ESSENTIALS of Risk Management in Finance

- Understand the major categories of risk that all organizations face and how they impact one another
- Utilize the latest risk management tools and technologies for making informed business decisions
- Learn how to apply practical, cutting-edge risk strategies that work across industries and across national borders
- Understand why most anti-fraud and corruption programs fail and how you can succeed
- Explore commonly used risk approaches in the banking, insurance, and brokerage industries

Anthony Tarantino
with **Deborah Cernauskas**

ESSENTIALS of Risk Management in Finance

Anthony Tarantino

with Deborah Cernauskas

WILEY

John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Tarantino, Anthony.
Essentials of risk management in finance/Anthony Tarantino with Deborah Cernauskas.
p. cm. — (Essentials series)
Includes bibliographical references and index.
ISBN 978-0-470-63528-5 (pbk.); ISBN 978-0-470-94633-6 (ebk);
ISBN 978-0-470-94634-3 (ebk); ISBN 978-0-470-94635-0 (ebk)
1. Financial risk management. I. Cernauskas, Deborah, 1956– II. Title.
HG173.T3457 2011
658.15'5—dc22

2010032745

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Preface

Beginning in 2007, the world suffered through the worst economic crisis since the Great Depression of the 1930s. The most sophisticated risk management strategies and techniques in the hands of global financial industry leaders failed in a spectacular and catastrophic manner. Quantitative and qualitative modeling, the core foundation of computational finance, also failed, even though it was in the hands of the most respected scientists and mathematicians utilizing massive computing assets and resources. However, organizations that applied prudential risk management approaches have fared far better. This included taking a holistic and enterprise-wide approach, plus an ethical tone-at-the-top, thus avoiding the seductive and nearly irresistible appeal of mortgage-backed securities and related investments.

The catastrophic failure in risk management and computational finance among the world's leading financial institutions demonstrates the need for a more holistic, interdisciplinary, and enterprise-wide approach to risk management, which combines accounting, economics, mathematics, operations, and technology. It also demonstrates the need for the correct tone-at-the-top, in which ethical considerations are weighed as heavily as shortsighted business considerations in risk or opportunity decisions.

To avoid repeating painful failures in risk management and ethics, it is essential for today's accounting, business, finance, audit, IT, and

not-for-profit managers to accept that risk management is everyone's job. It is also important to understand that the complexity of markets, financial products, and risk management techniques is a risk. The global financial crisis (also known as the Great Recession of 2008–2009) contains elements of every type of risk, which combined to overwhelm regulators, investors, and corporate governance.

This basic survey book is designed to provide a short and easy-to-follow introduction to financial risk management, covered in its major components: credit, market, operational, legal, and reputational, along with the relationship between corporate governance and risk management, and the techniques to control risk. We will also use the new ISO 31000 and 31010 risk standards to provide readers with the means to conduct their own risk assessments and risk alignments.

There are some mathematical concepts included, but they are kept at levels that general readers will find easy to grasp.

Readers will acquire a good basic understanding of the major areas of risk exposure that all organizations, both public and private, face in operating in today's complex global marketplace. Risk management is an essential element in all business activities. As a consequence, notions of risk management have quickly changed from a cost of doing business and distraction to acceptance as an essential part of any viable organization.

This Essentials book involves an analysis of contemporary theories and techniques in risk management used in a variety of industries. It also provides insights into best practices and next generation techniques.

Readers entering new careers will find that the book prepares them for government, not-for-profit, business, and IT positions in which risk management will play an ever-expanding role. Experienced professionals will find it a handy reference guide. Although limited as an overview, this book provides extensive references and links so readers can easily dive deeper into the coverage areas.

Organization of this Book

The book provides an overview of financial risk management in the introduction. The second chapter surveys the major risk management standards, frameworks, and associations in widespread use today.

Chapter 1 Introduction to Risk Management

Chapter 2 Risk Frameworks and Standards

The new ISO 31000/31010 risk management framework and Six Sigma for its approach to risk assessments and risk alignments are discussed in the following chapters.

Chapter 3 Conducting Your Own Risk Assessment and Alignment

Chapter 4 Six Sigma in Risk Assessments

Essentials of Risk Management in Finance uses the Basel II categories of risk management, which identify operational, credit, market, and liquidity risk. We treat legal risk, financial crimes, and internal controls as subsets of operational risk. We treat portfolio risk as a subset of market risk. We also include other important areas of risk—reputational, information/data, and product. The Basel committee also identified reputational risk as important, but beyond the scope of the current framework. We treat it as a consequence of other operational risk failures. The categories and subcategories of risk are:

Chapter 5 Operational Risk

Chapter 6 Legal Risk

Chapter 7 Financial Crimes (Fraud and Corruption)

Chapter 8 Internal Controls (U.S. and International SOX)

Chapter 9 Environmental and Product Risks—Sustainability

Chapter 10 Data Governance and Risk

We next discuss risks associated with the marketplace and investment portfolios.

