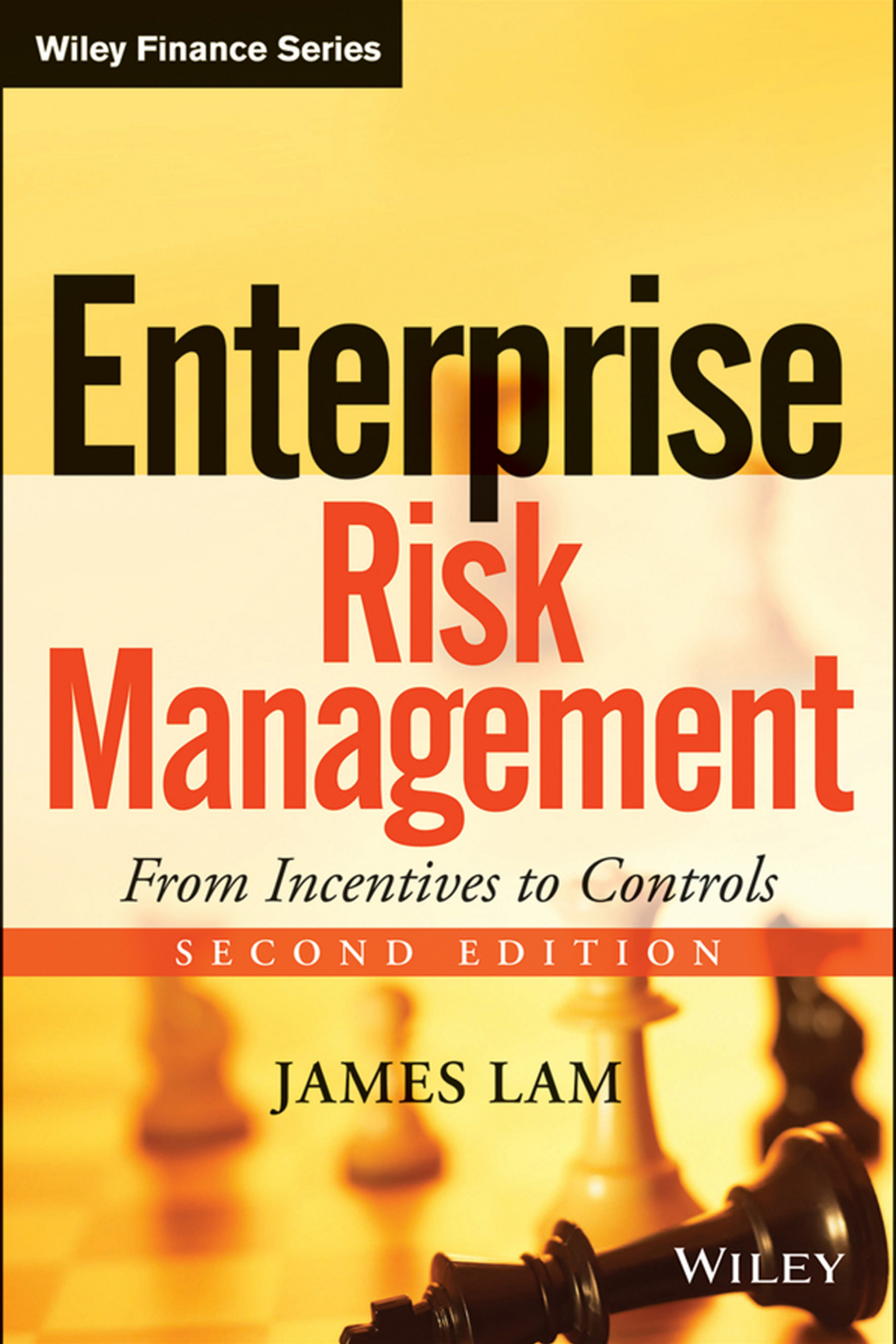
Wiley Finance Series

Enterprise Risk Management

From Incentives to Controls

SECOND EDITION

JAMES LAM



WILEY

Praise for the First Edition of *Enterprise Risk Management*

"In the aftermath of Enron, WorldCom, and Sarbanes-Oxley, every publicly traded company should be concerned about risk management. This book takes a pragmatic approach to risk management that can benefit any CEO or senior executive. Lam lays out clear strategies to address what is often a highly complex issue."

—William L. Walton, Chairman and CEO,
Allied Capital Corporation

"Author James Lam provides one of the most practical, insightful books on risk management that I have read in the last thirty years. It clearly reflects experience and deep understanding of the art as well as the science in risk management practices. A must-read for all who wish to advance risk management practices in their businesses."

—Sandra Jansky, Executive Vice President, Chief Credit
Officer, SunTrust Banks, Inc., (Chairperson,
Risk Management Association)

"In this book, James Lam has provided an effective overview of business risk. *Enterprise Risk Management* will be useful to professional risk managers and business executives seeking to understand the latest tools and organizational approaches."

—Robert Simons, Charles M. Williams Professor of Business
Administration, Unit Head — Accounting & Control,
Harvard Business School

"The most comprehensive and engaging handbook on enterprise risk management, written by the pioneer of the chief risk officer function. Filled with practical examples and lessons learned, this book is destined to become one of the most widely read primers on today's top business initiative. James Lam is *the* authority on enterprise risk management, and I highly recommend this book to all board directors, senior executives, and risk managers."

—Cassandra R. Schultz, Vice-President &
Chief Risk Officer, KeySpan Corporation

"James Lam's book *Enterprise Risk Management: From Incentives to Controls* provides an insightful roadmap to best practices in risk management. Based on a solid and successful career in risk management, James' advice is both timely and relevant and should be required reading for all risk management professionals."

—Michael J. Litwin, Chief Credit and Risk Officer,
Merrill Lynch Capital

"It's hard to imagine a more timely book. James Lam provides us with an excellent overview of enterprise risk management. A worthwhile read for professionals in a wide range of industries — from financial institutions to energy firms."

—Richard L. Sandor, Ph.D., Chairman and
Chief Executive Officer, Chicago
Climate Exchange, Inc.

"This book provides highly user-friendly insights into the many theoretical and practical aspects of enterprise-wide risk management. The case studies are particularly timely and provide a deeper understanding of the day-to-day real world complexities of implementing an effective risk management program."

—Dr. Robert Mark, Chief Executive Officer, Black Diamond

"While enterprise risk management has been a hot topic for discussion and debate, Lam manages to provide us with the first fully developed framework on the subject. Essential reading for anyone interested in the subject of risk and the successful implementation of risk management."

—Tobey J. Russ, President & Chief Executive Officer,
Chubb Financial Solutions, LLC

"*Enterprise Risk Management* is managerial science. James Lam has been a consistent voice for the business benefits of risk management and has thoughtfully and clearly articulated the business case for ERM. Long at the forefront of the profession, even having coined the title "Chief Risk Officer", James uses real-life examples, practical suggestions and insights from his many years of practice to simplify risk management without being simplistic. This is a must-read for CEOs, CFOs, board members and others who want and need to know of this modern discipline to business management."

—David R. Koenig, Chair of the Board of Directors,
Professional Risk Managers' International Association

"Our bank has greatly benefited from the implementation of enterprise-wide risk management. The concepts introduced by James Lam through case studies, theory, and his business experiences provide insightful analysis and form the foundation for any broad based risk management program. This book is an excellent read for managers of all levels responsible for risk management."

—William C. Nelson, Vice Chairman and
Chief Risk Officer, Bank of Hawaii Corporation

Enterprise Risk Management

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Australia and Asia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Finance series contains books written specifically for finance and investment professionals as well as sophisticated individual investors and their financial advisors. Book topics range from portfolio management to e-commerce, risk management, financial engineering, valuation and financial instrument analysis, as well as much more.

For a list of available titles, visit our website at www.WileyFinance.com.

Enterprise Risk Management

From Incentives to Controls

Second Edition

JAMES LAM

WILEY

Cover Design: Wiley
Cover Image: © iStockphoto / claudiobaba

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

Library of Congress Cataloging-in-Publication Data:
Lam, James.
Enterprise risk management : from incentives to controls / James Lam. — Second edition.
pages cm — (Wiley finance)
ISBN 978-1-118-41361-6 (hardback); ISBN 978-1-118-83436-7 (ebk);
ISBN 978-1-118-83443-5 (ebk)
1. Risk management. I. Title.
HD61.L36 2013
658.15'5—dc23

2013034352

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my parents, Kwan Lun and Mary, who took the greatest risk of their lives when they gave up their comfortable teaching careers in Macao and moved our family to New York City in 1971. While their lives became harder, their decision has opened up a whole new world of opportunities for me and my sister, Lily. With deepest love and appreciation I dedicate this book to my dad and mom.

Contents

Preface

Plato once said that every man should have a son, plant a tree, and write a book. Well, with my wife Pam, we have three sons—our eldest son Brandon and our twins Austin and Garrett. I've planted several trees, mostly with the help of my gardener. And this is my first book, and it is on my forte, risk management.

I have spent my entire career of 30 years in risk management. About half of that time I've worked as a consultant, preaching the gospel of best practices in risk management. The other half of my career I've spent in industry, trying to practice what I've preached under the realities of day-to-day business. More recently, in November of 2012 I joined the Board of Directors of E*TRADE Financial Corporation, where I chair the Risk Oversight Committee and am a member of the Audit Committee. My rotations through these three roles—as consultant, manager, and board member—have taught me that successful risk management is all about balance.

Firstly, risk management is about balancing risk and reward. Interestingly, the Chinese characters for risk (危机) are actually the combination of the characters for danger and opportunity. Business leaders are natural risk takers because they were put into leadership positions as a result of past successes. The challenge for leaders is to take *intelligent* risks. Running a successful business is all about pursuing the right business opportunities given the company's financial and managerial capabilities.

Risk management is also about balancing art and science. Considerable attention has been paid to advances in quantitative risk management—perhaps too much attention. Pick up the average risk management book or journal and the major focus will typically be on derivatives or risk measurement techniques. Risk products and models do play an important part in risk management, but it can be dangerous to put too much emphasis on them. Consider the collapse of Long-Term Capital Management (LTCM), a hedge fund managed by Nobel Prize winners whose mastery of the most sophisticated risk products and models was second to none. As LTCM's troubles reminded the world, the scenarios that lead to financial disasters happen, almost by their nature, when there is an unexpected confluence of events. Such scenarios are very difficult for models to predict. So there

remains an element of art in risk management, which is based on management experience and judgment.

Finally, risk management is about balancing processes and people. A company can survive and may even thrive if it has good people and bad processes, but it cannot if the reverse is true. At the end of the day, a company's risk profile is driven by the decisions and actions of its employees. While risk management processes such as risk reporting and audit can provide useful monitoring, it is more important to ensure that the right people are in place to begin with, and that they are motivated by the right culture and incentives. Risk management is ultimately about people.

The Second Edition of *Enterprise Risk Management* is organized into five main sections. The first, Risk Management in Context, provides an introduction and sets the foundation for the book. We will begin this section by reviewing why a company should strive for a balance between risk and return, including some basic reasons with regard to why risk management is an important management issue. As has been wisely said, history tends to repeat itself unless we learn from it, so we will go on to discuss the lessons to be learned from the major financial disasters of years past. The reader may be familiar with some of these cases discussed throughout the book, while others will hopefully be new. While the particular circumstances of these financial disasters differ significantly, there are uncanny similarities in their themes and causes, which can be distilled into seven essential lessons to be learned. After drawing these lessons from the past, we will analyze the key concepts, processes, and tools underlying risk management.

In the second section, The Enterprise Risk Management Framework, we will start by discussing the business rationale for integrating risk management processes, as well as the seven building blocks for developing an enterprise risk management program. We will also consider the role of a chief risk officer. In the rest of Section II, we will examine each of the building blocks in greater detail, specifically the control processes and practical approaches that apply to each building block.

In the third section, Risk Management Applications, we will study the applications of risk management in two dimensions—functions and industries. We will begin by discussing the functional requirements for credit, market, and operational risks. We then turn to a deliberation of how risk management has evolved from a control function, strictly concerned with minimizing downside risk, to one that enables performance optimization. Throughout the rest of this section, we will consider risk management in four key industry segments—financial institutions, energy firms, and nonfinancial corporations. In each industry segment, we will discuss key business and risk management trends, as well as contrast financial disasters and best-practice applications.

In the fourth section of the book, A Look to the Future, we will appraise emerging topics in risk management with respect to people and technology. In the First Edition of *Enterprise Risk Management* (2003) I had made 10 predictions on the future of risk management. As a follow-up, this section provides a summary of a June 2012 *Risk Professional* article written by Bill Scotti that revisited those predictions in order to see how prescient they were.

The final section of the book, ERM Implementation, is entirely new for the Second Edition. We will examine the key implementation requirements as companies move up the Enterprise Risk Management (ERM) Maturity Model; these requirements begin with the tone from the top regarding the role of the board. Next, we will discuss risk assessment, which is an ERM tool used by the majority of companies. However, as with quantitative models such as value-at-risk, risk assessment (a qualitative tool) can be fraught with potential pitfalls if not used appropriately. Given that one of the most critical success factors for ERM is the integration of risk management into business processes, we will discuss applications and examples of risk-based decision making. Finally, we will review how to design and implement effective dashboard reporting for management and the board.

Acknowledgments

This book is a reflection of my 30-year career in risk management. As such, I should first thank two of my early mentors. Charlotte Chamberlain, of Jefferies & Company, contributed to my professional development by challenging me to improve my writing and presentation skills. Charlotte was also a risk taker when she hired me, at age 23, as vice president in charge of asset/liability management for Glendale Federal (then a $15 billion bank). Jon Moynihan, of PA Consulting, taught me that a successful professional must develop a T skill set with both broad general management skills (the horizontal line) and deep technical expertise (the vertical line). Based on Jon's advice, I've strived to develop business management and risk management as my T.

Effective risk management is driven by not only sound theory, but also sound practice. Best practices in risk management can only emerge when sound theories and models are tested in the confines of the real world. Two individuals provided me with significant opportunities in this regard. Rick Price hired me in 1993 to help set up a new capital markets business at GE Capital, and gave me the first opportunity to define the role of a chief risk officer in managing market, credit, and operational risks. Jerry Lieberman was very supportive of the enterprise-wide risk management program that I established at Fidelity Investments between 1995 and 1998, especially in managing operational risks and balancing the hard and soft sides of risk management.

This book features several case studies that illustrate approaches to implementing best practices. In order of appearance, I would like to thank Jim Brockbank of EDC for the case study on credit risk, Leslie Daniels-Webster of JP Morgan Chase for the case study on market risk, Mike Litwin of Heller for the case study on operational risk, and Bob Mark, formerly CRO of CIBC, for the case study on ERM at financial institutions.

I would also like to thank the partners and consultants who provided invaluable input to me while we worked together at Oliver, Wyman & Company and ERisk. Special thanks go to Marlyn Bilodeau, Kim Birkbeck, Alexia Dorozynski, John Drzik, Jennifer Pence, Anna Lewis, Rob Mackay, Duncan Martin, Rebecca Prout, Anna Liu, George Morris, Peter Nakada,

Curtis Tange, and Tom Yu. I am especially grateful to Sumit Paul-Choudhury, who provided extensive editorial support and input. His contributions are reflected throughout this book.

For the second edition, I would like to thank my research team from Wellesley College. Special thanks go to Camille Basurto, Melissa Chen, Virginia Hung, Bridgid Ruf, Chelsea Shen, and Elizabeth Vandorpe. I want to especially thank Maymay Liu for her significant research and writing support.

Finally, I would like to thank my editor Bill Falloon and Development Editor Meg Freeborn from John Wiley & Sons. Bill has been involved in the risk management field for many years and it is truly a pleasure to work with someone who understands the subject matter.

SECTION

One

Risk Mangement in Context

CHAPTER 1

Introduction

One evening in the autumn of 1995, I flew into Boston to have dinner with Denis McCarthy, then the chief financial officer (CFO) of Fidelity Investments. McCarthy was the person to whom I would report if I accepted an offer to become the first chief risk officer for the corporation. I asked him what the main objective would be for this new position. His reply: "We want to operate in an environment in control, not a controlled environment."

I took that job with the understanding that Fidelity wanted to improve its risk management practices, but not at the price of destroying the entrepreneurial spirit and product innovation that had made it the largest mutual fund company in the United States.

Fidelity was not alone then and is not alone now. Every business faces the parallel challenges of growing earnings and managing risks. A thriving business must identify and meet customer needs with quality services and products; recruit and retain talented people; and correctly make business and investment decisions that will lead to future profit opportunities. However, the pursuit of new profit opportunities means that a business must take on a variety of risks. All of these risks must be effectively measured and managed across the business enterprise.

Otherwise, today's promising business ventures may end up being tomorrow's financial disasters. As I am fond of telling audiences when speaking on the importance of risk management: "Over the longer term, the only alternative to risk management is crisis management—and crisis management is much more expensive, time consuming, and embarrassing." The majority of such audiences have experienced one or more crises in their time, and so this is a message that rings true.

Every business decision involves an element of risk. There are risks involved in making investments, hedging with derivatives, or extending credit to a retail customer or business entity. There are also risks involved when developing and pricing new products, hiring and training new employees, aligning performance measurement and incentives with business objectives, and establishing a culture that balances revenue growth and risk management.

Over time, individual business decisions and risks collectively build up into a company's overall risk portfolio, which will have a unique risk profile. This risk profile will determine the company's earnings, and earnings volatility, over the business cycle. Some decisions will be winners and some will be losers. Some risks will offset each other, some risks will be unrelated to each other, and some will compound each other. In order to manage risk effectively, a business must address not only its underlying risks, but also the inter-relationships between them.

As we will see from the numerous case studies discussed in this book, ineffective risk management can lead to reduced earnings or even bankruptcy. However, risk management means different things to different people. In this book, risk management is defined in its broadest business sense. Risk management is not just about using derivatives to manage interest rate and foreign exchange exposures—it is about using a portfolio approach to manage the full range of risks faced by an enterprise. Nor is risk management only about establishing the right control systems and processes—it is also about having the right people and risk culture. And although the term has come to have some negative connotations, risk management is not only about reducing downside potential or the probability of pain, but also about increasing upside opportunity or the prospects for gain.

Individual investors managing their portfolios must be careful when it comes to the amount of risk that they take on. If they take on too much risk, perhaps by making aggressive investments, the losses could exceed their risk tolerance, or be too uncertain for comfort. On the other hand, if they fail to take on *enough* risk by making conservative investments, they may earn returns that are stable, but inadequate for achieving their financial objectives.

Striking an optimal balance between risk and return is not only important to the individual investor, it is also an imperative for business management. The concept of "no risk, no return" is widely accepted in the business world. A corollary to that concept is "higher risk, higher return", a positive relationship illustrated in Figure 1.1. This is how many people think about the trade-off between risk and return, and it has the virtue of simplicity. However, it is certainly not valid if risk is put into its proper perspective.

A better way to think about risk and return is illustrated in Figure 1.2. The focus is no longer on the relationship between risk and *absolute* return, but about the *relative* or *risk-adjusted* return. A company in Zone 1 is not taking enough risk, and its capital is being underutilized. This company would be better off increasing risk through a growth or acquisition strategy, or reducing capital through higher dividends. In Zone 3, however, the company is taking too much risk. This company's risk level is above and beyond its risk absorption capability in terms of capital and liquidity resources, and/or its risk management capability in terms of people and systems.

