of employee health and safety rules, organized labor activities, and discrimination claims. People risks can also include inadequate training and management, human error, lack of segregation, reliance on key individuals, lack of integrity, and lack of honesty. These operational risks may be intensified by poor training, inadequate controls, poor staffing resources, or other factors. These types of operational risks cover losses intentionally or unintentionally caused by an employee, that is, employee errors (general transaction errors, incorrect routing of transaction, etc.), employee misdeeds, or that involve employees, such as in the area of employment disputes, human resource issues (employee unavailability, hiring or firing, etc.), personal injuries, physical injury (bodily injury, health and safety, etc.), and wrongful acts (fraud, unlawful trading, etc.).

In a people operational risk case, the United Kingdom's Financial Services Authority (FSA) fined ABN Amro £900,000 in April 2003[12] for "serious compliance failures." According to the FSA, the compliance environment within a financial organization is a fundamental protection against the spread of poor standards of conduct. ABN Amro failed to provide adequate resources for its compliance function, which resulted in the absence of robust compliance. In July 2003, JPMorgan Chase agreed to pay €135 million and Citigroup agreed to pay €120 million to the Securities and Exchange Commission for their roles in Enron's manipulation of its financial statements.[13] These are operational risks arising from fraud or incompetence, allowed by control weaknesses in processes or systems, failure of employees or the employer due to conflict of interest or from other internal fraudulent behavior. It is well known in most financial organizations that fraud is initiated from people and is one of the most important risks with unknown further implications. Human processing errors (for example, mishandling of software applications, reports containing incomplete information, payments made to incorrect parties without recovery, unnecessary rejection of a profitable trade or improper trading strategy due to incomplete information) are all examples of operational risk resulting from people. Even if an organization's processes and technology are flawless, human actions (whether accidental or deliberate) can put a business at risk.

5. External Events

Banks tend to have the least control over this source of operational risk, yet it still needs to be managed. External risks can arise from unexpected legislative changes, such as consumer affairs, and from physical threats,