Chapter 11 Market Risk—From Value at Risk to Black Swans

Chapter 12 Volatility, Risk Aversion, and Portfolio Management

We then provide an overview of the risks associated with credit, which is a universal issue for all those not doing business on a cash basis.

Chapter 13 Credit Risk

We continue with a discussion of corporate governance, including the compensation issues around the principal/agent problem, and alternatives to Western approaches (i.e., Islam).

Chapter 14 Corporate Governance and Compensation

Chapter 15 Faith-Based Risk Management—Shariah

We end with a brief overview of the most dangerous types of risk enterprises face: reputational, liquidity, and solvency.

Chapter 16 Reputational Risk

Chapter 17 Liquidity and Solvency: Enterprise-Ending Risks

Basel III Update

While this book was going to press, the oversight body of the Basel Committee on Banking Supervision announced revisions to the Basel II capital accords resulting in more stringent capital requirements. Basel III outlines a stepped process whereby banks will move from a 2 percent core capital ratio to a 7 percent core capital ratio over the next several years. An additional round of regulations for systemically important global banks is under development by the Basel Committee.

Basel III will profoundly impact us all and requires a survival guide. While we discuss Basel III in general terms in this book, we are

preparing an *Essentials of Basel III* to fully prepare you for the tightening of credit markets, the impact on commodity prices, and what to expect from the central banks of major economies like the United States, China, Japan, and the European Union. Bankers fear that tougher capital requirements will stifle lending and economic growth.

Acknowledgments

This text would not have been possible without the support and encouragement of the faculty and students of Santa Clara University's Leavey School of Business. Thanks to George Chacko, Sanjiv Das, and Carrie Pan, faculty in the finance department at SCU, for guidance and mentoring. The text is based on the MBA and undergraduate risk management classes taught in 2009 and 2010.

We also wish to acknowledge the support and encouragement of our Wiley colleagues and friends: Tim Burgard, our senior editor; Helen Cho, our senior editorial assistant; and Laura Cherkas, our production editor.

Special thanks go to Alexandra Tarantino for final editing of production proofs.

Contents

CHAPTER 1

Introduction to Risk Management

To avoid repeating the painful failures in risk management that occurred during the global financial crisis of 2007 to 2009 (also known as the Great Recession), it is essential for today's business, IT, risk, compliance, and audit managers to understand the big picture of risk management and to accept that risk management goes along with every position in business, technology, accounting, and finance. This is also true for many managers in the not-for-profit and government sectors.

This book is designed to provide an introduction to financial risk management, including operational, credit, market, reputational, liquidity, solvency, legal, and portfolio risk. These categories are based on the Basel II Capital Accords used by the global banking industry, but are applicable to all enterprises and organizations.

You will acquire an understanding of the major areas of risk exposure that all organizations, both public and private, face in operating in today's complex global marketplace. Risk management is an essential element in all business activities.

You will also be provided with actionable methods, techniques, and tools to improve risk management in your organization. This includes the basics of conducting risk assessments and risk alignments.

Definition of Risk and Financial Risk Management

Definitions of *risk* typically refer to the possibility of a loss or an injury created by an activity or a person. Risk management seeks to identify, assess, and measure risk and then develop countermeasures to handle it—not to eliminate risk.

Financial risk management applies a systematic and logical approach to uncertainties in operations, reputation, credit, liquidity/solvency, portfolios, and markets. Without risk management, an organization would simply rely on luck to avoid disasters. Risk management typically means seeking to mitigate and minimize the impact of risk, which is fundamentally different from avoiding it entirely. An organization that is completely risk averse is not likely to be attractive to investors and may be doomed to ultimately fail.

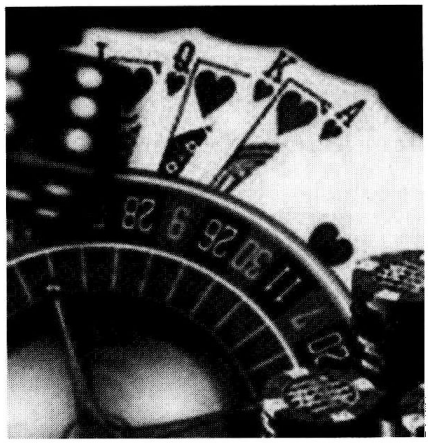
Risk should not be viewed as inherently bad. All opportunities come with some degree of risk—two sides of the same coin.

Gambling, Investment Risk, Chance, and Probability

Gambling can be defined as playing a game of chance for money or stakes. It requires one to risk money, or other things of value, on the outcome of something involving chance. *Investing* is to put money or other things of value to use by an expenditure or purchase in an investment vehicle that offers profitable returns. An investment vehicle may be a security or derivative, and can range from an asset-backed security to a stock or bond. An investment vehicle is used to make a profit on capital invested in it.