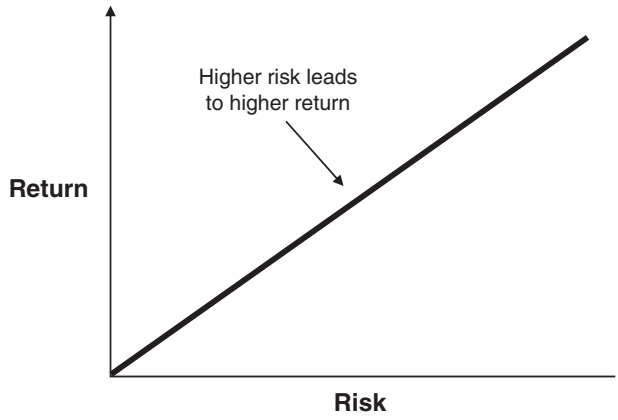


FIGURE 1.1 Risk and Absolute Return

In Zone 2, the company has found the sweet spot that optimizes its risk/return profile. The problem is that most companies do not even have good information on enterprise-wide risk exposures (which is to say, where they are on the horizontal axis), let alone where they are on the risk-adjusted return curve. To make matters worse, the net present value (NPV) and economic value added (EVA) models frequently used in strategic planning naturally favor higher-risk investments unless proper adjustments are made

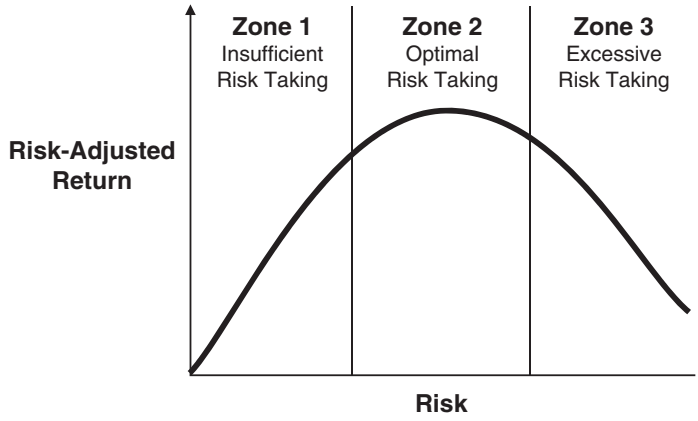


FIGURE 1.2 Risk and Relative Return

to account for risk. Over time, investments guided by these unadjusted models may inadvertently lead a company to drift into Zone 3.

A principal message of this book is that a company should develop an integrated approach to measuring and managing all of its risks in order to optimize its risk/return profile. A key management requirement for risk/return optimization is to integrate risk management in the business processes of the company.

We've seen, then, that risk is an inescapable part of doing business and argued that a business should strive toward its optimal risk-return profile. However, there is another question that deserves examination: why manage risk? Indeed, why read this book?

A company could conceivably agree that it bears risks but feels it inappropriate to manage them, rather than simply live with them. Risk management may seem to be irrelevant, too costly, or not in accordance with the interests of the company's stakeholders. Some academics have argued positions close to these, as we will see. Certainly, before a company invests money and other valuable resources into risk management (and before the reader spends any more time reading this book), the value proposition of risk management needs to be clearly established.

Perhaps the best way to answer the question "why manage risk?" is to borrow a popular technique used by diet and other self-improvement programs. That simple but effective technique is to paint a clear picture of *the gain of action* along with an equally clear picture of *the pain of inaction*. In the next section, we'll paint the happy picture—the benefits of effective risk management in terms of the expected benefits and gains. In the section thereafter, we'll paint the dire picture of the severe negative consequences—the pain—that may be suffered if effective risk management is not in place.

THE BENEFITS OF RISK MANAGEMENT

Numerous academic papers have established the theoretical basis for managing risk—arguing that it can reduce taxes, reduce transaction costs, and improve investment decisions.[1] However, beyond the theory there are at least four practical reasons why risk management should be of paramount importance to the management of a firm. In this practical context, risk management should be defined more broadly to include internal controls as well as hedging.

Let's now take a look at these four reasons in turn.

Reason #1: Managing Risk Is Management's Job

One notion in modern finance theory is that managing risk, or more specifically hedging, is not necessary because an investor can reduce risk through a

diversified investment portfolio. Regardless of what some theoreticians may argue, you will never in the real world hear a fund manager or individual investor tell a company's management: "Don't worry about managing risk or bankrupting the company—I have a large diversified portfolio."

Managing the risks of a business enterprise is the direct responsibility of its management, not its shareholders. While modern portfolio theory is a major contributor to the theory and practice of finance and risk management today, the argument that the investor can better manage or diversify risks does not ring true in the real world. The average individual investor probably spends more time buying a new car than addressing the risks of his or her investment portfolio. Even the professional fund manager is several degrees away from the insider knowledge required for effective risk management, which includes:

- Historical data on risk/return results, volatilities, and correlations;
- Current risk exposures and concentrations in the business; and
- Future business and investment plans that may alter the firm's risk profile.

Given the complexity of the above information, as well as the lack of full transparency to outsiders, the shareholder cannot be expected to make optimal risk/return decisions. Measuring and managing enterprise-wide risks is a great challenge even for the enterprise's management, who have superior access to information and support from risk management professionals. The most that shareholders can do is to elect an independent and risk-astute board that will represent their interests, and walk away with their investment dollars if they are not happy with management's performance. In the meantime, it remains management's job to ensure that the company achieves its business objectives and is not exposed to excessive risks.

Reason #2: Managing Risk Can Reduce Earnings Volatility

One of the key objectives of risk management is to reduce the sensitivity of a firm's earnings and market value to external variables. For example, the stock prices of companies that are more active in, say, market risk management should exhibit lower sensitivity to market prices. This is borne out by the empirical evidence. For example, in a study[2] published in 1998, Peter Tufano of the Harvard Business School ranked gold producers in terms of the intensity of their hedging activities. The conclusion was that the stock prices of those in the top quartile were about 23 percent less sensitive to gold price changes than those of the bottom quartile. A more recent study conducted in 2007 corroborates Tufano's findings, and further reveals that the gold producers that hedge more tend to have larger asset values:

extensive hedgers, modest hedgers, and non-hedgers have, respectively, average asset values of $1,140 million, $614 million, and $200 million.[3] This demonstrates how gold producers are aware of how the importance of risk management grows in direct proportion to the size of the company.

As such, companies exposed to interest rates, foreign exchange rates, energy prices, and other market variables can better manage earnings volatility through risk management. Managing earnings volatility today is more important than ever given that the stock market severely punishes stocks that fail to meet earnings expectations. At the same time, the Securities Exchange Commission (SEC) and other regulatory bodies are cracking down on earnings management practices that use accounting techniques to smooth out earnings. In this business environment, management must pay more attention to managing the underlying risks of the business.

Reason #3: Managing Risk Can Maximize Shareholder Value

In addition to managing earnings volatility, risk management can help a business enterprise to achieve its business objectives and maximize shareholder value. Companies that undertake a risk-based program for shareholder value management typically identify opportunities for risk management and business optimization that can add 20 to 30 percent or more to shareholder value. Such improvements can be achieved by ensuring that:

- Target investment returns and product pricing are established at levels that reflect the underlying risks;
- Capital is allocated to projects and businesses with the most attractive risk-adjusted returns, and risk transfer strategies are executed to optimize portfolio risk and return;
- The company has the appropriate skills to manage all of its risks in order to protect against large financial losses or damage to its reputation or brand;
- Performance metrics and incentives, at both the individual and business unit levels, are in congruence with the enterprise's business and risk objectives; and
- Key management decisions, such as mergers & acquisitions and business planning, explicitly incorporate the element of risk.

Strategies for achieving these objectives, and case studies of how they work in practice, will be discussed in the main sections of the book.

In a 2009 study,[4] Massimo Mancini of the Kellogg School of Management has supported the notion that active risk management contributes to shareholder value. Using hedging as a proxy to define active risk management,

Mancini studied the fuel hedging practices of airlines: he noted that hedgers were rewarded with 15 to 16 percent more economic value than nonhedgers. Risk management adds value not only to individual companies, but also supports overall economic growth by lowering the cost of capital and reducing the uncertainty of commercial activities.

Reason #4: Risk Management Promotes Job and Financial Security

On an individual level, perhaps the most compelling benefit of risk management is that it promotes job and financial security, especially for senior managers. In the aftermath of the 2008 turmoil in financial markets, a significant number of CEOs, COOs, chief risk officers (CROs), and business group heads of financial institutions lost their jobs because of poor risk management performance. Senior executives in other industries have faced similar fates in the wake of risk management problems. More recently, senior executives involved in corporate frauds and accounting scandals have appeared on national TV being led away in handcuffs and face the potential of severe criminal sentences.

In addition to career risks, senior executives with a significant portion of their wealth tied up in company stocks and options have a direct financial interest in the success and survival of the firm. These incentives, if structured appropriately, work to put the skin in the game for managers, resulting in a strong alignment between management and shareholder interests. Risk management provides managers with a higher degree of job security and protects their financial interests in their firm.

INTEGRATION ADDS VALUE

Risks faced by companies are highly interdependent. Consider these risks in the form of a Venn diagram (Figure 1.3). Next, realize that key interdependencies exist between financial risk and business risk, business risk and operational risk, and operational risk and financial risk. Now further examine the fact that each of these major categories of risk is comprised of more granular risks. For example, financial risk, as demonstrated in Figure 1.3, can be broken down into market risk, credit risk, and liquidity risk. These financial risks in turn have their own interdependencies. Let's examine loan documentation as a practical example of a key interdependency between operational risk and financial risk (i.e., specifically credit risk).

As a business process, the quality of loan documentation is usually considered an operational risk. However, if a specific loan is performing (i.e., the

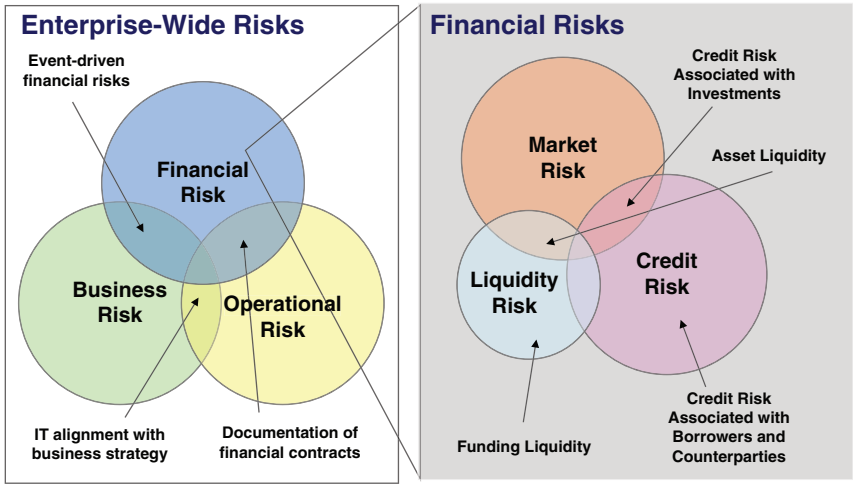


FIGURE 1.3 RISK INTERDEPENDENCIES

borrower is making timely loan payments), the quality of that specific loan document has no real economic impact. On the other hand, if that loan is in default, the quality of the loan documentation can have significant impact on loss severity, with respect to collateral and bankruptcy rights. Interestingly, loss analyses conducted by James Lam & Associates at lending institutions revealed that up to one-third of "credit losses" were associated with operational risks.

With such a complex, interlocking system of company-wide risks, it is obvious that a silo-based risk management strategy is inferior to the integrated framework of ERM. Having separate organizational units or individuals address specific risks requires that these risks be segmented and then isolated in different parts of a company. Because risks are highly interdependent, this distribution cannot be efficient or effective. Targeting individual risks as silos will not account for the interdependencies between them, meaning associated risks may not be captured and the big picture may be completely overlooked. Gaps and redundancies will result in an inefficient system. In addition to the critical issue of interdependences, another key weakness of a silo-based risk management approach is the challenge of aggregating risk exposures across the organization. For example, if business units use different methodologies and systems to track counterparty risk, then it would be difficult to quantify the aggregate exposure for a single counterparty. While the individual exposures at each business unit might be acceptable, the total counterparty exposure for the organization may be too great.

Enterprise risk management (ERM) provides integrated analyses, integrated strategies, and integrated reporting with respect to an organization's key risks, which address their interdependencies and aggregate exposures. In addition, an integrated ERM framework supports the alignment of oversight functions such as risk, audit, and compliance. Such an alignment would rationalize risk assessment, risk mitigation and reporting activities. Moreover, an integrated ERM framework would consider how macroeconomic factors can impact the organization's risk/return profile, such as interest rates, energy prices, economic growth, inflation, and unemployment rate.

More examples that demonstrate how integration adds value can be found in other areas of business management and technology. In business management, I believe that the integration of strategy and risk is the next frontier in ERM. A number of studies—James Lam & Associates (2004), Deloitte Research (2005), and The Corporate Executive Board (2005) have found that strategic risks represented approximately 60 percent of the root causes when publicly traded companies suffered significant market value declines, followed by operational risks (approximately 30 percent) and financial risks (approximately 10 percent). The integration of strategy and risk allows a company's board and management to better understand and challenge the underlying assumptions and risks associated with the business strategy.

In technology, system integration also brings many benefits, since such integration allows for enterprise-level data management, robust business and data analytics, straight-through transaction processing, and more effective reporting and information sharing.

Further examples where integration adds value can also be found outside of business, such as in exercise and martial arts. In fitness programs, cross-training is recognized by fitness experts as having many benefits. By integrating cardio with strength training, flexibility training, and endurance training, athletes can prevent injuries, rehabilitate injuries, enhance strength and power, and improve the functional strength of their bodies.

In the world of mixed martial arts, which has developed in the past 20 years, the integration of various styles has demonstrated that it can add value to centuries old practices and beliefs. Traditionally, it was believed that a silo-based approach to martial arts was superior and that a martial artist should be dedicated to one specific style. Single style martial artists would argue about which style was the most superior. However, the emergence of mixed martial arts has changed that attitude. A mixed martial artist combines karate, kung fu, jujitsu, tae kwon do, wrestling, and multiple other fighting styles, allowing them to adapt to any situation; this gives them a significant advantage when in combat with a fighter trained in a single style.

The key point here is that integration adds value, whether it is in the practice of ERM or many other aspects of business and life.

CAUTIONARY TALES

Ultimately, the arguments above may not sway skeptical managers. Arguments based on the potential gains of improved risk management can be supported by those that point out the potential pain of ineffective risk management. However, these are very often rebutted by the sentiment that "it couldn't happen here" or "if it ain't broke, why fix it?" In these cases, it is worth reminding the skeptics that history has repeatedly demonstrated how bad things can and do happen to good companies.

If anyone ever doubts that risk management is a critical issue for any business enterprise, they should take a hard look at Figure 1.4. The wheel of misfortune illustrates that risk management disasters can come in many different forms, and can strike any company within any industry. Beyond purely financial losses, the mismanagement of risks can result in damage to the reputation of the individual companies, or a setback for the careers of individual executives. The damage can quickly escalate until a previously healthy firm suddenly faces bankruptcy; indeed, the cumulative losses suffered by U.S. thrifts in the mid-1980s bankrupted not just individual companies, but the entire industry.

A close examination of these disasters serves two purposes. First, it underlines the importance of risk management. Second, it offers an insight into the prime tenets of a new, advanced approach to risk management—the approach called enterprise risk management, with which this book is primarily concerned. We'll develop these tenets in the next few chapters.

Let's take a deeper look now, going beyond the immediate headlines to assess the underlying causes and find some more durable truths. An entire book, if not several, could undoubtedly be written about notorious business disasters of the twentieth and twenty-first centuries, but we will review six actual cases here:

1. Bausch & Lomb, a consumer products company;
2. Kidder, Peabody, an investment bank;
3. Metallgesellschaft, an energy company;
4. Morgan Grenfell, an asset management company;
5. Société Générale, a global bank; and
6. MF Global, a commodity trading firm.

The Shortsightedness of Bausch & Lomb

In 1993, the optical manufacturer Bausch & Lomb (B&L) was a world leader in contact lenses and sunglasses. B&L was a company run very much according to the numbers, with failure to reach sales targets regarded as

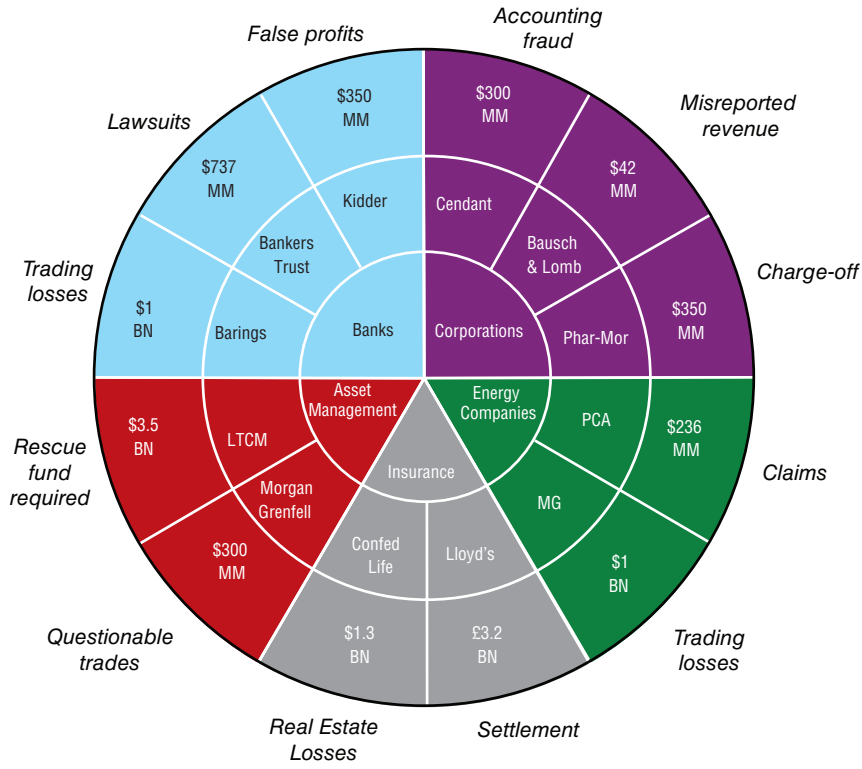


FIGURE 1.4 Wheel of Misfortune

inexcusable. According to the *CPA Journal* (1 September 1998), the company's contact lens division (CLD) had met or exceeded expectations for no less than 48 consecutive months, but in fall 1993 it was becoming apparent that it was not going to make its numbers.

The CLD made back some ground by offering distributors heavily discounted prices and extended payments. This promotion produced sales that surpassed third-quarter forecasts, but had the considerable drawback that the glut of contact lenses now in the market would depress fourth-quarter sales even more than they had been in the third quarter. If the CLD were to meet its fourth-quarter earnings expectations, it would have to resort to still more extreme measures.

It did. The CLD told its distributors that their relationships with B&L would only be maintained if between them they took on its remaining inventory. Most accepted, although this meant accepting ridiculously huge

volumes of product—some ended up with as much as two years' worth of inventory. At the same time, the CLD also fell foul of its retail customers after *Business Week* alleged that it had been selling the same lenses as disposables (priced as low as $7.50) and as traditional lenses (priced at $70). More than 1.5 million buyers of the expensive lenses sued; the claim was ultimately settled in 1996 for a reported $68 million.

The CLD's actions—which, when uncovered, led to an SEC investigation and a $22 million charge against earnings—might have been considered an isolated aberration, had it not been for the fact that another B&L division was also employing dubious practices to shift product at around the same time. The Asian Pacific Division (APD) sold half a million pairs of sunglasses that were shipped to a warehouse in Hong Kong rather than to their putative buyers. This meant that the APD's accounts receivable balance rose rapidly; but rather than raise provisions against bad debts, it conducted exchange transactions so that the customers in question received credits to their accounts and then repurchased the goods.

The APD generated another $20 million of misreported revenue; together, the two rogue divisions led to a $17.6 million overstatement of net income. The company corrected its financial statements in 1996 and paid $42 million to settle a class-action suit brought by shareholders in 1997. The damage was done, however. B&L's share price grew only sluggishly as U.S. equity markets boomed during the 1990s, despite healthy revenues—perhaps the ultimate irony for a company that had valued performance above all else.

