MANAGING OPERATIONAL RISK

Practical Strategies to Identify and Mitigate Operational Risk within Financial Institutions

DOUGLAS ROBERTSON

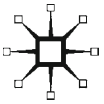
Managing Operational Risk

Managing Operational Risk

Practical Strategies to Identify and Mitigate Operational Risk within Financial Institutions

Douglas Robertson

palgrave
macmillan



MANAGING OPERATIONAL RISK

Softcover reprint of the hardcover 1st edition 2016 978-1-137-44215-4

First published 2016 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire, RG21 6XS.

Palgrave Macmillan in the US is a division of Nature America, Inc., One New York Plaza, Suite 4500, New York, NY 10004-1562.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

ISBN 978-1-349-56569-6 ISBN 978-1-137-44217-8 (eBook)
DOI 10.1007/978-1-137-44217-8

Distribution in the UK, Europe and the rest of the world is by Palgrave Macmillan®, a division of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Library of Congress Cataloging-in-Publication Data

Robertson, Douglas D.
Managing operational risk : practical strategies to identify and mitigate operational risk within financial institutions / Douglas Robertson.
pages cm
Includes bibliographical references and index.

1. Financial institutions—Risk management. 2. Banks and banking—Risk management. 3. Auditing, Internal. I. Title.

HG173.R57 2015
332.1068′1—dc23 2015019820

A catalogue record for the book is available from the British Library.

To Laura and Mariana

Contents

Illustrations

Figures

Tables

Acknowledgments

I would like to thank Leila Campoli and Brian Foster for first suggesting that a working paper from an obscure government regulatory agency might have the makings for a book. I would also like to thank Laurie Harting, Bradley Showalter, and Marcus Ballenger of Palgrave Macmillan for patiently helping that transformation take place, and Kristy Lilas and Meenakshi Venkat for excellent editorial assistance. Much of chapter 3 of this book originally appeared as Economics Working Paper 2011–1, March 2011, US Office of the Comptroller of the Currency (OCC). I would like to thank Oliver Berndt, Mike Carhill, Mark Levonian, Rebecca Miller, David Nebhut, Morey Rothberg, Desiree Schaan, Sherrill Shaffer, Kostas Tzioumis, Gary Whalen, and seminar participants at the Eastern Finance Association and Southern Finance Association for helpful comments and suggestions on that working paper. I wrote this book while employed as a Senior Financial Economist and Lead Expert for Regulatory Analysis at the OCC. I would like to thank Roger Tufts for comments on the manuscript. The views expressed in this book are solely those of the author and do not necessarily reflect those of the OCC or the US Department of the Treasury.

Acronyms

ABS	Asset-Backed Securities
AIG	American International Group
AMA	Advanced Measurement Approaches
AML	Anti–Money Laundering
ARM	Adjustable Rate Mortgage
BSA	Bank Secrecy Act
CDO	Collateralized Debt Obligations
CDS	Credit Default Swaps
DMAIC	Defining, Measuring, Analyzing, Improving, and Controlling
DTI	Debt-to-Income
EIC	Examiner-in-Charge
FDIC	Federal Deposit Insurance Corporation
FICO	Fair Isaac Corporation
GAO	Government Accountability Office
ISDA	International Swaps and Derivatives Association
LTV	Loan-to-Value
MRA	Matters Requiring Attention
NRSRO	Nationally Recognized Statistical Rating Organization
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
P&L	Profit and Loss
RMBS	Residential Mortgage-Backed Securities
SAR	Suspicious Activity Report
SCP	Synthetic Credit Portfolio
SEC	Securities and Exchange Commission

SIV	Structured Investment Vehicle
SPV	Special-purpose Vehicle
TALF	Term Asset-Backed Securities Loan Facility
UOM	Units of Measure
VaR	Value-at-Risk

1
Introduction to Operational Risk

The working definition of "operational risk" among financial institutions is the risk of loss from inadequate or failed internal processes, people, and systems or from external events.[1] Practically speaking, operational risk is the risk of loss from problems such as human error, system failures, and bad weather—to name a few of the many almost-inherent business complications that qualify as operational risks. Operational risk is just a relatively new term for some very old risks like fraud and embezzlement, and some newer risks like cybercrime and computer system failures.

Operational risks come in many forms and can cause losses of almost any size. The losses can be insignificantly small or large enough to destroy an institution almost overnight. Just as the term "operational risk" is relatively new, the methods and strategies for managing it are similarly new and still developing. To date, these operational risk management strategies have primarily involved measuring past operational risks and allocating capital to meet minimum regulatory capital requirements and, if possible, purchasing insurance or some other risk-transfer product. The objective of this book is to introduce and encourage the use of a third tool to identify, manage, and control operational risk, namely, quality assurance inspections. There is nothing new about the quality assurance

inspection methods themselves—they come directly from the auditor's well-worn toolkit—but their incorporation into the playbook for managing operational risk would open a crucial new front in the escalating battle against costly, destabilizing, and often destructive operational risks.

Any organization can apply quality inspection methods to any operational risk, with the likely exception of external events such as earthquakes and floods. Whereas contingency planning and drills are generally the best means for managing the risks posed by external events, quality inspection methods are more applicable to the other three sources of operational risk: processes, people, and systems. Processes, people, and systems are also inputs into an organization's production process, which yields products or services. If those three inputs are working well, then the quality of the final product or service will usually be the best the organization has to offer. If any of these inputs are performing inadequately, that is, they pose an operational risk, then the quality of the final product or service is likely to suffer, which in turn could damage the institution's reputation and profitability and thereby weaken its long-term outlook.