There is not a clear distinction between gambling and investment risk, but one can argue that risk taking in investments is good and adds capital to markets and thus contributes to society. One can also argue that gambling is inherently bad and adds limited value to society, although it does support some economies—Native American tribes, Las Vegas, and so on. Ironically, gambling risks are more identifiable,

measurable, and quantifiable than investment risks. Investment risks can be mitigated, whereas gambling risks typically cannot.



Risk can also be viewed as *probability* or the *chance* of making an incorrect decision. The risks of making a wrong decision are unique to the decision being made and may be realized only if a wrong decision is made. Unlike gambling, chance, and probability, risk management offers mitigation techniques.

Enterprise and Systemic Risk

Enterprise risk can be viewed as all processes that present risk to an organization. *Enterprise risk management (ERM)* comprises the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. The goal of ERM is to provide a framework for risk management that:

- Identifies specific events, situations, and environments relevant to the organization's objectives and their applicable risks and opportunities.
- Assesses those risks in terms of their likelihood and consequences.
- Develops a risk mitigation strategy appropriate to the exposure (balancing the mitigation costs and benefits).
- Monitors and reports on the risk mitigation progress.

ERM mitigation strategies include:

- Avoidance: Ending the activities and processes that created the risk.
- Reduction: Reducing the likelihood and/or the consequences the risk through mitigation.
- Transference: Transferring or sharing a portion of the risk via insurance or other vehicles.
- Monitoring: Ongoing tracking and auditing of mitigation counter measures.
- Acceptance: Accepting the risk and taking no action.

Systemic risk is a term now in common use because of the global financial crisis and is typically used to explain the risk to an entire national economy and society caused by enterprise risk failures of large institutions deemed too big to fail. It is probably more accurate to describe these organizations as too interconnected to fail. Their size does present risk to the overall economy, but it is their ability to create a domino effect in which their failures cascade down into the failure of several other organizations that compels national treasuries to intervene. Lehman Brothers and AIG are the poster children for systemic risk failures in the last few years.

EXECUTIVE INSIGHT

Systemic Risks Increase after the Global Financial Crisis

Systemic and enterprise risks are distinct but very much interrelated. The catastrophic enterprise risk failures of Lehman Brothers, AIG, and several global banks presented a systemic risk to the United States and several Euro Zone economies. Interestingly, the large majority of my Santa Clara University MBA students expressed concerns that the global financial crisis has

increased our systemic risk for two reasons. First, national governments have set a bad precedent of bailing out large corporations rather than letting them fail, and thus have rewarded their reckless risk taking. Second, the major consolidation of banks reduces the distribution of risk so that the surviving banks present an even larger systemic risk. Their concerns are well founded, especially because there has been little government action to address the huge unregulated credit default swap (CDS) and derivatives markets or to reform rating agencies.

Relationships among Governance, Risk, and Compliance

Just as risk and opportunity go hand in hand, risk goes hand in hand with governance and compliance. *Governance* is the relationship between those who govern and those whom they govern over. *Compliance* is the system of laws, regulations, and standards that control the governance and risk management process. It may be best to understand the compliance side of this triangle as a hierarchy with laws at the top and enterprise-level tasks at the bottom.

- Laws are created by national, state, and local legislatures.
- Regulations are created by agencies and typically make the rules that public and private companies must adhere to.
- Standards are created by regulatory agencies and international organizations that establish the audit standards by which compliance to regulations are validated.
- Enterprises create policies (higher level) and procedures (detailed level) to comply with standards by which they will be audited.
- Procedures lead to a large number of specific and auditable tasks to enforce policies, standards, regulations, and laws.

TIPS AND TECHNIQUES

The Hierarchy of Laws, Regulations, and Standards

A common misconception is that enterprises only comply with national and state laws. Although this is true on the surface, enterprises are measured by how they pass statutory (legally required) audits against compliance and risk standards and frameworks (addressed in Chapter 2). These audits are conducted by government regulators and external auditors. Standards are the detailed and actionable face of laws and regulations. In the case of the Sarbanes-Oxley Act (less than 30,000 words), public companies in the United States must follow the audit standards from the Public Company Accounting Oversight Board (PCAOB). The PCAOB's Audit Standards 1, 3, 4, 5, and 6 total more than 50,000 words. Auditors create audit questionnaires, process charts, risk/control metrics, audit test scripts, findings, and remediations that typically run into thousands of pages. Enterprises create general policies and detailed procedures to pass PCAOB and other statutory audits. Each procedure comprises a multitude of required tasks and supporting documentation.

The pyramid graphic in Exhibit 1.1 is a good way to view this hierarchy.

Risk Management and Internal Controls

The process that an organization, its internal auditors, its external auditors, and its regulators would typically follow to validate the effectiveness of internal controls that impact financial reports would typically include these steps:

- Identify business processes, especially those impacting financial reporting.
- Identify the risks associated with each process.