The Curtains Close on Kidder, Peabody

At the beginning of 1994, business at General Electric appeared to be going swimmingly. Under the direction of Jack Welch, considered by many to be one of the world's top CEOs, it had reported 51 consecutive quarters of earnings and was widely regarded as one of the few truly successful conglomerates. All that was about to change.

Trouble was brewing at Kidder, Peabody, the investment bank in which GE held an 80 percent stake. Kidder had already caused GE embarrassment in 1987—the year after it was acquired—when it was fined $25.3 million by the SEC for insider trading. This time the problem was much more complex and controversial. Kidder was about to take a $210 million charge after taxes against first quarter earnings for 1994, resulting in a first-quarter loss of $140 million.

Kidder alleged that the loss was due to bogus profits recorded by Joseph Jett, the 36-year-old managing director of the government-trading desk. Jett's basic strategy was to enter into forward contracts that involved the exchange of strips (interest-only government paper) for bonds. His employer

claimed, however, that when the date of the exchange came, Jett would roll the loss-making contracts forward and log fictitious profits (as reported in *The Wall Street Journal*, 18 April 1994).

Jett recorded $350 million in profits in 1993—enough to earn him a $9 million bonus. His $10 million compensation exceeded even that of Jack Welch. But according to Kidder, the profits were phony; Jett had allegedly concealed a $9.5 million loss in 1992, $45 million in 1993, and $29 million in the first few months of 1994. Jett claimed that he was made a scapegoat for Kidder's underperformance.

What really happened may never be known. Although the SEC subsequently found Jett guilty of books and records violations, no criminal charges were ever filed and the National Association of Securities Dealers (NASD) cleared him of fraud. But the aftermath was nonetheless devastating. Jett was only the first to go, followed either through dismissal or resignation by at least five former colleagues including the CEO and the head of brokerage. Kidder itself was sold later that year to a rival brokerage, Paine Webber, for a knockdown price of just $90 million.

Although the Jett affair was more opaque than many later trading fiascoes, many of its root causes—inadequate oversight of traders and understanding of trading strategies—have been repeated. Most notable was Barings, the venerable UK merchant bank which collapsed in 1995 after more than $1 billion of trading losses run up by rogue trader Nick Leeson. Kidder's tale, and the others like it, suggest that companies should not be so dazzled by the golden geese that they stop looking for the rotten eggs.

Meltdown at Metallgesellschaft

One of the most celebrated financial disasters of the 1990s was the massive loss racked up in crude oil trading by Metallgesellschaft Refining and Marketing (MGRM), an American subsidiary of the international trading, engineering, and chemicals conglomerate Metallgesellschaft (MG).

In 1992, MGRM implemented an apparently lucrative marketing strategy. The company agreed to sell specified amounts of petroleum products every month for up to 10 years, at pre-agreed prices above the current market price. The company then used a stack hedging strategy, under which it purchased a succession of short-term energy futures to hedge its long-term commitments. The assumption was that if oil prices dropped, the futures position would lose money, while the fixed-rate position would increase in value. If the oil price rose, on the other hand, the futures gains would offset the losses from the fixed-rate position.

This neat solution turned out to be badly flawed. Under MGRM's strategy, the company would gain over a long period of time if the oil price

dropped, as it sold oil month-by-month at the pre-arranged higher rate. However, it would be exposed to losses made on the energy futures immediately, as margin calls came in. In addition, there was no stable relationship between the long-term forward commitments and the short-term energy futures—another major risk for the company. Thus, when oil prices actually dropped, the company faced a cash flow crisis and ultimately a funding crisis that reached all the way back to the parent company. In December 1993, MG was forced to bail out MGRM and cash in its positions at a loss totaling more than $1 billion.

Academics have been arguing about whether MG did the right thing ever since. Theoreticians such as the Nobel prize-winning economist Merton Miller and his colleague Christopher Culp maintain that had MG been able to persevere, in the long term it would have made a profit, recouping the losses on the futures through profits on the sale of petroleum. Others have pointed out that this is irrelevant, given that the company could not have done so in practice, while some have cast doubt on the size of the potential long-term gains. An auditors' report, commissioned by MG shareholders, maintains that 59 million barrels' worth of the long-term contracts had a negative value of about $12 million, so the value of these contracts could never have offset the losses, even in the long term.

The MG episode illustrates a concept that can be referred to as *funding risk*—the risk that positions may be profitable in the long run, but bankrupt a company in the short run. This is a risk that arises if negative cash flows are mismatched with positive cash flows, with the emphasis jointly placed on *cash* and *flows*. It is not enough just to think about how *much* money a strategy will bring in; risk managers must also think about *when* that money will come in.

Morgan Grenfell's Asset Mismanagement

Morgan Grenfell Asset Management (MGAM) was doing well in 1994. Pension assets managed by the company's Investment Services division had grown from $7.6 billion to $10 billion during 1994. The firm was fast developing a reputation for being knowledgeable and effective.

In 1995, however, one of its employees embarked on a course of action that would culminate in a media spectacle big enough to overshadow those successes. Sometime during that year, fund manager Peter Young began making covert purchases of large quantities of stock in companies that could charitably be described as little known. What Young saw in these companies was known only to himself; some of them were very unlikely to have been endorsed by MGAM's investment guidelines.

One example was Solv-Ex, a company described by *Barron's* as having "a rather checkered past and nothing more tangible than ambitious

plans for exploiting Canada's Athabasca tar sands for oil and minerals" (4 November 1996). Young bought $30 million of stock in this gem—not at a discount, as might be expected for an extremely risky bulk purchase, but at a $2-a-share premium.

Young also managed to circumvent a Securities and Investment Board regulation forbidding a fund from owning more than 10 percent of any company. He did this by establishing a system of companies, apparently through a Swiss law firm. These companies were paired, so that each owned some 90 to 95 percent of its partner company, while Young purchased the other 5 to 10 percent for the funds under his control.

In September 1996, the London regulators began investigating the valuation of assets in MGAM's three largest European funds. Trading on the funds shut down for three days and resumed only after Deutsche Bank, the parent company, replaced the questionable assets in the fund with $300 million in cash. Nonetheless, about 30 percent of investors left the funds within the next few weeks, taking $400 million with them.

The turmoil in the wake of this scandal was enormous. MGAM had to compensate more than 80,000 investors and was fined by the City of London regulators. Establishing the value of the compensation required two teams, each with 100 members, from two major accounting firms. Questions about how Young had been allowed to get away with his eccentric trading for so long—especially given reports that he had been cautioned about breaching investment guidelines months before the suspension—continued to haunt MGAM.

Young, meanwhile, briefly returned to the limelight a few months later, when he made his first court appearance wearing a dress and full make-up. Whatever the motivation behind this switch in gender polarity, it served as a suitably surreal coda to an affair that had been as perplexing as it had been expensive.

Société Générale Blindsided

The financial world was shaken to its core in early 2008 when Société Générale, then counted amongst the most esteemed financial institutions in the world, announced that a single trader, Jérôme Kerviel, had caused the bank a net loss of 4.9 billion euros. The bank's top officers were left reeling, caught completely by surprise—how could they have been blindsided by such blatant and flagrant violations of company policy?

In the immediate aftermath of the incident, many critics pointed the finger at Kerviel, hurling accusations of personal greed and ambition—he was labeled a rogue trader and blamed entirely for the fiasco. However, when police raided Kerviel's home, they found none of the evidence that would condemn

him as an unstable individual with uncontrollable, reckless urges—his apartment was simple, with no luxurious extravagances, and he did not even own a car. As James B. Stewart writes in *The New Yorker,* "how could one person have amassed an exposure, as Kerviel had, of fifty billion euros without his superiors at the bank knowing?"[5] He goes on to note that Kerviel quickly gained the sympathy of the public, with 50 percent of respondents in a *Le Figaro* poll blaming Société Générale itself for what happened.

As the months rolled by and investigators painstakingly unraveled the mystery around the relationship between the trader and the bank, it became evident that this was more complex than a simple case of rogue trading—and the story that the bank's top level executives had no idea what was going on became less and less credible. For example, internal and external audits of the bank uncovered the fact that around 74 alerts about Kerviel's unusual trading activities slipped under the radar of the bank's risk systems. There is now also substantial evidence that highlights the ineffective supervision of Kerviel's direct superiors, who rarely checked on the transactions of individual traders.

It is also important to consider the highly complex nature of the derivatives that Kerviel was trading in—due to their, as implied by the nomenclature, derived value, derivatives can fall and rise significantly in value in response to comparatively smaller changes in the market. Since there is an unavoidable element of unpredictability to markets, a trader can find himself abruptly deserted by his golden touch when the markets shift unfavorably.

Kerviel discovered that he could avoid this by performing intra-day trades, which would not show up on the bank's daily records—he could offset any losses with false trades to cover his own tracks. He was encouraged by his initial successes, and was even praised by his superiors for a job well done—Kerviel says that while his superiors reprimanded him for his trading activities, he did not take it seriously, because he was not punished. Eventually, his supervisors appeared to grant him free rein, exempting his computer from the company's system of alerts.

This demonstrates that while it is evident there was some form of ERM in place at Société Générale, top executives did not implement it in the face of such potentially high profits—greed overpowered caution. Kerviel believed his superiors approved of his strong performance, regardless of the methods he used, which seems a reasonable statement, considering he was given a bonus of three hundred thousand euros in 2007 for his trading performance. Kerviel was aware that his illicit trading was constantly setting off the bank's internal trading risk management system—information that was most definitely accessible to his superiors—but since no one actually brought it up with him, he did not stop.

However, as the number of false trades built up, the bank could no longer turn a blind eye to Kerviel's actions—correspondence with Deutsche Bank, one of the firms that Kerviel had forged trades with, revealed that it had no knowledge of Kerviel's contracts. Kerviel's house of cards came tumbling down in a matter of days, when further investigation of his hidden trades yielded losses of around fifty billion euros that more than cancelled his previous stellar gains.

In the end, Société Générale decided to liquidate Kerviel's trades instead of hoping for a miracle in the markets that would turn the tides in their favor, which likely swelled the already enormous amount of loss; the bank also had to borrow heavily from Morgan Stanley and J.P. Morgan to avoid bankruptcy. All Société Générale trading was temporarily halted, which resulted in a four percent drop in share prices, while Kerviel was taken to court and immediately sent to jail.

In a nutshell, as Kerviel's psychologist succinctly summarizes, "the combination of the financial and personal success derived from his hidden trading, plus the lax supervision by his superiors . . . had a strong effect in the reinforcement" of Kerviel's trading practices.[6] Kerviel says that he was not, by any means, the only Société Générale trader who performed illicit trades for the sake of higher profit margins, which speaks to the extent to which profit was emphasized over risk management within Société Générale.

As such, it seems that it was not the case that Société Générale did not have established risk management procedures—it was simply that its employees chose not to follow them for the sake of higher profits, which speaks to the importance of fully implementing ERM. While Jérôme Kerviel certainly made rash decisions, he was ultimately just one weak link in an entire chain that was faulty and vulnerable to breakage.

MF Global Goes Under

Following a series of illegal transactions that moved customer funds for corporate purpose, MF Global filed for what would become "the eight-largest bankruptcy in U.S. history" on October 31, 2011.[7]

Jon Corzine, CEO of MF Global, put the company under suspicion when he vehemently voted against a Commodities Futures Trading Commission proposal that would enforce greater control on how companies like MF Global could invest clients' money. Corzine's aversion to risk management during his reign at MF Global is a continuation of his reputation for making big market bets at Goldman Sachs, where he previously served as the head of its fixed-income division.

Further investigation revealed that MF Global had deliberately tried to cover up its enormous debt risks by tapering short-term borrowing "at the

ends of its fiscal quarters" so that it was much lower than the "average and peak levels for the full quarters" by a full 16 to 24 percent.[8]

MF Global defended itself vigorously in this regard, insisting that this pattern occurred organically, as a result of natural market conditions and client activities. Of course, as Charles Mulford, a professor at the Georgia Institute of Technology, wryly puts it, "I'm left to wonder why client needs are always reduced at the end of the quarter."[9]

In financial lingo, this is called *window dressing*. Window dressing is not illegal, and by no means was MF Global the only financial institution that practiced this. However, Corzine's usage of clients' money to make up for the bank's crippled financial assets in the wake of the European debt crisis *was* in direct violation of the law. Under Corzine's guidance, MF Global invested 6.3 billion on European debt. This amounted to more than 500 percent of its tangible common equity. Inevitably, when the European economies collapsed, MF Global found itself sinking. In terms of risk management, it seems unbelievable that such a concentrated risk position was allowed to take place—evidence of the weaknesses of a top-down hierarchy system.

In a desperate last-ditch attempt to save the ship, MF Global's top executives decided to use their clients' money to pay off short-term debts. For example, on October 28, 2011, Edith O'Brien, former assistant treasurer at MF Global, was ordered to transfer $175 million from clients' accounts to pay off an overdraft at J.P. Morgan Chase.

Corzine tried to calm the markets: mere days before MF Global filed for bankruptcy, he told investors that "the firm was taking steps to reduce its market exposure," while in reality, the company only continued to take on more risk as it shifted more assets around to try and save itself.[10] When it failed to do so, it had to throw the towel in. Unlike Goldman Sachs, MF Global was *not* too big to fail, and so it was left to drown.

Bausch & Lomb, Kidder Peabody, Metallgesellschaft, MGAM, Société Générale, and MF Global: six very different companies. But it should already be apparent that there are common themes that can be drawn from these and other headline-grabbing incidents. We'll explore these in the next chapter.

CHAPTER 2

Lessons Learned

A Chinese philosopher once said that a smart man learns from his own mistakes and a wise man from the mistakes of others, but a fool never learns. Most of us would rather be smart and wise than foolish. In order to avoid taking the fool's path to potential disaster, it is important for companies to develop organizational processes that allow them to learn from their mistakes. Ideally, the same processes would also allow them to learn from the mistakes and the best practices of other companies.

There is no shortage of learning opportunities. It seems as if a major business disaster happens every few months, reminding us of the dangers faced by all enterprises. Organizations fortunate enough to avoid a major crisis often experience lesser problems or near misses which highlight underlying exposures to risk.

Left unchecked, these exposures could lead to a major loss or incident in the future. If these disasters are to be averted, an organization must be open to the discussion of past mistakes, and must be able to learn from them. Moreover, the same process should promote organizational learning about the costly mistakes made by other companies as well as about the application of industry best practices.

When I started Fidelity Investments' enterprise risk management program in 1995, the concepts of lessons learned and best practices were central to initiatives to raise risk awareness. In the early stages of the program, my team (Global Risk Management) organized regular meetings of the company's top 200 executives, including corporate managers, business unit heads, and senior financial and risk management professionals. High on the agenda at these meetings was a discussion of the lessons learned from major disasters in the financial services industry, such as the troubles of Barings Bank and Kidder, Peabody. In each of these case studies, participants examined the sequences of events, the root causes of the problem, and the financial and business impact that they went on to have. The focus of any such case analysis, however, was on how Fidelity Investments could avoid

similar problems. These meetings were invaluable in building and maintaining awareness regarding risk management among the senior executives.

Another learning initiative for us was a series of visits to about a dozen financial institutions as part of an exercise in best-practice benchmarking. This initiative included visits to Brown Brothers, Chase, GE Capital, State Street Bank, and others. As a result of these visits, more than 100 best-practice applications were documented in a database that was part of the educational section of an Intranet-based Global Risk management information system (MIS). This database allowed all Fidelity Investments' risk management professionals to benefit from the insights gained from these best-practice visits, while the Intranet gave the user the capability to search for and identify best practices by risk, company, or application.

One of the most striking insights gained from these visits was the high value that other companies placed on their learning processes for risk management. For example, State Street Bank had a six-week launch program for new associates that trained them in business and risk management processes, while Brown Brothers had an errors and omissions program that educated employees about where problems usually occurred in their operations and how they could be avoided. Several of the companies we visited implemented systematic learning processes that reviewed important incidents, losses above a certain threshold, and other issues such as risk policy violations.

Following these visits, Fidelity Investments launched a number of initiatives at both the corporate and business unit levels. These initiatives included a risk college, loss and incident review processes and follow-up best practice visits with our business partners and institutional clients. We also conducted an internal consulting project for a business unit. That business unit experienced an 85 percent reduction in annual losses after the introduction of a risk event log. Any loss above a certain threshold was recorded in this log and subsequently reviewed by the risk management committee—chaired by the business unit president—to ascertain the root cause of the problem and develop prevention procedures.

My experiences at Fidelity—and elsewhere—suggest that lessons learned from mistakes and from the best practices of other companies can be a valuable supplement to those learned from the examination of a company's own operations. While a certain number of minor losses should be expected as a matter of routine in any business, management should nonetheless view every *significant* loss or incident as a learning opportunity. Without a systematic process for capturing and learning from such incidents and losses, a company is more likely to repeat old mistakes that could potentially develop into a real crisis.

The six cases described in the last chapter represent only a very small sample of the risk management failures that have hit the headlines in recent

years, or of the range of risk management problems that can cause financial losses. Collectively, these and other cases should serve as a loud wake-up call: improper risk management and control can have dangerous consequences. Lapses in risk management have resulted in significant losses for companies in different industries and countries around the world. A number of those companies—some once considered pillars of their industries—no longer exist because they couldn't survive the financial and reputational losses they suffered.

The circumstances surrounding each story are unique, with the culprit(s) ranging from a single rogue trader involved in unauthorized trading to groups of individuals involved in unsound business practices that were at one time accepted (or even encouraged) by management. Some events occurred over days or months, while others took more than a decade to unfold, or even longer. Despite the many differences, there are some common themes. We can distill these into seven "key lessons":

1. Know your business;
2. Establish checks and balances;
3. Set limits and boundaries;
4. Keep your eye on the cash;
5. Use the right yardstick;
6. Pay for the performance that you want; and
7. Balance the yin and the yang.

We'll look at these in more detail in the section below.

LESSON #1: KNOW YOUR BUSINESS

Perhaps the most important lesson one can learn is that managers are obligated to know the business. This responsibility should be shared by everyone involved in the business, ranging from the board of directors to front-line supervisors and employees, and is an integral component of risk management. In credit risk management, for example, know the customer is widely accepted as a tenet of a sound credit program, and has been adopted as a requirement by several regulatory agencies.

While it is critical for managers with responsibility for oversight and approval to know their businesses, it is also important for *all* employees to understand how their individual accountabilities could affect the risks of the organization, and how their functions and responsibilities relate to others within the company. Business managers should be knowledgeable about all aspects of the business, including high-level business and operational

processes, key drivers of revenue and cost, and the major risks and key exposures involved (i.e., know the risks).

Failure to know the business was a contributing factor in both the Kidder, Peabody and Metallgesellschaft fiascoes. In a report of an internal investigation that he led in 1994, the former SEC enforcement chief Gary Lynch noted that Jett's supervisors "never understood [his] daily trading activity or the source of his apparent profitability," while GE's auditors ". . . really didn't understand much about government [debt] trading." Overall, the Lynch Report was highly critical of management's failure to supervise, understand, and monitor the activities on the trading desk.

In Metallgesellschaft's case, had senior management better understood the cash flow implications of its New York arm's activities, the company might never have embarked upon its disastrous hedging strategy—or at least, might have unwound it in a more orderly fashion, and thus avoided the resulting liquidity squeeze and hedging loss. It appears that Metallgesellschaft, more than most, fell victim to an inappropriate, rather than intrinsically flawed, strategy.

LESSON #2: ESTABLISH CHECKS AND BALANCES

A prerequisite of effective risk management is that there should be a system of checks and balances to prevent any given individual or group of individuals from gaining excessive power to take risks on behalf of an organization.

This can be thought of as the application of portfolio diversification to the management of people and processes, rather than assets and liabilities. It is not desirable, from a risk management perspective, to have a concentration of market risk exposure in a specific segment (emerging markets, say) or a concentration of credit risk exposure in an individual counterparty. Likewise, it is not desirable to allow an individual or group of individuals to amass a concentration of the power or authority to commit the company's capital to a specific risk-taking activity. This might range from an individual trader with the power to make enormously leveraged bets on market prices to an executive whose orders go unquestioned by other managers or non-executive directors.