In this book, we examine several instances of operational failures in financial institutions that had severe consequences for the institutions involved. Because financial markets inextricably link many financial institutions to one another, we'll see how operational risks within one institution can quickly affect entire financial markets and even the regulatory agencies responsible for overseeing those institutions and markets. Our first example of such an infectious operational risk, which we consider in detail in chapter 3, originated in the US mortgage market in the early 2000s and led to the sequence of events that became the Great Recession. What was the operational risk that initiated the avalanche of losses that created

a crisis in credit markets and rapidly spilled into the broader US and global economies? It was an operational risk known as bad lending, but before we explore that operational risk in detail and explain why it is an operational risk problem rather than a credit risk problem, we need some additional background information on operational risks in general: the various types of operational risks, their characteristics, and the three fundamental ways to manage them.

Types and characteristics of operational risk

Although the specific operational risks with which any financial institution must contend will usually differ from one institution to the next, the operational risks across institutions are generally similar. Because a complete list of potential operational risks would be enormous and constantly growing longer as new products and product platforms emerge in the financial sector, a necessary first step in operational risk management is to sort operational risks into several broad categories. In addition to organizing an unwieldy area of risk management, categorizing operational risks will also help with subsequent risk measurement and resource allocation decisions.

There are several ways to think about categorizing operational risks. One way financial institutions often categorize operational risks is by sorting them according to the frequency and severity of losses attributed to the risk. It is common to subdivide both frequency and severity into low and high subcategories, which produces a simple 2-by-2 matrix, as shown in table 1.1. Distinguishing between low and high losses causes the operational risks to fall into one of four frequency/severity categories: low-frequency and low-severity risks, low-frequency and high-severity risks, high-frequency

Table 1.1 A 2-by-2 Operational Risk Matrix

		Severity of Loss	
		Low	High
Frequency of Loss	Low	Least Concern	High Concern
	High	High Concern	Greatest Concern

Source: Author.

and low-severity risks, and high-frequency and high-severity risks. As the degrees of concern shown in table 1.1 suggest, operational risks of low severity and frequency are generally of little concern to an institution. If, however, a business line introduces operational risks that are high frequency and high severity, then most institutions may want to avoid that business line.

Although the high and low distinction may be a useful simplification, it is important to remember that the frequency and severity categories actually reflect much broader and more continuous spectrums. For instance, the frequency spectrum can be subdivided into annual, monthly, weekly, daily, and even hourly categories. Indeed, as Michael Lewis, the author of several books illuminating the complex inner workings of financial markets, informs us, for high-frequency trading activities, the relevant frequency spectrum now extends into nanoseconds.[2] Similarly, the severity spectrum reflects dollar amounts of each loss, so operational risk managers could subdivide loss severity ranges into specific dollar amounts, for example, less than $10, $10–$100, $100–$1,000, and so on. Combining specific dollar amounts with specific frequencies would immediately help operational risk managers convey additional information about the extent of a particular operational risk exposure. For instance, consider the additional information conveyed in describing an operational risk as

leading to losses of less than $10 several times per month compared to saying an operational risk is a low-frequency/low-severity risk. Being specific about the dollar amounts associated with risks can help each institution determine the difference between low severity and high severity and show that what might be a low-severity event for a large bank could be a high-severity event for a small bank.

Regulatory reporting requirements for operational risks in the United States currently only apply to large banks. These reporting requirements look at seven loss-amount categories ranging from less than $10,000 to $1 billion or more.[3] This level of detail, of course, would result in a matrix that is much larger than a 2-by-2 matrix, so for discussion purposes the low/high distinction is useful.

In addition to classifications based on frequency and severity, we can also distinguish operational risks in terms of whether they originate internally or externally and whether the risk reflects an action that is intentional or unintentional. The author and professor Christopher Marshall has written an extremely useful overview of how financial institutions can measure and manage operational risks.[4] Much of this book applies the fundamental approach to identifying operational risk that Marshall describes. In discussing different characteristics of operational risks, Marshall also points out that another important distinction is whether the operational risk is controllable or uncontrollable. According to Marshall, an operational risk is controllable if an organization is able to prevent a loss or mitigate the risk. The proactive risk mitigation strategies described in chapters 3 and 4 are especially applicable to an institution's internal controllable operational risks. Whether those internal and controllable operational risks are intentional or unintentional is of less importance, and the frequency and severity of the operational risks will depend a great deal on the rigor with which

the financial institution applies those risk mitigation strategies. Overall, where a particular operational risk falls in terms of these various categories will often determine the appropriate risk management approach, the appropriate number of resources to dedicate to resolving the problem, and, therefore, the ultimate outcome for the institution.

Catastrophic operational risks

From a management perspective, perhaps one of the most important categorical distinctions for operational risks is between potentially catastrophic and noncatastrophic risks. A catastrophic operational risk is one that exposes the company to a loss so severe that it threatens the viability of the entire company. Many operational risks result in operational failures that occur on a small scale every day, that is, they are high frequency but low severity, and financial institutions tend to be familiar with these risks and are able to manage them with little or no incident. Occasionally, however, operational risks that lead to losses of $1 billion or more can explode onto the scene with dramatic and devastating effect. Many of these more dramatic and highly publicized examples of operational risk involve losses related to unauthorized trading. For example, unauthorized trading led to losses of approximately $1.3 billion by Barings Bank in 1995, $2.6 billion by Sumitomo Corporation in 1996, over $7 billion by Société Générale in 2008, and $2 billion by UBS in 2011. Trading losses were also responsible for JPMorgan Chase's $6 billion loss related to the London Whale events.

In an effort to help banks and their supervisors establish procedures for coping with operational risk, the Basel Committee on Banking Supervision (Basel Committee) created another means of categorizing operational risks by establishing seven broad types of operational risks for data-collection purposes.