Re-engineering efforts pose a potential problem in this respect. Checks and balances are often, by definition, redundant processes, and so may be re-engineered out of a key operation or process altogether. It is important to realize that a system of checks and balances, along with the segregation of key duties, is not only a safeguard against errors made by people, processes, and/or systems, it is also fundamental to sound business management. Real life examples include appointing an independent board of directors, creating

effective risk and audit committees, or even something as simple as having someone proofread an important document.

The collapse of Barings Bank is perhaps the best-known example of this principle. Both the trading and the accounting functions at Barings' Singapore branch reported to rogue trader Nick Leeson, enabling him to conceal mounting losses for over a year. The scandal that erupted when Barings ultimately collapsed under the weight of Leeson's billion-dollar losses led banking regulators and industry groups around the world to establish segregation of duties and independent risk management as core principles in risk management. In response, companies established risk management and back-office operations that were independent of the profit centers.

The case of Morgan Grenfell Asset Management also illustrates the need for effective checks and balances. Both Young's immediate boss and the company's compliance department were supposed to sign off on each of Young's purchases of unlisted shares, so they should have known exactly what was happening. However, it was not until Young's holdings of unlisted shares hit more than three times the legal limit that his boss first told him to reduce them.

LESSON #3: SET LIMITS AND BOUNDARIES

Just as business strategies and product plans tell a business where to go, risk limits and boundaries tell a business when to stop.

It is widely accepted that risk limits are an integral part of a sound risk management program. For market risk, these risk limits may include trading limits, product limits, duration and other limits on a position's sensitivity to movements in market prices or rates (e.g., delta, gamma, vega, theta, also known as the Greeks of option pricing), value-at-risk limits, and stop-loss limits. For credit risk, they may include mark-to-market and risk-adjusted limits by counterparty, risk grade, industry, and country. For operational risks, the risk limits may include minimum quality standards (or conversely, maximum error rates) by operation, system, or process. They may also include firm deadlines to resolve outstanding audit items.

In addition to limits on financial and operational risks, boundaries should be established to control business risks, which include standards for sales practices and product disclosures. Boundaries should also be established to control organizational risks, such as the company's hiring policies *vis-a-vis* background checks on prospective employees, or its termination policies if an employee violates company policy. As part of a board-approved ERM policy, companies should establish a "statement of risk appetite" that provides explicit risk limits and tolerance levels of critical risks. Without

clear limits and tolerances, the management of a fast-growing company is in the position of the driver of a racing car with no brakes.

In the Metallgesellschaft case, the company's failure to set appropriate limits on hedging activities compounded the problem. Forward and futures positions continued to grow larger even as oil prices fell: by the time the petroleum positions were liquidated, they were estimated to be worth 85 days of Kuwait's entire output. In the MGAM case, the damage would likely have been contained if Young had been censured and his dealings investigated as soon as unlisted shares passed the legal limit.

LESSON #4: KEEP YOUR EYE ON THE CASH

Willy Sutton, the infamous bank robber, was once asked why he robbed banks. He replied: "Because that's where the cash is." This simple answer contains an important lesson for all financial institutions, as well as for the finance/treasury operations of any corporation. Crime—whether fraud, embezzlement, or straightforward theft—follows cash. And more innocent trading and operational errors are most immediately painful when they affect cash.

It's therefore important to make sure that there are appropriate safeguards for managing cash positions and cash flows. These include basic controls, such as authorized signatures to initiate, approve, and make cash transfers. They also include the development of internal processes to measure, monitor, reconcile, and document cash transactions and positions. Actual cash flows and positions can also provide management with valuable reasonableness checks against the company's trading systems and profitability models.

New and emerging technologies such as e-commerce, electronic banking, and smart cards will provide financial institutions with new challenges in this important area. Inadequate cash management and accounting systems represent opportunities for potential fraud to go undetected, as well as blind spots for trading and operational errors. In the Kidder case, Jett's trading operations recorded $350 million of profits on paper, but no one reconciled Kidder's cash positions with the reported profits over the course of three years. As Gary Lynch said in a *60 Minutes* interview: "They were always unrealized profits." In the case of Enron, the company reported $3.3 billion in net income over the five years ending 2000. Over the same period, James Lam & Associates found that Enron reported only $114 million of total cash generated—a mere 3 percent of reported income. A long time delay between reported earnings and actual cash flows should be a warning indicator for any company. To quote one analyst: "Cash is king. Accounting is opinion." The lesson here is to focus on the cash.

LESSON #5: USE THE RIGHT YARDSTICK

The measures of success used (or not used) by a company to track individual and group performance are collectively a key driver of behavior, and by extension, of risk. Most companies establish performance goals in terms of sales, revenue and profitability. Some have adopted the balanced scorecard approach, and augment their financial measures with performance measures pertaining to quality, customer satisfaction, and internal processes. If management is to gain a proper risk/return perspective, it is important that risk measures (similar to those alluded to in Lesson 3) are incorporated in the processes that generate management reports and measure performance. An integrated set of risk measures should provide management with timely information on all types of risks faced by the company, including actual (*ex-post*) and early warning (*ex-ante*) risk indicators.

Use of an inappropriate yardstick was clearly one of the factors leading to Bausch & Lomb's troubles. The focus on sales and earnings targets, plus an extremely demanding atmosphere, resulted in behavior that had adverse consequences on a variety of levels, from customer dissatisfaction to stock price. The disasters that befell the company were caused, at root, by an unyielding desire to succeed. Had the company not placed such heavy emphasis on growth at all costs—or, to put it differently, on return regardless of risk—things would likely have turned out differently.

Other companies regularly set aggressive earnings growth targets in the range of 15 to 20 percent per year. These companies should ask themselves: are these targets realistic when the general economy is growing at 3 to 4 percent? What kind of pressures do these targets put on the business units? How will people behave if aggressive sales and earnings goals are not balanced with the appropriate controls and measures for risk? As has been said, the road to hell is paved with good intentions.

LESSON #6: PAY FOR THE PERFORMANCE YOU WANT

The other dimension of performance measurement is the issue of compensation and incentives. Organizations need to take a close and careful look at how compensation and incentives are designed and implemented, and whether or not they reinforce desired behavior and performance. The combination of performance measurement and incentive compensation is probably one of the most powerful drivers of human behavior and organizational change. This can either work in favor of the company's risk management objectives—or against them.

For example, the performance of managers and employees might be measured by, and rewarded for, sales- or revenue-based results alone, with

no consideration given to risk exposures or losses. In that case, it should be expected that the company would be exposed to increasingly higher levels of potential risk that may ultimately become inconsistent with its risk appetite and capitalization. Management should therefore pay careful attention to the signals that performance measurement and incentive compensation systems send out, to ensure that they are consistent with the company's business and risk management objectives.

As one of my professors at UCLA once said: "If you go into a company and see smart people doing stupid things, nine times out of 10 they are being paid to do so." Improper incentive structure is a root cause of recent problems associated with the lack of independence in equity research (e.g., analysts recommending the stocks of investment banking clients while privately trashing the same stocks). In the Kidder case, did it make sense that in 1993 Jett earned a bonus of $9 million and his boss, Ed Cerrullo, earned $20 million—more than Jack Welch, the parent company's well-regarded chairman and CEO?

LESSON #7: BALANCE THE YIN AND THE YANG

Much of the focus of risk management has to date been on building infrastructure: independent risk functions and oversight committees; risk assessments and audits; risk management policies and procedures; systems and models; measures and reports; and risk limits and exception processes. All of this makes up what might be called the hard side (the yang) of risk management.

However, it is equally (if not more) important that companies should focus on the soft side (the yin) of risk management. Soft initiatives might include:

- Setting the tone from the top and building awareness through demonstration of senior management's commitment;
- Establishing the principles that will guide the company's risk culture and values;
- Facilitating open communication for discussing risk issues, escalating exposures, and sharing lessons learned and best practices;
- Addressing change management, including training and development programs; and
- Reinforcing desired behavior and results through performance measurement and incentives.

While the hard side focuses on processes, systems, and reporting, the soft side focuses on the people, skills, culture, values, and incentives. In many

respects, the components of the soft side are the key *drivers* of risk-taking activities while the components of the hard side are *enablers*, which support risk management activities. As discussed in Chapter 1, there can be no reward without risk; but risk should not be taken recklessly or randomly. That means that both the soft and hard sides—the yin and the yang—of risk management are necessary; managers should therefore take a balanced approach to managing risk at their companies.

As was suggested at the beginning of this chapter, learning is a critical part of any successful enterprise risk management program. An organization open to learning is less likely to repeat past mistakes, and more likely to benefit from new developments and innovations in the field of risk management. That is, to be smart and wise, and not to make a fool of oneself.

CHAPTER 3

Concepts and Processes

In this chapter we will examine the key concepts and processes that underpin risk management. We begin by reviewing the major categories of risk faced by most organizations. Next we will discuss the key concepts that should be considered in the assessment and quantification of any risk. Based on these concepts we will review the processes for promoting risk awareness, measuring risk, and controlling risk. We will conclude this chapter with what I consider to be one of the most important ideas in this book, and that is: every risk can be thought of as a bell curve!

Risks come in all shapes and sizes; risk professionals generally recognize seven major types:

1. ***Strategic risk*** is the risk that corporate and business strategies (e.g., mergers and acquisitions [M&A]), growth strategies, product innovations) are flawed or ineffectively executed;
2. ***Business risk*** is the risk that annual financial and operating results may not meet management and stakeholder expectations;
3. ***Market risk*** is the risk that prices and rates will move in a way that has negative consequences for a company;
4. ***Credit risk*** is the risk that a customer, counterparty, or supplier will fail to meet its obligations;
5. ***Liquidity risk*** is the risk that a company cannot raise cash to meet its requirements in a timely and cost-effective manner;
6. ***Operational risk*** is the risk that people, processes, or systems will fail, or that an external event (e.g., earthquake, fire) will negatively impact the company; and
7. ***Compliance risk*** is the risk that the company may violate laws and regulations.

Other types of risk have also been suggested. For example reputational risk is the risk that a company's brand and reputation may be negatively impacted. However, others argue that reputational risk is a second-order risk and is the consequence of other primary risk factors.

Each of these broad risk types encompasses a host of individual risks. Credit risk, for example, includes everything from a borrower default to a supplier missing deadlines because of financial problems. In risk identification and assessment, it is important to consider the root cause. For example, as mentioned above a supplier may not perform due to its own financial issues (credit risk) or due to technology and process issues (operational risk). Although there are commonalities and interdependencies between all categories of risks, each ultimately requires specialized attention.

How can a manager with responsibility for enterprise-wide risk hope to stay on top of all these various risks? It is impractical to simply hire an expert for every risk—since risk is a part of every business decision, this approach would require a risk manager for every business manager.

A more practical solution is to make risk a part of every employee's thinking and job responsibility. This has two advantages: first, no one is better placed to understand the risks of an activity better than those who specialize in that area; second, this approach means that risk is managed throughout the company.

However, this requires a substantial effort in training and education. Many staff, whether junior or senior, will not be familiar with risk management and particularly not with quantitative forms of risk analysis. Although these quantitative analyses are often very important, they are not practical for every type of risk and fall under the responsibility of the corporate risk management function.

General employees therefore need to be taught to recognize and assess risks in ways that are relatively easy to understand. Fortunately, there are a number of key *risk concepts* that will apply to the risks of any kind of business and must be addressed by any effective risk management program.

RISK CONCEPTS

Not all of the risk concepts described in this section can be readily (or meaningfully) quantified, particularly if operational risks are involved. As we'll see, however, they are nonetheless important for understanding the nature of risk in any organization and should form the basis of the questions that a risk manager asks when assessing risk. Let's consider them in turn.

Exposure

What do I stand to lose? Generally speaking, the exposure is the maximum amount of damage that will be suffered if some event occurs. All other things

being equal, the risk associated with that event will increase as the exposure increases. For example, a lender is exposed to the risk that a borrower will default. The more it lends to that borrower, the more exposed it is and the riskier its position is with respect to that borrower. Exposure measurement is a hard science for some kinds of exposures—typically those which result in direct financial loss such as credit and market risk—but may be much more qualitative for others, such as operational and compliance risk.

Volatility

How uncertain is the future? Volatility, loosely meaning the variability of potential outcomes, is a good proxy for risk in many applications. This is particularly true for those that are predominantly dependent on market factors such as options pricing. In other applications, it is an important driver of the overall risk in terms of potential loss.

Generally, the greater the volatility, the higher the risk. For example, the number of loans that turn bad is proportionately higher, on average, in the credit card business than in commercial real estate. Nonetheless, it is real estate lending that is widely considered to be riskier, because the loss rate is much more volatile. Companies can be much more certain about potential losses in the credit card business—and prepare for them better—than they can in the commercial real estate business.

Like exposure, volatility has a specific, quantifiable meaning in some areas of risk. In market risk, for example, it is synonymous with the standard deviation of returns and can be estimated in a number of ways. The general concept of uncertain outcomes, is, however, useful in considering other types of risk, too: a spike in energy prices might increase a company's input prices, for example, or an increase in the turnover rate of computer programmers might negatively affect a company's technology initiatives.

Probability

How likely is it that some risky event will actually occur? The more likely the event is to occur—in other words, the higher the probability—the greater the risk. Certain events, such as interest rate movements or credit card defaults, are so likely that they need to be planned for as a matter of course and mitigation strategies should be an integral part of the business' regular operations. Others, such as a fire at a computer center, are highly improbable, but can have a devastating impact. A fitting preparation for these is the development of back-up facilities and contingency plans that will likely be used infrequently, if ever, but must work effectively if they are.

Severity

How bad might it get? Whereas exposure is typically defined in terms of the worst that could *possibly* happen, severity is the amount of damage that is actually *likely* to be suffered. The greater the severity, the higher the risk. Severity is the partner to probability: if we know how likely an event is to happen, and how much we are likely to suffer as a consequence, we have a pretty good idea of the risk we are running.

Severity will often be a function of other risk factors, such as volatility. For example, consider a $100 equity position. The exposure is $100, since the stock price could theoretically drop all the way to zero and all the money tied up in the stock could be lost. In reality, however, it is not likely to fall that far, so the severity is less than $100. The more volatile the stock, the more likely it is to fall a long way. The severity associated with this position is therefore greater, and the position more risky.

As with our other risk factors, this way of thinking can also be applied to risks that are less easy to quantify. Consider, for example, the succession process after a key employee leaves or retires. Given that a change in management must occur at some point in time, and that the succession of new management will generally have a significant and potentially disruptive impact on the organization, it is alarming that companies don't plan more carefully for this risk.

Time Horizon

How long will I be exposed to the risk? The longer the duration of an exposure, the higher the risk is. For example, extending a 10-year loan to the same borrower has a much greater probability of default than a one-year loan. The time horizon can also be thought of as a measure of how long it takes (or, equivalently, how difficult it is) to reverse the effects of a decision or event.

The key issue for financial risk exposures is the liquidity of the positions affected by the decision or event. Positions in highly liquid instruments such as U.S. Treasury bonds can usually be reduced or eliminated in a short period of time, while positions in lightly traded securities or commodities such as unlisted equity, structured derivatives, or real estate take much longer to sell off. For operational risk exposures, the time horizon can be thought of as the time required for the company to *recover* from an event. A fire that burns a computer center to the ground will leave a company exposed during the time before back-up facilities come online—a much greater risk if such back-up procedures are not well established and tested.

Companies usually have little control over the level of market liquidity, or over many of the events that lead to operational risks. However, they do have some control over their effects. Problems arise when companies do not recognize that a risk event has occurred, are not aware of the time horizon associated with that risk, and/or have not developed an exit strategy.

Correlation

How are the risks in my business related to each other? If two risks behave similarly—they increase for the same reasons, for example, and/or by the same amount—they are considered highly correlated. The greater the correlation, the higher the risk. Correlation is a key concept in risk diversification. Highly correlated risk exposures, such as loans to the same industry, investments in the same asset class, or operations within the same building, increase the level of risk concentrations within a business. Thus, the degree of risk diversification in a business is inversely related to the level of correlations within that business. With financial risks, diversification can be achieved through risk limits and portfolio allocation targets, both of which are designed to reduce risk concentrations. With operational risk, diversification can be achieved through separation of operational units and/or redundant systems. A word of caution: seasoned risk professionals recognize that price corrections approach one during times of crisis. For example, during the 2008 financial crisis, all global asset prices (e.g., real estate, equities, bonds, and commodities) fell in concert, with the exception of U.S. Treasuries. As such, companies should stress-test their correlation assumptions because diversification benefits may not be there when they are needed the most.

Capital

How much capital should I set aside to cover unexpected losses? Companies hold capital for two primary reasons. The first is to meet cash requirements, such as the costs of investments and expenses. The second is to cover unexpected losses arising from risk exposures. The level of capital that management wants to set aside for these two purposes is often called *economic capital*.

The overall level of economic capital required by a company will depend on the credit rating that it wants. The more creditworthy the company wants to be, the more capital it will have to hold against a given level of risk. This is fairly intuitive: a credit rating (or the concept of creditworthiness generally) is an estimate of how likely a company is to fail. Clearly,

it is less likely to fail if it has more capital to absorb any unexpected loss. So, a company that wants a triple-A credit rating will have to hold far more capital against a certain set of risks than another company that has the same risks but is satisfied with a sub-investment-grade rating, such as double-B.

The concept of economic capital also applies to the individual business units *within* a company. Those business units which run greater risks (and therefore stand more chance of losing money) will have to be allocated more economic capital if they are to comply with the firm's overall target creditworthiness. The allocation of economic capital to business units has two important business benefits.

First, it links risk and return explicitly. Higher allocations of economic capital require business units that take more risks to compensate by generating greater profits. Second, economic capital allows the profitability of all business units to be compared on a consistent risk-adjusted basis. As a result, business activities that contribute to, or detract from, shareholder value can be identified easily, so management has a powerful and objective tool to allocate economic capital to its most efficient users. In effect, this creates an *internal capital market* where good businesses will grow and bad businesses will die.

RISK PROCESSES

An appreciation of the risk concepts described previously is fundamental in understanding the nature of risk. This understanding in turn supports the first step in any risk management process: promote risk awareness. The second step is to measure risk; the third is to control it. For all the quantitative sophistication that can be thrown at it, risk management is still ultimately carried out by people, and the three parts of a corporate risk management process can usefully be illustrated in terms of the ways that people manage risks in their everyday lives.

First, risk awareness. Most people think (at least a little!) about what they are currently doing and what they plan to do next; accidents happen when they misjudge an unfamiliar situation or fail to pay sufficient attention to a seemingly familiar one. People break legs when they first go skiing and cut their fingers when they drift off while chopping vegetables.

Companies obviously don't think in this way, but they do need to use the collective intelligence of their management and staff to think through the risks consequent upon the company's current and proposed activities. Promoting risk awareness should be the starting point for any

risk management process. Half the battle is already won if people can be successfully encouraged to consider the risks involved in their activities, and to understand their roles and responsibilities in managing them. Mistakes can then be avoided or quickly corrected.

Awareness alone is not enough, however. It is one thing to know that a potential risk exists; it is another to know when it becomes a real threat and how serious it is. A person might see a distant threat (a car bearing down from a distance), or feel an immediate one (a tack in the foot). The scale and speed of the reaction will differ.

Similarly, a company must be able to recognize changes in its operating environment that signal potential risks and must also notice when a part of the company is unexpectedly afflicted by some event. That means effective transmission of information into and through the company, which in turn implies the need for efficient communications technology and clear, consistent reporting of risks (i.e., risk measurement).

Having identified and quantified the risk, a person must decide if anything should be done about it (i.e., risk control). A person might control his risks in a number of different ways. He might feel that a given risk is minor (the chance of being hit by a meteorite, for example) and continue about business as usual. He might simply limit potential risk—perhaps by capping the amount he is willing to bet on a spin of the roulette wheel. Alternatively, he might actually take action in order to reduce a risk—to move out of the way of an oncoming car or pull the tack out of his foot. He might even pay someone more skilled to carry out a risky activity—electrical rewiring, for example—on his behalf.

Similarly, a company might recognize a potential risk but be content to do nothing about it; establish and enforce risk policies and limits; change strategic direction; make a tactical alteration to one of its business units; or transfer a specific risk through insurance or hedging.

Ultimately, the function of risk management, whether for an individual or for a company, is to ensure that the level of risk remains within some acceptable range, while ensuring that life or business continues to be as enjoyable as possible. It's worth noting that different people have different appetites for risk—they are comfortable with different amounts of risk and also with different types of risk. So are different companies, with internal risk limits and credit ratings being key measures of these propensities.

It's also worth noting that people don't really think about a risk, assess it, and finally do something about it. In practice, people constantly reevaluate their situation in a way that involves continuous feedback between thoughts, senses, and actions. The same should be true for any company operating in the real world. A risk management process can only be effective

to the extent that risk awareness, risk measurement, and risk control strategies are fully integrated. We'll discuss these three components in the next sections.

RISK AWARENESS

Risk awareness is the starting point of any risk management process. The objective of promoting risk awareness is to ensure that everyone within a business is:

- Proactively identifying the key risks for the company;
- Seriously thinking about the consequences of the risks for which he or she is responsible; and
- Communicating up and down the organization those risks that warrant others' attention.

In a risk-aware environment, most risk management issues should be addressed before they become bigger problems.

There are many organizational processes and initiatives that can promote risk awareness within a company. Five of the most successful are:

1. Set the tone from the top;
2. Ask the right questions;
3. Establish a risk taxonomy;
4. Provide training and education; and
5. Link compensation to risk.

Let's consider these in turn.

Set the Tone from the Top

In risk management even more than other corporate initiatives the involvement of senior management, and of the CEO in particular, is critical to success. The reason? Some aspects of risk management run counter to human nature. While people are eager to talk about marketing or product successes, or even cost-saving opportunities, they are generally much less enthusiastic about discussing actual or potential losses, particularly those related to their businesses.

Overcoming this reluctance requires applied authority and power. The CEO must therefore be fully supportive of the risk management process, and "set the tone" not only through words, but also through actions.

The CEO must first communicate that risk management is a top priority for the company at presentations, meetings, and in other forums. More importantly, the CEO must demonstrate his or her commitment through actions. Does the CEO actively participate in risk management meetings? Has the company allocated an appropriate budget to support risk management? Are senior risk executives involved in major corporate decisions? What happens when a top producer violates risk management policies? How the CEO and senior management respond to these questions will speak volumes about their true commitment to the risk management process.

Ask the Right Questions

It has been said that senior management may not always have the right answers, but it is their obligation to ask the right questions. So what are the key questions senior management should ask about risk? The acronym R.I.S.K.—Return, Immunization, Systems, and Knowledge—can help:

- ***Return.*** What are the expected returns on the risks we are taking? What kinds of risk exposures are being created if a business unit is growing or making money at an exceptional rate?
- ***Immunization.*** What limits and controls do we have in place to minimize the downside?
- ***Systems.*** Do we have the appropriate systems to track and measure risks?
- ***Knowledge.*** Do we have the right people and skills for effective risk management?

Establish a Risk Taxonomy

We saw in the last section how efficient communication is a key requirement for the risk management process. One of the ways in which communication can be made efficient is by ensuring that people understand what each other mean—something which is not a given in the world of risk, where definitions are frequently poorly understood, open to interpretation, or extremely broad. That is, a company should strive to establish a common language for risk.

One important part of this effort should be to establish a taxonomy of risk—a common structure for describing the categories and sub-categories of risks, as well as the tools, metrics, and strategies for risk management. A taxonomy is not only useful in talking about risks, but allows them to be broken

down into manageable components which can then be aggregated for exposure measurement and reporting purposes. This is not a one-off process; it should be iterative and reflect the dynamic and changing nature of the business.

Provide Training and Development

Executives involved in establishing risk management programs often cite training and development as one of their major accomplishments. In addition to promoting risk awareness, training and development equips employees with the skills and tools they need to manage the risks for which they are responsible.

Risk education should start at orientation, with new employees being introduced to risk management concepts and briefed on the various risk functions within the company just as they are introduced to its other management philosophies and operational functions. It should also include ongoing training programs that are tailored to the skills required for the individual's job responsibilities. These should tie the individual's responsibilities to the risk management policies of the company—and to the thinking behind them. To put it another way, employees should understand the spirit as well as the letter of the law.

Link Risk and Compensation

People naturally pay most attention to what their job accountabilities are and how their financial incentives are tied to their performance. Clearly, risk awareness can be most powerfully cultivated by making sure that employees understand that risk management is part of their job, and that their incentive compensation is linked to the business and risk performance at both the business and individual levels. It is important that these facts should be seen to be true for *all* employees. If there is a perception that the same ground rules don't apply to all employees (particularly senior ones), others will soon stop paying attention or see the rules as something that can be circumvented in the pursuit of a career.

RISK MEASUREMENT

The axiom "what gets measured gets managed" is largely true in risk management. Unfortunately risk measurement and reporting remains a major challenge for many companies today. Most struggle with the constraints

associated with data, analytics, and systems resources. Frequently, there is no good historical data on losses and other risk metrics, and there is a lack of internal discipline to report and capture important risk information. At the other extreme, some companies drown their boards and senior managers in data, much of it irrelevant and impenetrable.

Whether or not a company has too much or too little risk data and reports, senior management and the board need appropriate risk information to support business and policy decisions. What should be included in an executive risk report? That partly depends, of course, on the nature of the business. However, there are certain key elements that should be a part of any executive risk report—losses, incidents, risk assessments, and key risk indicators. Let's consider these in turn.

Losses

Losses arising from credit, market, and operational risks should be systematically captured in a loss database and summarized in the risk report. While the loss database should account for losses at a detailed level, only overall levels of loss and important trends should be reported to senior management. The risk report should highlight specific losses above a threshold and total losses relative to revenue or volume. Businesses should also track actual losses against expected or budgeted levels.

Incidents

The risk report should report the major risk incidents for the period, regardless of whether these result in a financial loss or not. Risk incidents might include loss of a major customer account, policy violations, systems failures, frauds, lawsuits, and so on. The potential impact, root causes, and business response to the major incidents should be reported. Any emerging trends or significant patterns in incidents should also be highlighted.

Risk Assessments

While losses and incidents reflect risk performance after the fact, the risk report should also provide management's advance assessment of potential risks. The risk concepts discussed earlier should underpin this assessment. This portion of the risk report should address questions such as: What keeps you up at night? What are your top 10 risks? What uncertainties might prevent the achievement of business objectives? These are different questions that should

lead management to the same answers. Key risks might include new business or product launches, the absence of key staff, new technologies, and more.

Key Risk Indicators

The risk report should also include a section on the key risk indicators that quantify major trends and risk exposures for the business. These indicators might, for example, include credit exposures compared with credit limits in lending, or mark-to-market profit and loss (P&L) and value-at-risk (VaR) for trading businesses. Operational risk indicators might include processing errors, customer complaints, systems downtime, and unreconciled items. Risk/return metrics might include return on economic capital for businesses or the Sharpe ratio for investment portfolios.

It is important that the key risk indicators include forward-looking metrics that serve as early-warning signals. For example, widening credit spreads are usually an early warning of higher default rates and/or decreasing market liquidity. Higher employee turnover may be a leading indicator of increasing operational risks, such as higher error rates and lower customer satisfaction. Such early-warning indicators allow management to take pre-emptive action to mitigate potential risks. While businesses may track dozens or hundreds of risk indicators, they should report only the few that warrant senior management and board attention.

The prototype report in Figure 3.1 shows the key elements that should be included in a risk report. This risk reporting structure contains a self-correcting feature that should be a design requirement. That feature works as follows: losses and incidents are items that can be captured easily on a regular basis. Over time, however, management may notice that losses and incidents originate from risks that are not qualitatively discussed in risk assessments or quantitatively tracked in key risk indicators. It then has at least one of two problems that need to be addressed. Either the business or operational unit needs to improve its risk assessment and measurement efforts, and/or they are not escalating important risk issues to corporate management. Such a self-correcting feature should improve the quality and candor of risk measurement and reporting on continuous basis.

RISK CONTROL

The risk management process does not stop at promoting risk awareness or measuring risk exposures. The ultimate objective is to optimize the risk/return of the business; or, to put it slightly differently, to effect real change in

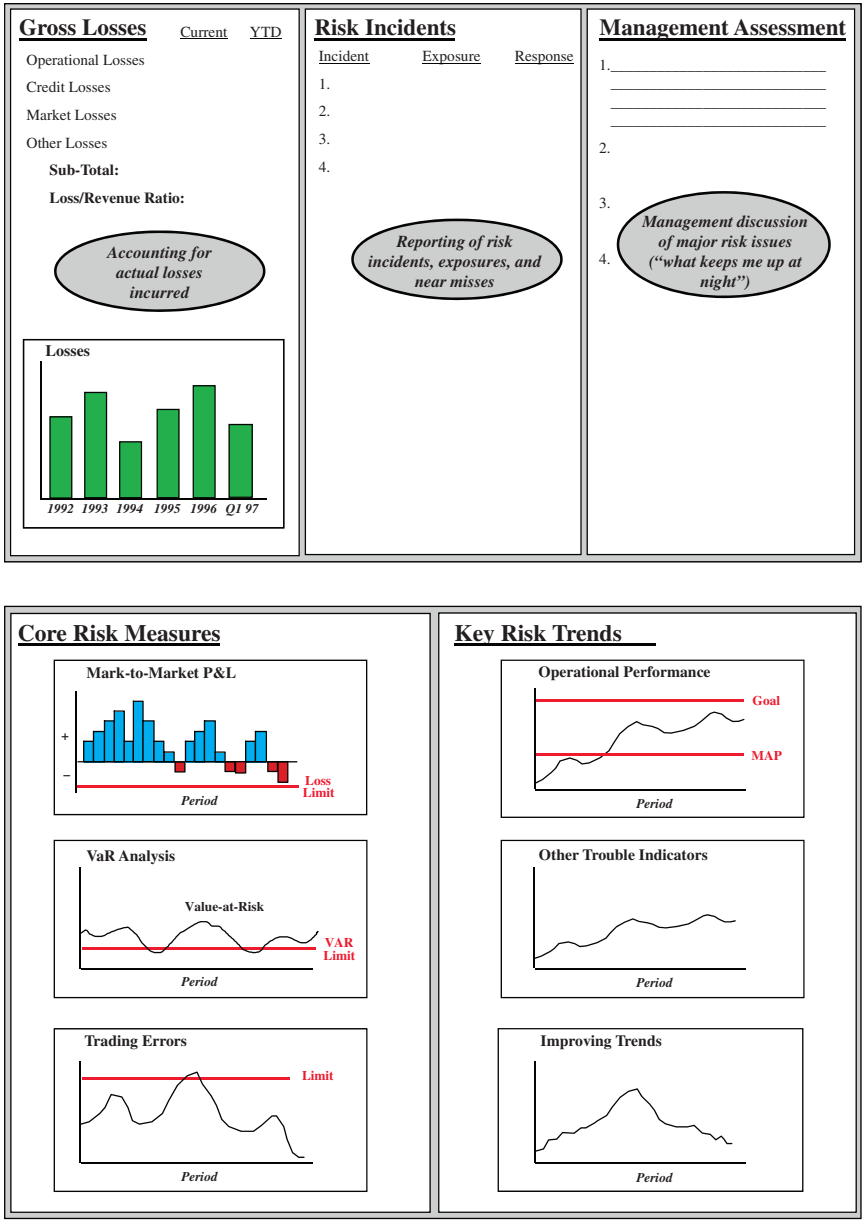


FIGURE 3.1 Risk Report

the risk profile of the company. There are three fundamental ways in which this can be done. The first is to support business growth; the second, to support profitability; the third, to control downside risks.

Support Business Growth

Risk management has a role to play as part of a cross-functional team that supports business growth. The risk team should work with line management, marketing, legal, operations, and technology representatives to establish and maintain a review process for vetting new business strategies[1] and ideas. This review process brings the right people together to discuss key issues at an early stage.

The review team should develop fair and objective criteria against which businesses and products will be evaluated, both at their outset and on an ongoing basis. This is not dissimilar to the way that many organizations handle individual risks. Banks, for example, compose lists of acceptable counterparties to speed up the approval process when a credit-sensitive transaction is proposed, and review outstanding transactions if the counterparty's status changes in well-defined ways, such as a decline in credit rating.

A key lever by which management can optimize risk/return is by allocating corporate resources to business activities with the highest risk-adjusted returns, subject to the risk limits discussed below. A risk/return matrix (as shown in Figure 3.2) can be a powerful strategic planning tool. This matrix shows the level of risk, expressed in economic capital and the return on that capital (i.e., ROE), for each business unit and risk type, and can be used to determine:

- Which business units are meeting or beating their hurdle rates of return on equity and thus contributing to shareholder value, and which business units are not?
- Are the credit, market, and operational risk levels at the businesses consistent with our expectations for their business plans?
- Do we have the right people and systems in place to manage these risk levels, both at corporate management and within the business units?
- How should we reallocate corporate resources in order to optimize risk/return and maximize shareholder value?

Support Profitability

Risk management can improve business profitability, as well as growth, by influencing pricing decisions. Put simply, the idea is that the price for any

Organizational Unit	Credit Risk	Market Risk	Operational Risk	Other	Total
Business Unit A	Economic Capital / ROE	$ / %	$ / %	$ / %	$ / %
Business Unit B					
• • •					
Business Unit N					
TOTAL	$ / %	$ / %	$ / %	$ / %	$ / %

FIGURE 3.2 Risk Matrix

product or transaction should reflect the cost of its underlying risks as well as more traditional costs. The cost of risk would obviously be higher for riskier transactions.

For example, the pricing on a loan should include the expected annual loss and the cost of capital[2] reserved against the loan, as well as funding and operational costs. In practice, commercial loans are often not fully priced, since banks frequently use lending to cement a customer relationship, not to generate profits as a standalone product. Risk-adjusted pricing can't change that fact of business life, but it does ensure that the bank knows how much it should be making from the customer overall to make up for the cheap loan. Risk-adjusted pricing has been applied throughout the financial services industry.

Non-financial corporations have been slower to adopt it, but can also benefit. Net present value (NPV) or economic value added (EVA) techniques for evaluating new investments and business performance do not usually incorporate the full cost of risk. This is because these tools are usually based on book capital, which typically doesn't fully capture expected loss, much less unexpected loss, and thus does not correspond to economic capital. The upshot is that NPV and EVA models are not sensitive to the underlying risks of the business. As such, they tend to overstate the profitability of high-risk businesses, and understate the profitability of low-risk ones. Adjustments to incorporate the full cost of risk, or the use

of economic capital instead of book capital, should greatly enhance the usefulness of these models.

Control Downside Risks

While risk management supports business growth and profitability, it should also control downside risks. It is important to remember that downside risks, including losses and failures, are an integral part of doing business.

A drug company faces the risk of a significant loss in research and marketing costs every time it introduces a new drug. A bank faces the risk of default with every loan. Any company developing a product or system faces the risk of cost overruns, schedule delays, and eventual underperformance.

The point here is that business is all about taking risks, and that risk management should not seek to eliminate downside risks, but to control them within an acceptable range. The acceptable range, as suggested earlier, will reflect the company's risk appetite, which is in turn determined by the human, financial, and technology resources available to manage the business and its associated risks. The risk appetite can be expressed in terms of the amount and likelihood of actual and potential loss; these are in turn controlled through stop-loss and sensitivity limits respectively.

Stop-loss limits control the amount of losses an institution can incur due to its risk positions. While stop-loss limits have been widely adopted in controlling market risk for trading houses, the same concept can be extended to other types of risk. For example, a stop-loss limit can be established for credit risk with actual credit losses being measured by the combination of charge-offs (i.e., realized losses) and *mark-to-market* losses based on credit spreads[3] (i.e., unrealized losses). For operational risks, management can control downside risk by setting limits on indicators such as error rates, systems downtime, and outstanding audit items.

When actual loss or performance hits one of these limits, it should trigger some management decision or action, including management reviews, hedging strategies, contingency plans, or exit strategies. Some companies even establish warning limits below the stop-loss limits, acting like the yellow signal before the red at the traffic light.

Sensitivity limits ensure that potential economic losses do not exceed management's threshold levels. Sensitivity limits control the amount of capital an institution has at risk given various adverse economic scenarios and its risk positions. These sensitivity limits can be developed by taking extreme values of risk factors such as market volatility or by repeatedly simulating the evolution of the business and the environment over time.

The key use of sensitivity limits is in avoiding excessive concentrations of risk. If a risk position exceeds the sensitivity limit, management will know that the potential loss in that business may be greater than what they want to accept and they may cut back or otherwise mitigate that risk accordingly. The concepts of stop-loss and sensitivity limits are generally applied in market and credit risk management, but are closely analogous to the total quality management (TQM) techniques used for operational risk management. Companies such as General Electric and Allied-Signal track actual and potential error rates against a six-sigma standard and corrective actions are taken if performance falls below that threshold.

In addition to stop-loss and sensitivity limits, basic exposure limits (total credit exposure to emerging markets, say, or market exposure to technology stocks) can be established to control downside risks. Setting risk limits is, however, only part of the risk control process. If they are to be useful, information about limits (and particularly about violations of limits) must be reported efficiently to management, who must then act on this information decisively whenever necessary.

The appropriate frequency of reporting depends on both the nature of the business and on the audience. Companies trading in global capital markets or managing multi-site phone centers, for example, might need real-time risk monitoring for the business managers. Companies operating in less volatile conditions might need daily or weekly reporting. A monthly or quarterly interval should be appropriate for limit reports that go to senior management and the board.

Capital allocation, risk-adjusted pricing, and limit setting are three ex ante ways of controlling how much risk a company takes on. However, this is at best half the story: there are other techniques available for managing the risks that have already been taken on. One part of such management is to understand what those risks actually are, which implies a focus on better risk analysis and on the data and technology needed to perform and report on such analysis.

Another is to understand which risks offset or exacerbate each other. Duration matching is a common risk management technique under which a financial institution matches the interest rate sensitivities of its assets and liabilities to make sure that their prices change in the same way when interest rates change. Active portfolio management, which grew increasingly popular at financial institutions in the 1990s, is another technique that seeks to establish if a new risk will disproportionately increase or decrease the overall risk of a portfolio.

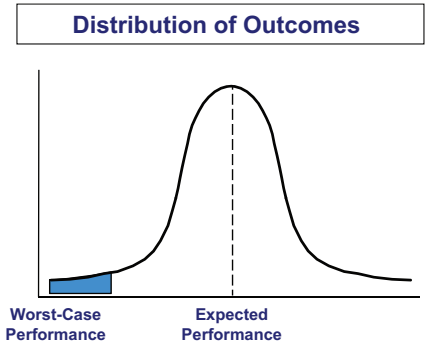
These internal management techniques are usually preferred because they are typically longer term and more cost effective than transferring risk

to an external party. However, they take time to implement and can only alter a company's risk profile up to a point. When time, resources, or flexibility are scarce, risk transfer, through either derivatives or insurance, can provide timely and effective solutions.

RISK IS A BELL CURVE

We've introduced a range of key concepts and processes in this chapter. One simple way of unifying all of these concepts is to think of risk as a bell curve, such as the one depicted in Figure 3.3. The mean of the bell curve represents expected performance. Risks are variables that can cause actual performance to deviate, either for better or for worse, from the expected performance. The distribution of potential outcomes in terms of the range of the bell curve represents the risk.

The objective of risk management is to optimize risk/return tradeoff, or to optimize the shape of the bell curve. In other words, risk management strategies are meant to improve expected performance and/or narrow the distribution of potential outcomes. Management may accept a wider distribution of outcomes if the improvement in expected performance warrants it. Let's consider the idea of risk as a bell curve in terms of five major types of risk.



Examples:

1. **Strategic risk. Enterprise value vs. value drivers**
2. **Business risk. Expected earnings per share (EPS) vs. earnings drivers**
3. **Financial risk. Net interest margin vs. interest rate changes**
4. **Operational risk. IT performance vs. single points of failure (SPOFs) and cyber security**
5. **Regulatory risk. Regulatory standing vs. compliance requirements**

FIGURE 3.3 Risk is a Bell Curve

Strategic risk

In strategic risk, expected performance can be thought of as the projected enterprise value based on the long-term strategic plan. The risks that could increase or decrease that value include macroeconomic conditions, competitive actions, and the company's effectiveness in formulating and executing its strategic plan. These variables represent the strategic risk for the company.

Business risk

In terms of business risk, projected earnings per share (EPS) for the next year can be a good proxy for expected performance. The risks involved in achieving that objective may include market share, new customers, pricing margins, and cost management. These risks could drive earnings volatility.

Financial risk

With respect to financial risk, we can use interest rate risk as an example. Expected performance could be represented by net interest margin or the difference between interest income and interest expense. Key risk variables may include asset/liability duration mismatches, interest rate levels, and pricing spreads.

Operational risk

Using information technology (IT) as an example, the expected performance may be that critical systems are available at least 99 percent of the time. Key risk variables may include single points of failure (SPOFs) that could bring down these critical systems or cyber security exposures that could allow harmful viruses or malware to enter the IT environment.

Regulatory risk

For most companies, expected performance would be excellent regulatory standing in terms of compliance with key laws and regulations. Potential risks include new regulations that the company may not be fully prepared for or new employees who are not aware or trained in the company's compliance procedures.

All of the concepts and techniques discussed in this chapter can be applied to a single risk. However, their true power emerges when they are used to manage a portfolio of risks in an integrated manner. We'll see why that should be in the next section.

CHAPTER 4

What Is ERM?

In the last chapter, we reviewed the concepts and processes applicable to almost all of the risks that a company will face. We also argued that all risks can be thought of as a bell curve. Certainly, it is a prerequisite that a company develop an effective process for each of its significant risks. But it is not enough to build a separate process for each risk in isolation.

Risks are by their very nature dynamic, fluid, and highly interdependent. As such, they cannot be broken into separate components and managed independently. Enterprises operating in today's volatile environment require a much more integrated approach to managing their portfolio of risks.

This has not always been recognized. Traditionally, companies managed risk in organizational silos. Market, credit, and operational risks were treated separately and often dealt with by different individuals or functions within an institution. For example, credit experts evaluated the risk of default, mortgage specialists analyzed prepayment risk, traders were responsible for market risks, and actuaries handled liability, mortality, and other insurance-related risks. Corporate functions such as finance and audit handled other operational risks, and senior line managers addressed business risks.

However, it has become increasingly apparent that such a fragmented approach simply doesn't work, because risks are highly interdependent and cannot be segmented and managed by entirely independent units. The risks associated with most businesses are not one-to-one matches for the primary risks (market, credit, operational, and insurance) implied by most traditional organizational structures. Attempting to manage them as if they are is likely to prove inefficient and potentially dangerous. Risks can fall through the cracks, risk inter-dependencies and portfolio effects may not be captured, and organizational gaps and redundancies can result in suboptimal performance. For example, imagine that a company is about to launch a new product or business in a foreign country. Such an initiative would require:

- The business unit to establish the right pricing and market-entry strategies;
- The treasury function to provide funding and protection against interest rate and foreign-exchange (FX) risks;
- The Information Technology (IT) and operations function to support the business; and
- The legal and insurance functions to address regulatory and liability issues.

It is not difficult to see how an integrated approach could more effectively manage these risks. An enterprise risk management (ERM) function would be responsible for establishing firm-wide policies and standards, co-ordinate risk management activities across business units and functions, and provide overall risk monitoring for senior management and the board.

Nor is risk monitoring any more efficient under the silo approach. The problem is that individual risk functions measure and report their specific risks using different methodologies and formats. For example, the treasury function might report on interest rate and FX risk exposures, and use value-at-risk as its core risk measurement methodology. On the other hand, the credit function would report delinquencies and outstanding credit exposures, and measure such exposures in terms of outstanding balances, while the audit function would report outstanding audit items and assign some sort of audit score, and so on.

Senior management and the board get pieces of the puzzle, but not the whole picture. In many companies, the risk functions produce literally hundreds of pages of risk reports, month after month. Yet, oftentimes, they still don't manage to provide management and the board with useful risk information. A good acid test is to ask if the senior management knows the answers to the following basic questions:

- What are the company's top 10 risks?
- Are any of our business objectives at risk?
- Do we have key risk indicators that track our critical risk exposures against risk tolerance levels?
- What were the company's actual losses and incidents, and did we identify these risks in previous risk assessment reports?
- Are we in compliance with laws, regulations, and corporate risk policies?

If a company is uncertain about the answers to any of these questions, then it is likely to benefit from a more integrated approach to handling all aspects of risk—enterprise risk management (ERM).[1]

ERM DEFINITIONS

Since the practice of ERM is still relatively new, there have yet to be any widely accepted industry standards with regard to the definition of ERM. As such, a multitude of different definitions is available, all of which highlight and prioritize different aspects of ERM. Consider, for example, a definition provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2004:

> *"ERM is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

Another definition was established by the International Organization of Standardization (ISO 31000):

> *Risk is the "effect of uncertainty on objectives" and risk management refers to "coordinated activities to direct and control an organization with regard to risk."*

While the COSO and ISO definitions provide useful concepts (e.g., linkage to objectives), I think it is important that ERM is defined as a value-added function. Therefore, I would suggest the following definition:

> *Risk is a variable that can cause deviation from an expected outcome. ERM is a comprehensive and integrated framework for managing key risks in order to achieve business objectives, minimize unexpected earnings volatility, and maximize firm value.*

The lack of a standard ERM definition can cause confusion for a company looking to set up an ERM framework. No ERM definition is perfect or applicable to every organization. My general advice is for each organization to adopt an ERM definition and framework that best fit their business scope and complexity.

THE BENEFITS OF ERM

ERM is all about integration, in three ways.

First, enterprise risk management requires an integrated risk organization. This most often means a centralized risk management unit

reporting to the CEO and the Board in support of their corporate- and board-level risk oversight responsibilities. A growing number of companies now have a Chief Risk Officer (CRO) who is responsible for overseeing all aspects of risk within the organization—we'll consider this development later.

Second, enterprise risk management requires the integration of risk transfer strategies. Under the silo approach, risk transfer strategies were executed at a transactional or individual risk level. For example, financial derivatives were used to hedge market risk and insurance to transfer out operational risk. However, this approach doesn't incorporate diversification within or across the risk types in a portfolio, and thus tends to result in over-hedging and excessive insurance cover. An ERM approach, by contrast, takes a portfolio view of all types of risk within a company and rationalizes the use of derivatives, insurance, and alternative risk transfer products to hedge only the residual risk deemed undesirable by management.

Third, enterprise risk management requires the integration of risk management into the business processes of a company. Rather than the defensive or control-oriented approaches used to manage downside risk and earnings volatility, enterprise risk management optimizes business performance by supporting and influencing pricing, resource allocation, and other business decisions. It is during this stage that risk management becomes an offensive weapon for management.

All this integration is not easy. For most companies, the implementation of ERM implies a multi-year initiative that requires ongoing senior management sponsorship and sustained investments in human and technological resources. Ironically, the amount of time and resources dedicated to risk management is not necessarily very different for leading and lagging organizations.

The most crucial difference is this: leading organizations make rational investments in risk management and are proactive, optimizing their risk profiles. Lagging organizations, on the other hand, make disconnected investments and are reactive, fighting one crisis after another. The investments of the leading companies in risk management are more than offset by improved efficiency and reduced losses.

Let's discuss the three major benefits to ERM: increased organizational effectiveness, better risk reporting, and improved business performance.

Organizational Effectiveness

Most companies already have risk management and corporate-oversight functions, such as finance/insurance, audit and compliance. In addition, there may be specialist risk units: for example, investment banks usually

have market risk management units, while energy companies have commodity risk managers.

The appointment of a chief risk officer and the establishment of an enterprise risk function provide the top-down coordination necessary to make these various functions work cohesively and efficiently. An integrated team can better address not only the individual risks facing the company, but also the interdependencies between these risks.

Risk Reporting

As previously noted, one of the key requirements of risk management is that it should produce timely and relevant risk reporting for the senior management and board of directors. As we also noted, however, this is frequently not the case. In a silo framework, either no one takes responsibility for overall risk reporting, and/or every risk-related unit supplies inconsistent and sometimes contradictory reports.

An enterprise risk function can prioritize the level and content of risk reporting that should go to senior management and the board: an enterprise-wide perspective on aggregate losses, policy exceptions, risk incidents, key exposures, and early-warning indicators. This might take the form of a risk dashboard that includes timely and concise information on the company's key risks. Of course, this goes beyond the senior management level; the objective of ERM reporting is by its nature to increase risk transparency throughout an organization.

Business Performance

Companies that adopt an ERM approach have experienced significant improvements in business performance. Figure 4.1 provides examples of reported benefits of ERM from a cross-section of companies. ERM supports key management decisions such as capital allocation, product development and pricing, and mergers and acquisitions. This leads to improvements such as reduced losses, lower earnings volatility, increased earnings, and improved shareholder value.

These improvements result from taking a portfolio view of all risks; managing the linkages between risk, capital, and profitability; and rationalizing the company's risk transfer strategies. The result is not just outright risk reduction: companies that understand the true risk/return economics of a business can take more of the profitable risks that make sense for the company and less of the ones that don't. We'll go into more detail on how these improvements are achieved in subsequent chapters.

Benefit	Company	Actual Results
Market value improvement	Top money center bank	Outperformed S&P 500 banks by 58% in stock price performance
Early warning of risks	Large commercial bank	Assessment of top risks identified over 80% of future losses; global risk limits cut by one-third prior to Russian crisis
Loss reduction	Top asset-management company	30% reduction in the loss ratio enterprise-wide; up to 80% reduction in losses at specific business units
Regulatory capital relief	Large international commercial and investment bank	$1 Billion reduction of regulatory capital requirements, or about 8-10%
Risk transfer rationalization	Large property and casualty insurance company	$40 million in cost savings, or 13% of annual reinsurance premium
Insurance premium reduction	Large manufacturing company	20-25% reduction in annual insurance premium

FIGURE 4.1 ERM Benefits

Despite all these benefits, many companies would balk at the prospect of a full-blown ERM initiative were it not for the existence of heavy internal and external pressures. In the business world, managers are often galvanized into action after a near miss—either a disaster averted within their own organization or an actual crisis at a similar organization.

In response, the board and senior management are likely to question the effectiveness of the control environment and the adequacy of risk reporting within their company. To put it another way, they will begin to question how well they really know the organization's major risk exposures.

Such incidents are also often followed by critical assessments from auditors and regulators—both groups which are constitutionally concerned with the effectiveness of risk management. Consequently, regulators focus on all aspects of risk during examinations, setting risk-based capital and compliance requirements, and reinforcing key roles for the board and senior management in the risk management process.

This introspection often leads to the emergence of a risk champion among the senior executives who will sponsor a major program to establish an enterprise risk management approach. As noted above, this risk champion is increasingly becoming a formalized senior management position—the chief risk officer, or CRO.

Aside from this, direct pressure also comes from influential stakeholders such as shareholders, employees, ratings agencies, and analysts. Not only

do such stakeholders expect more earnings predictability, management have fewer excuses today for not providing it. Over the past few years, volatility-based models such as value-at-risk (VaR) and risk-adjusted return on capital (RAROC) have been applied to measure all types of market risk within an organization; their use is now spreading to credit risk, and even to operational risk. The increasing availability and liquidity of alternative risk transfer products—such as credit derivatives and catastrophe bonds—also means that companies are no longer stuck with many of the unpalatable risks they previously had no choice but to hold. Overall, the availability of such tools makes it more difficult and less acceptable for companies to carry on with more primitive and inefficient alternatives. Managing risk is management's job.

THE CHIEF RISK OFFICER

The role of a chief risk officer has received a lot of attention within the risk management community, as well as from the finance and general management audiences. Articles on chief risk officers and ERM appear frequently in trade publications such as *Risk Magazine* and *Risk and Insurance*, but have also been covered in general publications such as *CFO* magazine, the *Wall Street Journal*, and even *USA Today*.

Before I discuss the role of the chief risk officer, let me share with you how I came up with that title. In August 1993, Rick Price hired me to help him set up a new capital markets business within the Financial Guaranty Insurance Group at GE Capital. My job was to manage all aspects of risk, and I had direct management responsibilities for all functions outside of sales and trading, which included market and credit risk management, back-office operations, and business and financial planning.

Since this was a new business, Rick didn't have a title in mind for me and asked me to come up with an appropriate one. Around this time, GE and many other companies were appointing "chief information officers" (CIOs) whose jobs were to integrate IT resources and elevate the role of technology in the business. Today's CIOs are usually responsible for developing and implementing integrated technology strategies that include mainframes, PCs, networks, and the Internet.

The CIO trend and my new integrated responsibilities for market, credit, and operational risks gave me the idea for the role and title of the chief risk officer or CRO. The CRO would be responsible for developing and implementing an ERM strategy including all aspects of risk. I used the CRO title at GE Capital and subsequently at Fidelity Investments.

Today, the role of the CRO has been widely adopted in risk-intensive businesses such as financial institutions, energy firms, and non-financial

corporations with significant investment activities and/or foreign operations. Today, I would estimate that as many as up to 80 percent of the biggest U.S. financial institutions have CROs.

The recent financial and economic meltdowns have increased the demand for comprehensive ERM frameworks. As an indication of this increased demand, executive management training programs in ERM are increasingly offered by leading business schools. For example, in November 2010, Harvard Business School implemented a five-day program designed to train CEOs, COOs, and CROs in managing risk as corporate leaders: there have been two other sessions to date, one in February 2012, and one just recently, in February 2013.[2]

Typical reports to the CRO are the heads of credit risk, market risk, operational risk, insurance, and portfolio management. Other functions that the CRO is commonly responsible for include risk policy, capital management, risk analytics and reporting, and risk management within individual business units. In general, the office of the CRO is directly responsible for:

- Providing the overall leadership, vision, and direction for enterprise risk management;
- Establishing an integrated risk management framework for all aspects of risks across the organization;
- Developing risk management policies, including the quantification of the firm's risk appetite through specific risk limits;
- Implementing a set of risk indicators and reports, including losses and incidents, key risk exposures, and early warning indicators;
- Allocating economic capital to business activities based on risk, and optimizing the company's risk portfolio through business activities and risk transfer strategies;
- Communicating the company's risk profile to key stakeholders such as the board of directors, regulators, stock analysts, rating agencies, and business partners; and
- Developing the analytical, systems, and data management capabilities to support the risk management program

Still, given that enterprise risk management is still a relatively new field, many of the kinks have yet to be smoothed out of the Chief Risk Officer role. For example, there are still substantial amounts of ambiguity with regard to where the CRO stands in the hierarchy between the board of directors and other C-level positions, such as CEOs, CFOs, and COOs.

In many instances, the CRO reports to the CFO or CEO—but this can make firms vulnerable to internal friction when serious clashes of interest

occur between corporate leaders. For example, when Paul Moore, former head of regulatory risk at HBOS, claimed that he had been "fired . . . for warning about reckless lending," the resulting investigations led to the resignation of HBOS' chief executive, Sir James Crosby, as the deputy chairman of the Financial Services Authority.[3]

One organizational solution is to establish a dotted-line reporting relationship between the chief risk officer and the board or board risk committee. Under extreme circumstances (e.g. CEO/CFO fraud, major reputational or regulatory issues, excessive risk taking beyond risk appetite tolerances), that dotted line may convert to a solid line so that the chief risk officer can go directly to the board without fear for his or her job security or compensation. Ultimately, to be effective, risk management must have an independent voice. A direct communication channel to the board is one way to ensure that this voice is heard.[4]

For these dotted-line reporting structures between the CRO and the board (and between the business line risk officers and the CRO), it is critical that an organization clearly establish and document the ground rules. Basic ground rules include risk escalation and communication protocols, and the role of the board or CRO in hiring/firing, annual goal setting, and compensation decisions of risk and compliance professions who report to them.

Another board risk oversight option is to alter existing audit committees to incorporate risk management. In a survey of the S&P 500, "58 percent of respondents said that their audit committees were responsible for risk management."[5] However, this presents problems of its own; oftentimes, audit committees are already working at maximum capacity just handling audit matters, and are unable to properly oversee ERM as well. Henry Ristuccia, of Deloitte, affirms that unless the "audit committee [can improve] its grasp of risk management . . . a separate risk committee needs to be formed."[6]

The lack of an ERM standard is also a significant barrier to the positive development of the CRO role. Mona Leung, CFO of Alliant Credit Union, says that "we have too many varying definitions" of enterprise risk management, with the result that ERM means something different to every company, and is implemented in different ways. Of course, firms from different industries should (and must) tailor their approaches to risk management in order to meet the requirements of their specific business models and regulatory frameworks, but nonetheless, it is important to have a general ERM standard.

Despite the remaining ambivalences in the structure of the CRO role, I believe that it has elevated the risk management profession in some important ways. First and foremost, the appointment of executive managers whose primary focus is risk management has improved the visibility

and organizational effectiveness of that function at many companies. The successes of these appointments have only increased the recognition and acceptance for the CRO position.

Second, the CRO position provides an attractive career path for risk professionals who want to take a broader view of risk and business management. In the past, risk professionals could only aspire to become the head of a narrowly focused risk function such as credit or audit. Nearly 70 percent of the 175 participants in one online seminar that I gave on September 13, 2000, said they aspired to become CROs.

Today, CROs have begun to move even further up the corporate ladder by becoming serious contenders for the positions of CEO and CFO. For example, Matthew Feldman, formerly CRO of the Federal Home Loan Bank of Chicago, was appointed its CEO and President in May of 2008. Likewise, Deutsche Bank CRO Hugo Banziger was a candidate for UBS CEO. Kevin Buehler, of McKinsey & Co.'s, affirms that the gradual movement of CROs from control functions to more strategic roles is the primary contributing factor to their success, and that with the coming years, this progress is only likely to accelerate.[7]

Finally, the value that companies attribute to CROs is reflected in the escalating salaries observed in the marketplace. Based on my discussions with CROs and executive recruiters, the high-end compensation packages for CROs have increased from the low to mid six figures in the beginning of the 1990s to more than seven figures by the end of the decade. Today, at large financial institutions a CRO can make upward of $10 million in annual compensation, and those reporting to the CRO are reporting up to seven-figure packages. Across different industries and organizational sizes, the average CRO salary was reported to be about $184,000: a 7.5 percent increase since 2008.[8]

Some argue that a company shouldn't have a CRO because that job is already fulfilled by the CEO or the CFO. Supporting this argument is the fact that the CEO is always going to be ultimately responsible for the risk (and return) performance of the company, and that many risk departments are part of the CFO's organization. So why create another C-level position of CRO and detract from the CEO's or CFO's responsibilities?

The answer is the same reason that companies create roles for other C-level positions, such as chief information officers or chief marketing officers. These roles are defined because they represent a core competency that is critical to the success for the company—the CEO needs the experience and technical skills that these seasoned professionals bring. Perhaps not every company should have a full-time CRO, but the role should be an explicit one and not simply one implied for the CEO or CFO.

For companies operating in the financial or energy markets, or other industries where risk management represents a core competency, the CRO position should be considered a serious possibility. A CRO would also benefit companies in which the full breadth of risk management experience does not exist within the senior management team, or if the build-up of required risk management infrastructure requires the full-time attention of an experienced risk professional.

What should a company look for in a CRO? An ideal CRO would have superb skills in five areas. The first would be the leadership skills to hire and retain talented risk professionals and establish the overall vision for ERM. The second would be the evangelical skills to convert skeptics into believers, particularly when it comes to overcoming natural resistance from the business units. Third would be the stewardship to safeguard the company's financial and reputational assets. Fourth would be to have the technical skills in strategic, business, credit, market, and operational risks. And, last but not least, fifth would be to have consulting skills in educating the board and senior management, as well as helping business units implement risk management at the enterprise level. While it is unlikely that any single individual would possess all of these skills, it is important that these competencies exist either in the CRO or elsewhere within his or her organization.

COMPONENTS OF ERM

A successful ERM program can be broken down into seven key components (see Figure 4.2). Each of these components must be developed and linked to work as an integrated whole. The seven components include:

1. Corporate governance to ensure that the board of directors and management have established the appropriate organizational processes and corporate controls to measure and manage risk across the company.
2. Line management to integrate risk management into the revenue-generating activities of the company (including business development, product and relationship management, pricing, and so on).
3. Portfolio management to aggregate risk exposures, incorporate diversification effects, and monitor risk concentrations against established risk limits.
4. Risk transfer to mitigate risk exposures that are deemed too high, or are more cost-effective to transfer out to a third party than to hold in the company's risk portfolio.

5. Risk analytics to provide the risk measurement, analysis, and reporting tools to quantify the company's risk exposures as well as track external drivers.
6. Data and technology resources to support the analytics and reporting processes.
7. Stakeholder management to communicate and report the company's risk information to its key stakeholders.

Let's consider these in turn.

Corporate Governance

Corporate governance ensures that the board of directors and management have established the appropriate organizational processes and corporate controls to measure and manage risk across the company. The mandate for effective corporate governance has been brought to the forefront by regulatory and industry initiatives around the world. These initiates include the Treadway Report from the United States, the Turnbull Report from the UK, and the Dey Report from Canada. All of these made recommendations for establishing corporate controls and emphasized the responsibilities of the board of directors and senior management. Additionally, the Sarbanes-Oxley Act provides both specific requirements and severe penalties for non-compliance.

From an ERM perspective, the responsibilities of the board of directors and senior management include:

- Defining the organization's risk appetite in terms of risk policies, loss tolerance, risk-to-capital leverage, and target debt rating.
- Ensuring that the organization has the risk management skills and risk absorption capability to support its business strategy.
- Establishing the organizational structure of the ERM framework and defining the roles and responsibilities for risk management, including the role of chief risk officer.
- Implementing an integrated risk measurement and management framework for strategic, business, operational, financial, and compliance risks.
- Establishing risk assessment and audit processes, as well as benchmarking company practices against industry best practices.
- Shaping the organization's risk culture by setting the tone from the top not only through words but also through actions, and reinforcing that commitment through incentives.
- Providing appropriate opportunities for organizational learning, including lessons learned from previous problems, as well as ongoing training and development.

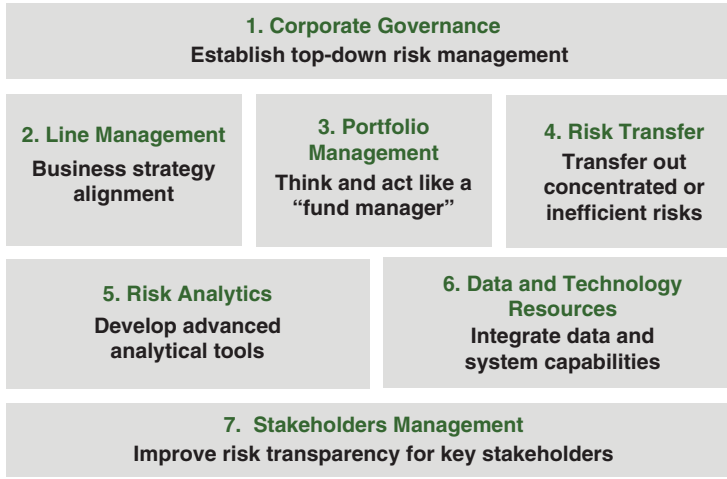


FIGURE 4.2 Seven Components of ERM

Line Management

Perhaps the most important phase in the assessment and pricing of risk is at its inception. Line management must align business strategy with corporate risk policy when pursuing new business and growth opportunities. The risks of business transactions should be fully assessed and incorporated into pricing and profitability targets in the execution of business strategy.

Specifically, expected losses and the cost of risk capital should be included in the pricing of a product or the required return of an investment project. In business development, risk acceptance criteria should be established to ensure that risk management issues are considered in new product and market opportunities. Transaction and business review processes should be developed to ensure the appropriate due diligence. Efficient and transparent review processes will allow line managers to develop a better understanding of those risks that they can accept independently and those that require corporate approval or management.

Portfolio Management

The overall risk portfolio of an organization should not just happen—that is, it should not just be the cumulative effect of business transactions conducted entirely independently. Rather, management should act like a fund manager and set portfolio targets and risk limits to ensure appropriate diversification and optimal portfolio returns.

The concept of active portfolio management can be applied to all the risks within an organization. Diversification effects from natural hedges can only be fully captured if an organization's risks are viewed as a whole, in a portfolio. More importantly, the portfolio management function provides a direct link between risk management and shareholder value maximization.

For example, a key barrier for many insurance companies in implementing ERM is that each of the financial risks within the overall business portfolio is managed independently. The actuarial function is responsible for estimating liability risks arising for the company's insurance policies; the investment group invests the company's cash flows in fixed-income and equity investments. The interest rate risk function hedges mismatches between assets and liabilities. However, an insurance company which has implemented ERM would manage all of its liability, investment, interest rate, and other risks as an integrated whole in order to optimize overall risk/return. The integration of financial risks is one step in the ERM process, while strategic, business, and operational risks must also be considered in the overall ERM framework.

Risk Transfer

Portfolio management objectives are supported by risk transfer strategies that lower the cost of transferring out undesirable risks, and also increase the organization's capacity to originate desirable but concentrated risks. To reduce undesirable risks, management should evaluate derivatives, insurance, and hybrid products on a consistent basis and select the most cost-effective alternative. For example, corporations such as Honeywell and Mead have used alternative risk transfer (ART) products that combine traditional insurance protection with financial risk protection. By bundling various risks, risk managers have achieved estimated savings of 20 to 30 percent in the cost of risk transfer.

A company can dramatically reduce its hedging and insurance costs—even without third-party protection—by incorporating the natural hedges that exist in any risk portfolio. In the course of doing business, companies naturally develop risk concentrations in their areas of specialization. The good news is that they should be very capable of analyzing, structuring, and pricing those risks. The bad news is that any risk concentration can be dangerous. By transferring undesirable risks to the secondary market—through credit derivatives or securitization, for example—an organization can increase its risk origination capacity and revenue without accumulating highly concentrated risk positions.

Finally, management can purchase desirable risks that they cannot directly originate on a timely basis, or swap undesirable risk exposures for desirable risk exposures through a derivative contract.

Risk Analytics

The development of advanced risk analytics has supported efforts to quantify and manage credit, market, and operational risks on a more consistent basis. The same techniques that allow for the quantification of risk exposures and risk-adjusted profitability can be used to evaluate risk transfer products such as derivatives, insurance, and hybrid products. For example, management can increase shareholder value through risk transfer provided that the cost of risk transfer is lower than the cost of risk retention for a given risk exposure (e.g., 12 percent all-in cost of risk transfer versus 15 percent cost of risk capital).

Alternatively, if management wants to reduce its risk exposure, risk analytics can be used to determine the most cost-effective way to accomplish that objective. In addition to risk mitigation, advanced risk analytics can also be used to significantly improve net present value (NPV)- or economic value added (EVA)-based decision tools. The use of scenario analyses and dynamic simulations, for example, can support strategic planning by analyzing the probabilities and outcomes of different business strategies as well as the potential impact on shareholder value.

Data and Technology Resources

One of the greatest challenges for enterprise risk management is the aggregation of underlying business and market data. Business data includes transactional and risk positions captured in different front- and back-office systems; market data includes prices, volatilities, and correlations. In addition to data aggregation, standards and processes must be established to improve the quality of data that is fed into the risk systems.

As far as risk technology goes, there is no single vendor software package that provides a total solution for enterprise risk management. Organizations still have to either build, buy, and customize or outsource the required functionality. Despite the data and system challenges, companies should not wait for a perfect system solution to become available before establishing an enterprise risk management program. Rather, they should make the best use of what is available and at the same time apply rapid prototyping techniques to drive the systems-development process. Additionally, companies should consider tapping into the power of the Internet/Intranet in the design of an enterprise risk technology platform.

Stakeholder Management

Risk management is not just an internal management process. It should also be used to improve risk transparency in a firm's relationship with key

stakeholders. The board of directors, for example, needs periodic reports and updates on the major risks faced by the organization in order to review and approve risk management policies for controlling those risks. Regulators need to be assured that sound business practices are in place, and that business operations are in compliance with regulatory requirements. Equity analysts and rating agencies need risk information to develop their investment and credit opinions.

An important objective for management in communicating and reporting to these key stakeholders is an assurance that appropriate risk management strategies are in effect. Otherwise, the company (and its stock price) will not get full credit, since interested parties will see the risks but may not see the controls. The increasing emphasis of analyst presentations and annual reports on a company's risk management capabilities is evidence of the importance now placed on stakeholder communication.

In this chapter we provided an overview of what is ERM. In the following chapters we will discuss each of the seven components of ERM in greater detail.

SECTION

Two

The Enterprise Risk Management Framework

CHAPTER 5

Corporate Governance

The 1990s can be considered the early years in ERM. These years were marked by a series of major risk management failures, with some of them—including those that struck at Barings Bank, Metallgesellschaft, and Sumitomo—generating damages of more than one *billion* dollars. The 2000s saw even more dramatic corporate frauds and failures—Enron, WorldCom, Adelphia—that destroyed tens of billions of shareholder value and brought equity markets to their knees.

These disasters had devastating consequences for the stakeholders of the companies involved—investors, employees, customers, and business partners. Some even threatened the stability of entire markets. For example, the collapse of Barings, in which rogue trader Nick Leeson racked up his colossal losses, threatened to seriously unsettle the futures markets. In the global copper market, Sumitomo's Yasuo Hamanaka was notoriously known as "Mr. Five Percent" due to his share of the market. The downfall of Enron—ironically once considered a leading institution in energy risk management—had severely hurt the energy trading markets.

The 2008 financial crisis brought even more turmoil to the global financial markets and underlying investor confidence in these markets. Notably, the collapse of AIG, Bear Stearns, Lehman Brothers, and other large financial institutions wreaked havoc in the interconnected global economies, dried up liquidity and trading in financial markets, and resulted in the loss of confidence in the overall capital markets system. In 2011, the Financial Crisis Inquiry Commission wrote: "the greatest tragedy would be to accept the refrain that no one could have seen this coming and thus find nothing could have been done. If we accept this notion, it will happen again."

The examinations that followed each of these cases, and others, revealed a common theme behind the institutions' troubles: a lack of effective risk management and board oversight of corporate and business operations. That in turn prompted a renewed emphasis from regulators, stock exchanges, and institutional investors on compliance with codes of best practice for

corporate governance. The passage of the Sarbanes-Oxley Act in 2002 established clear rules for corporate governance practices, such as requiring financial statement certification by the CEO and CFO, and ensuring independence of auditors and audit committees.

Corporate governance is an essential component of enterprise risk management because it provides top-down monitoring and management of risk. What is it? A straightforward definition of corporate governance comes from the California Public Employees' Retirement System (CalPERS), a major institutional shareholder and enthusiastic proponent of shareholder activism:

> *"The relationship among various participants in determining the direction and performance of corporations. The primary participants are (1) shareowners, (2) management (led by the chief executive officer), and (3) the board of directors."*[1]

Senior management and the board of directors have a responsibility to ensure that effective risk management is in place—a responsibility to the shareholders and business partners who stand to lose money, to the employees who stand to lose their livelihoods, and to other stakeholders in the business—but are removed from the day-to-day risk-taking activities of the company. Corporate governance allows them to manage the overall company risk profile.

The discipline of corporate governance begins at the top. The critical questions here are: How is a corporation's board of directors structured? Does it operate in a way that ensures their ability to fulfill their obligation to safeguard the resources of the company and the interests of corporate stakeholders?

Effective corporate governance requires the board to focus on general oversight and stewardship of the corporation, and to refrain from involvement in the day-to-day operations of the company. In this way, the board is able to maintain an integrated and relatively objective perspective on the company's operations, which helps it to steer the firm in the direction that will most benefit not only shareholders, but also the corporation in its entirety.

With the aid of a competent risk management function and an appropriate organizational structure, they can then direct and influence business and risk activities through policies and limits; ensure compliance with risk measurement and reporting, as well as audit processes; and create a strong culture that encourages desired business behavior by implementing compensation programs that reward risk-adjusted performance.

CODES OF CONDUCT

In recent years, different bodies around the world have written a number of codes of best practice on corporate governance. Many of these were commissioned by various stock exchanges worldwide, others by industry or executive associations, and some by institutional investors. One—the General Motors Board Guidelines—was actually commissioned by a corporation.

In the United Kingdom and in North America, as well as in many other countries around the world, Codes of Best Practice on Corporate Governance are coming to have a strong impact on how companies govern themselves. It is extremely important to note, however, that compliance with these guidelines is typically voluntary, although disclosure of compliance or non-compliance may not be. Both the London and Toronto Stock Exchanges, for example, now require companies listed on those exchanges to report annually on whether or not they comply with the Cadbury/Hampel and Dey Reports respectively. Where a company does not comply, it must provide an explanation as to why not, though there is no requirement that a company must change its practices to bring it in line with the guidelines.

Similarly, CalPERS' Core Principles and Governance Guidelines acknowledge that they describe only one way of doing things, and may not be universally accepted:

> *"CalPERS believes the criteria contained in both the Principles and the Guidelines are important considerations for all companies within the US market. However, CalPERS does not expect nor seek that each company will adopt or embrace every aspect of either the Principles or Guidelines. CalPERS recognizes that some of these may not be appropriate for every company, due to differing developmental stages, ownership structure, competitive environment, or a myriad of other distinctions. CalPERS also recognizes that other approaches may equally—or perhaps even better—achieve the desired goal of a fully accountable governance structure."*[2]

Nonetheless, the codes have had a significant impact on business practice. Stakeholders (particularly regulators and institutional investors) are increasingly reluctant to sanction companies that cannot demonstrate their proficiency in corporate governance. Compliance with a code is one easy way for a company to win approval.

For example, the Toronto Stock Exchange Committee on Corporate Governance and the Institute of Corporate Directors conducted a survey of corporate practices five years after the adoption of the Dey Report

guidelines, and found that "a number of the TSE guidelines are now broadly accepted business practices."[3] In the UK, the Financial Reporting Council revealed that by 2011, "80 percent of FTSE 350 companies [had] already [adopted] annual re-election of all directors:" a mandate that was written as a part of the UK Governance Code only a year before the study, in 2010.[4] Hence, there is evidence to suggest that the recommendations presented by codes of conduct are being adopted by leading companies.

BEST PRACTICES

The various codes have a number of commonalities from which several best practices in corporate governance can be synthesized. Each code has a slightly different focus, and therefore makes slightly different recommendations for the board. We'll consider some of the activities and issues most frequently cited: stakeholder communication, board independence, performance assessment, and executive and director compensation.

Stakeholder Communication

Communication with company stakeholders[5] is one of the most important—and sensitive—responsibilities of the board of directors. While corporate governance codes of best practice concur that, in general, management should speak for the company, the board does have a key role in disclosing certain types of information.

One of the most important vehicles for disclosing key information to stakeholders is the corporate annual report. As discussed earlier in this chapter, the London Stock Exchange (LSE) and Toronto Stock Exchange (TSE) have each adopted the recommendations of the Cadbury, Hampel, and Dey Reports on corporate disclosure, and require that companies outline their corporate governance practices in each annual report.

This has significantly improved investors' access to information on the operations of the board of directors, which is considered a key benefit of improved corporate governance practices. The annual reports of both the Bank of Montreal and BP Amoco, for example, contain detailed disclosures about the companies' corporate governance practices. These disclosures make specific reference to the corporate governance requirements of the TSE and LSE, respectively, and rate the companies' performance relative to those guidelines. These disclosures can also be found on their corporate websites, which significantly improves investors' access to information on corporate governance efforts.

However, the Securities Exchange Act of 1934 was amended in 1978 to require the disclosure of "such additional details of corporate governance as structure, composition, and functioning of issuers' board of directors [and] resignation of directors in Proxy statements."[6] As a result, shareholders of General Motors, General Electric, Campbell Soup, and Compaq have access to detailed information on certain aspects of the corporate governance practices at each of these companies. Moreover, following the Sarbanes-Oxley Act, the NYSE and Nasdaq have adopted more explicit corporate governance requirements for listed companies.

Board Independence

One of the most important changes in corporate governance practice in recent years concerns the issue of board independence. Most of the codes highlighted in this chapter specifically recommend the independence of the board of directors from the corporation and its management. England's Cadbury Report in 1992 provided one of the first recommendations that the board consist of a majority of independent directors:

> *"Apart from their directors' fees and shareholdings, [directors] should be independent of management and free from any business or other relationship which could materially interfere with exercise of their independent judgment."*[7]

This independence is considered critical to ensuring that the board is objective enough to act in the best interests of the organization's stakeholders. Furthermore, independence is key in ensuring that the board is able to exercise its primary responsibility of oversight or stewardship of the company without being overly involved in its day-to-day management.

As a result of these guidelines, many organizations have taken steps to ensure that the majority of their directors are able to bring the objectivity and outside perspective considered crucial to good corporate governance. A majority of board members are independent at many companies highlighted as having excellent corporate-governance practices. For example, most of General Electric's board members are unrelated to the company. This is also true of Bank of Montreal, BP Amoco, and Campbell Soup. At Compaq, named *Board of the Year* in 1997 by the Wharton School of the University of Pennsylvania, all board members except for the CEO are outside directors.

Conversely, a lack of board independence is apparent in a number of the disaster stories. All the directors of Metallgesellschaft's U.S. subsidiary, for example, were internal and related, resulting in a lack of independence and consequent allegations of conflict of interest in decision making.

There has been much debate in recent years as to whether it is appropriate for a company's chief executive officer to also be the chair of its board of directors. The UK Corporate Governance Code of the UK's Committee on Corporate Governance summarizes the concern as follows:

> *"There should be a clear division of responsibilities at the head of the company between the running of the board and the executive responsibility for the running of the company's business. No one individual should have unfettered powers of decision."*[8]

Other codes concur. Most suggest that the decision to have one individual act as both CEO and board Chair should be taken carefully and publicly justified. In recognition of the fact that it is extremely common to combine these positions in one individual, each of the codes suggests the appointment of a "lead director" as an option. The role of a lead director is to act in an independent capacity to coordinate board activities with the corporation's CEO, and to coordinate the other independent directors.[9] This lead director also has overall responsibility for ensuring that the board "discharges its responsibilities" in cases where the CEO is also the Chair.[10]

BP Amoco and Compaq both require the positions of Chairman of the Board and CEO to be held by different people. At the Bank of Montreal and Campbell Soup, where the CEOs serve as board chairs, the board's independence is strengthened by the existence of a lead director. Furthermore, each of these boards meets at least annually *without* the CEO being present to discuss issues where board independence is particularly important.

The issue of board independence also has implications for the board's governance structure. Each of the codes in question specifies that certain key committees should be comprised only of independent directors, the compensation, audit, and nominating or governance committees being most frequently cited as those which should remain wholly independent.

In keeping with this sentiment, General Motors decreed in its Board Guidelines and in a corporate by law that its audit, capital stock, director affairs, executive, executive compensation, and public policy committees would each consist of "only independent directors."[11] The same holds true for most committees at General Electric, the Bank of Montreal, BP Amoco, Campbell Soup, and Compaq.

One other key area where board independence comes into play is in the selection of new board members. The Dey Report specifies that a committee of exclusively outside (independent) directors should perform this nomination and selection, and the National Association of Corporate Directors (NACD) report concurs. "Creating an independent and inclusive process

for nominating . . . directors . . . will ensure broad accountability to shareholders and reinforce perceptions of fairness and trust between and among management and board members."[12]

Board Performance Assessment

Another widespread recommendation is that boards of directors should periodically make a formal evaluation of their performance against best-practice guidelines. Canada's Dey report recommends that "every board of directors should implement a process . . . for assessing the effectiveness of the board as a whole, the committees of the board, and the contribution of individual directors."[13] The NACD Report goes into more detail of how the evaluation process should be made, specifying what criteria should be evaluated and how.[14]

The Dey recommendation proved one of the most challenging for companies in Canada to adopt. Five years later, fewer than 20 percent of Canadian listed companies surveyed have in place "any formal process for assessing board effectiveness."[15] Many companies found themselves to be unsure of how to conduct such an evaluation in an unbiased and objective fashion. Even by 2005, says David Beatty, managing director of Canadian Coalition for Good Governance, only around "100 of Canada's largest companies claim to do board evaluations and as few as 25—mostly financial or oil and gas companies—do individual assessments."[16]

Nonetheless, some companies with leading-edge governance practices do conduct regular board self-evaluations. The General Motors Guidelines, for example, specify that the governance committee should "[report] an assessment of the Board's performance annually to the Board."[17] Recognizing one of the sensitivities that have prevented some boards from adopting self-assessment processes, General Motors' Guideline 22 goes on to state that the purpose of the assessment is "to determine whether the individuals sitting on the Board bring the skills and expertise appropriate for the Company and how they work as a group."

The board of the Bank of Montreal annually assesses both the board as a whole and the individual directors. To do this, the Bank prepares a written statement of what was expected of its directors, using the recommendations of the NACD. Based on this statement of expectations, directors complete a detailed survey about the performance of their peers. The results are compiled by an outside consultant, which produces a performance scorecard measuring effectiveness and activity.[18] According to the firm's counsel, Blair MacAulay, "it wasn't easy to implement, but it has been highly successful."[19]

Executive and Board Compensation

The codes are more divided on the role that the Board should play in setting performance objectives and conducting a performance review of the CEO, although this has proved considerably easier for corporations to comply with. The NACD report recommends that boards "regularly and formally" evaluate the CEO, and specifies that independent directors should have control over this process.[20]

Here again, the General Motors Board Guidelines hold with best practice as identified by the other codes, and require all independent directors of their Board to review the CEO's performance annually, "based on both qualitative and quantitative factors, including but not limited to: (1) the Company's financial performance; (2) accomplishment of the Company's long-term strategic objectives; and (3) development of the Company's top management team."[21] At BP Amoco, the board actively assesses the performance of its CEO and executives. At Campbell Soup, "the Compensation and Organization Committee shall lead the Board at least annually in an evaluation of the performance of the CEO . . . in one or more meetings of non-management directors at which the CEO is not present."[22]

Director compensation is, for obvious reasons, an issue of such importance that it is overtly mentioned by each code reviewed here, and has been the sole focus of numerous other studies and reports.[23] The UK Corporate Governance Code recommends that "a company should avoid paying more than is necessary" to motivate directors.[24] The Dey report recognizes, however, that while directors should certainly not be overcompensated, the board of directors of each company should "ensure the compensation realistically reflects the responsibilities and risk involved in being an effective director."[25]

An important point agreed upon by all of the codes is that a significant portion of directors' compensation should be in the form of company stock, which helps to ensure that the directors' objectives are aligned with those of shareholders. As General Motors Guideline 19 points out: "it is important for each director to have a financial stake in the Company to help align the director's interests with those of the Company's stakeholders." Guideline 19 mandates that "each non-employee director is required to own beneficially Common Stock of the Company . . . with a market value of at least $300,000."[26]

At General Electric, non-management directors are required to hold at least $500,000 worth of stock. In 2006, 60 percent of annual compensation to non-management directors was awarded in the form of stock, with the transparent intention of aligning interests.[27] The Bank of Montreal's board reviews directors' compensation and benchmarks it against other Canadian and North American banks annually. Furthermore, the board has decreed

that "a minimum of $100,000 of their $175,000 annual retainer fee" must be paid in Bank stock. Directors even have an option to take 100 percent of their retainer and fees in stock—in 2012, 83 percent of total director compensation was taken in this way.[28]

LINKING CORPORATE GOVERNANCE AND ERM

As mentioned above, the focus on corporate governance in general has provided a great deal of impetus for changes in corporate risk management practices. Some of the codes of best practice on corporate governance explicitly cite risk management as a key responsibility of the board.

Specifically, both the Dey Report and the Organisation for Economic Cooperation and Development (OECD) Principles of Corporate Governance overtly mention that the board has a responsibility for ensuring that appropriate systems and policies for risk management are in place.[29] The follow-up study to the Dey Report, "Five Years to the Dey", found that by 1999, 61 percent of Canadian-listed companies' boards had some formal process in place for managing risk.[30] A 1998 study of hundreds of Canadian companies (both listed and private) by the Conference Board of Canada found that directors' assumption of responsibility for risk management had increased 13 percent in the two years after the 1995 Dey Report went into effect.[31] Today, more than 60 Canadian companies participate on the Strategic Risk Council, which aims to bring together top-level management executives and help them "develop, implement, and sustain enterprise-wide risk management process."[32] The growth in the Council's numbers is a strong testament to the greater prominence that the Dey Report brought to risk management.

Another important link between corporate governance and enterprise risk management is that both have similar focuses on strategic direction, corporate integration, and motivation from the top of the organization. The ultimate aim of both corporate governance and ERM is to prevent such debacles as Metallgesellschaft and Barings. Not only was poor risk management to blame for the scandals that threatened these two organizations, so was ineffective corporate governance. Companies with poor corporate governance practices often have poor risk management skills, and vice versa.

Quite apart from anything else, good board practices and corporate governance are crucial for effective ERM. The development and success of ERM can be greatly enhanced with the commitment and involvement of the board of directors. In a strong company, the board is a single, independent body with an integrated perspective of the company's operations—the

ideal entity to put weight behind an ERM initiative. There are a number of aspects of ERM that are very closely allied to the work of the board: setting risk appetite and policy; determining organizational structure; and establishing corporate culture and values. As we will discuss in the Export Development Corporation case study in Chapter 12, the involvement of the board was a key success factor in their ERM program.

Risk Appetite and Policy

One of the early and tangible deliverables of an ERM initiative is the corporate risk policy—a statement of the corporation's overall approach to risk management including risk philosophy and principles, roles and responsibilities, risk tolerance levels, and reporting and monitoring processes. A risk policy is best formulated at the corporate management level with input from the business units, and approved by the board. It is essential that the risk policy documents the organization's risk appetite and clearly defines its risk tolerances in terms of limits. By codifying the overall structure for risk management and the organization's risk appetite, a risk policy helps communicate risk management standards and expectations throughout the organization.

A risk appetite statement is a mutual understanding between the executive management and the board of directors with regard to what risk levels are acceptable, considering the enterprise's strategy in maximizing value. Each organization establishes various business objectives in order to add value; the board and management should have a clear and common understanding of the risks that the organization is willing to accept. To fully integrate the risk appetite statement into the business operations and processes in the organization, the risk limits and tolerance levels established at the enterprise level (e.g., aggregate risk tolerances with respect to stressed losses, capital-at-risk, earnings-at-risk, cashflow-at-risk, target credit ratings) must be translated into risk limits and tolerance levels at the business and operating levels (e.g., business risk tolerances, operational risk tolerances, interest rate risk limits, market risk limits, and credit and counterparty risk limits).

An organization must consider its risk appetite at the same time it decides which business strategies and goals to pursue. Questions that should be addressed when developing or revising risk appetite statements include:

- What is the organization's overall strategy to maximize value, and the underlying business, financial, and operational objectives?
- What are the risk/return tradeoffs that the board and management should evaluate in determining the appropriate risk limits and tolerances?

- Are there any business, regulatory, or risk events that should trigger a review (and possible revision) of the risk appetite statement between revision dates?
- What risks and risk exposure levels are acceptable to the board, corporate management, and the business units?
- With respect to risk methodologies and metrics, how would the risk tolerances at the enterprise level map to the risk tolerances at the business and operating unit levels?
- How would risk exposures that exceed the risk limits and tolerances be handled with respect to risk escalations and exception management?
- What are the risk reports that should be provided to the board, corporate management, and business and operating unit management to monitor performance against the risk appetite statement?

The application of a risk appetite statement in the context of ERM naturally varies considerably from organization to organization. One good example of how the risk appetite statement supports ERM can be found in the Annual Report[33] of JP Morgan Chase:[34]

> *Risk is an inherent part of JPMorgan Chase's business activities. The Firm's risk management framework and governance structure are intended to provide comprehensive controls and ongoing management of the major risks inherent in its business activities. The Firm employs a holistic approach to risk management to ensure the broad spectrum of risk types are considered in managing its business activities. The Firm's risk management framework is intended to create a culture of risk awareness and personal responsibility throughout the Firm where collaboration, discussion, escalation and sharing of information is encouraged.*
>
> *The Firm's overall risk appetite is established in the context of the Firm's capital, earnings power, and diversified business model. The Firm employs a formalized risk appetite framework to clearly link risk appetite and return targets, controls and capital management. The Firm's CEO is responsible for setting the overall risk appetite of the Firm and the LOB [line of business] CEOs are responsible for setting the risk appetite for their respective lines of business. The Risk Policy Committee of the Firm's Board of Directors approves the risk appetite policy on behalf of the entire Board of Directors.*

Organizational Structure

No risk management effort can be truly successful unless it is aligned effectively with the organizational structure.

Ideally, the responsibility for implementing an enterprise risk management program should rest with an independent risk management function that reports directly to the CEO and/or board (through the CRO, if one has been appointed). This independence ensures that the risk management function is as unbiased and objective as possible, and the reporting relationship ensures that the risk management office has sufficient power within the organization to motivate good risk management practices.

The CRO, or nearest equivalent, should in turn report to a risk management committee of the Board. As discussed previously, the Board's direct involvement will ensure that the risk management program is executed with an integrated, holistic view of the organization in mind.

We previously discussed the importance of aligning employee incentives with good risk management practice. This alignment should begin at the executive level, which is where a risk-aware Board comes into play. The compensation and incentives of the Board, the CEO and other executives should clearly be in line with the company's risk management policy and appetite.

This does not mean going all-out for growth: a company should reward earnings stability to the extent that this fits its risk appetite. For example, CompuTrac decided in 1998 to restructure its CEO's compensation significantly, reducing his base salary by $230,000 over two years and lowering the strike price of his stock options to reflect its risk appetite and operations.[35] Similar logic should be applied in setting compensation for employees throughout the company.

Risk Culture and Corporate Values

One of the softest, but most important aspects of risk management is the integration of risk into a company's culture and values. Most obviously, risk needs be considered an integral part of corporate strategy. Risk management targets should be included among corporate goals, and major corporate initiatives should incorporate risk assessment and risk mitigation strategies.

Unfortunately, integration is also one of the most difficult aspects of risk management to implement: a 2008 study by McKinsey & Company demonstrates that only 39 percent of surveyed directors recognized "ERM as a core strategic function," while as many as a third saw the frameworks of ERM as only low value-added activities.[36] This speaks to the wide disparities in the opinions of directors as to the true importance of ERM.

Just as an organization's overall culture can be critical in determining how successful it will be, so will its risk culture determine the success of its ERM. A weak risk culture is one in which employees have little sense of the importance of risk management and their role in it. Such a culture will

compromise efforts to manage risk—perhaps fatally. If, on the other hand, risk management is seen as a central part of day-to-day operations, it is likely that a strong risk culture is in place. Such an environment allows for truly effective risk management. In order to measure and monitor their risk culture, a growing number of companies are performing annual risk culture surveys that are designed to show how employee behavior compares to desired behavior. These surveys track to what degree are employees assessing, communicating, and mitigating risks in a manner consistent with the company's risk management policies and standards.

Like all cultural issues, a key factor is whether management walks the walk as well as it talks the talk. For example, how does senior management react when a high-revenue producer blatantly violates risk management policies? Do they take corrective action or simply turn their backs to the problem? The decisions and actions of senior management will do more to influence behavior than any written policy. It's critical that they act accordingly.

CHAPTER 6

Line Management

The key revenue-producing activities of a business enterprise are usually organized into strategic business units by geography, customer group, product, or some combination of all these. These business units account for the vast majority of assets and employees in most organizations, and can also be the primary source of business, financial, and operational risks. Those responsible for these units, and their risks, are the *line management*.

Line managers face a wide variety of risks. Most common are those associated with day-to-day operations, such as defects in supplies of components or raw materials, or errors, failures, and wastage in production processes. In addition, line managers will face periodic risks associated with strategic business decisions, including new product launches, potential mergers and acquisitions, and changes to incentive packages. Finally, they also face catastrophic risks from once-in-a-lifetime calamities—natural disasters like fires or earthquakes, as well as extraordinary litigation.

Much has been written on the management of each of these kinds of risk, although sometimes only under the rubrics of quality management, general business management and continuity and crisis management rather than risk management.

In this chapter, we will concentrate on the interaction of the line managers and the enterprise risk management function.

As the origination point for many of the risks faced by a company, line management plays a key role in enterprise risk management. Since the line units have the closest contacts with customers and suppliers, their success in addressing risk issues will not only have a material effect on mitigating potential losses, but also on the reputation of the company as a whole. It is therefore critical for line managers pursuing new business and growth opportunities to align their business strategies with the overall corporate risk policy.

This means that the risks of business transactions should be fully assessed and incorporated into pricing and profitability targets. Specifically,

expected losses and the cost of risk capital should be included in the pricing of a product or the required return on an investment project. In business development, risk acceptance criteria should be established to ensure that risk management issues are considered as part of the assessment of new product and market opportunities.

In this chapter, we'll discuss these and other risk issues in greater detail:

- The relationship between line units and risk management;
- Key challenges for line risk management;
- Best practices for line risk management.

THE RELATIONSHIP BETWEEN LINE AND RISK FUNCTIONS

The relationship between line management and risk management is a key driver of the overall business and risk culture of a company. The challenge for any company is to establish an independent risk function without creating an adversarial relationship between the line and risk units. A healthy bond between the two is required for any enterprise risk management program to be successful.

As CRO of Fidelity Investments, I worked very hard to gain and maintain the trust and support of the business units.[1] My approach was to listen to their needs and requirements, provide them with regular updates on the ERM plan, engage them to discuss best practices and lessons learned, and, most importantly, to integrate risk practices into line management to help them achieve their business objectives. Other successful CROs have also built very strong relationships with the business units in their companies. For example, the CRO at CIBC (see Chapter 16) helped business units understand their own risk/return trade-offs and subsequently make better business decisions.

The relationship between line management and risk management can be characterized in terms of three organizational models:

1. **Offense versus defense:** In this model, business units are focused on revenue maximization and risk management is focused on loss minimization;
2. **Policy and policing:** Business units can only operate within the risk policies established by risk management, and their activities are monitored by risk, audit, and compliance functions; and
3. **Partnership:** Business units and risk management jointly evaluate and resolve risk management issues and share common goals and objectives.

These organizational models are by no means mutually exclusive. For example, a company can adopt the partnership model for day-to-day

business activities, but use the policy and policing model for highly sensitive issues (e.g., information security, sexual harassment). However, it is useful to discuss the implications of these approaches to highlight how they may impact business behavior and shape the risk culture of a company.

Offense and Defense

During my early years in risk management, I often heard risk professionals—and credit managers in particular—describe the line units as offense and risk management as defense. I always found this description unproductive. In sports, where this analogy no doubt originated, one team wins while the other loses; the two teams have opposite goals, and in many respects are at war with each other. Some cynics might say this is a pretty accurate depiction of line management versus risk management, though I would argue instead that it represents an unhealthy risk culture.

In the early 1990s, I worked as a consultant for one U.S. regional bank where the chief credit officer was fond of using the offense and defense analogy to describe the loan origination and credit departments. At that bank, the performances of the loan-origination units were measured on the basis of number and size of loans funded, loan fee income, and total size of the loan portfolio. Meanwhile, the performance of the credit department was measured by loan defaults, losses, and the overall credit quality of the loan portfolio. As a result, the loan origination units were better off if a loan was approved and the credit department was better off if it was declined, regardless of the risk/return economics of the loan. Given that the credit department or credit committee had to approve all loans above a certain size, these opposing objectives created a destructive business environment.

For example, the loan origination units would understate the credit risk of loans in order to get them approved, with the result that many loans were downgraded or went into default shortly after origination. They would also present loan proposals at the last minute, hoping that they would pass with little scrutiny. Meanwhile, the credit department was skeptical of the credit analysis performed by the origination units and would ask for more information and documentation. It would require a dozen or more signatures for large or complex loans in order to slow down the approval process and prevent last-minute proposals.

This circle of behavior became increasingly vicious, and the risk culture of this bank became increasingly dysfunctional over time. The credit managers called the loan originators cowboys, while the loan originators called the credit managers Dr. No's. Performance deteriorated markedly and the bank ultimately lost its independence when it was acquired by another bank.

This example illustrates the potential pitfalls of an offense versus defense model. When line and risk functions are given opposing objectives—and particularly when they are given opposing incentives—the result is almost inevitably adverse, and ultimately very detrimental to the business performance of a company. This problem is not unique to risk management; it can occur in relationships between line management and *any* control-oriented functions such as audit, finance, quality, legal, compliance, and so on.

Policy and Policing

In the policy and policing model often used by large, decentralized companies, the risk management function establishes policies and limits within which the line units must operate. These serve as the boundaries for line operations—they might consist of approved transactions, minimum credit standards, exposure limits, investment policies, and so on. Line operations within these policies and limits require no special approvals or reviews, while those outside them are approved or denied on a case-by-case basis. The risk management unit, along with the audit and compliance units, checks that these policies and limits are followed and reports exceptions and excesses to senior management.

Unlike the offense versus defense model, where the relationship between line and risk functions is strictly adversarial, the relationship under the policy and policing model is more like one of government and citizenry. Risk management serves as a lawmaker (and sometimes as law enforcement): the line functions have full operating autonomy as long as they don't violate any risk management policies. New situations are judged individually and their resolutions become part of the policy. This model is similar to the way that individuals and institutions are regulated in a common-law democratic society: they are free to act as they wish, so long as they remain within the law; punishments for law-breaking are partially based on circumstances; and the detailed interpretation of the law is established by precedent.

There are a number of problems with this model, however. The risk management function is not engaged in the day-to-day operations of line management and as a result may lose touch with the changing business environment. Over time, existing risk management policies may become outdated and new policies may not be established in a timely manner. In addition, audit and compliance processes are episodic and may not fully identify critical issues. Significant risk events can occur between examination periods no matter how good the audit and compliance functions may be.

The result is that there is likely to be a disconnect between the line and risk management. Typically, line units will complain that they are sometimes blindsided by ill-conceived risk policies, and that risk management doesn't

understand the market or their business. In contrast, risk management might say that they get blindsided by the line units' actions and decisions, and that the line units don't fully understand the risk management policies.

What makes this situation worse is that line management is biased against communicating problems to the risk management unit. Consider the analogy of government and citizenry. Those who break the law, whether deliberately or inadvertently, do not usually seek out the police to make a confession; this is even more true if it is unclear that a law has actually been broken. Citizens are only likely to admit to breaking the law if they believe it is possible that the law will be changed in such a way that it benefits them—or if they have a guilty conscience, in which case it is likely that the damage is already done.

Similarly, line units do not have strong incentives to report deliberate or accidental out-and-out policy violations, or to seek the advice of the risk management unit when it is not clear if a policy is being infringed. To put it another way, the line units may respect the letter of the law—although if they do not, the risk management unit may not find out in a prompt fashion—but they are unlikely to respect its spirit. Risk management will likely only hear about potential problems when the situation is too dire to be ignored, or when line management thinks the problem can be turned into an opportunity by a revision of policy.

Clearly, this is a caricatured picture of how the policy-and-policing model works. Arguments based on the greater good of the company carry some weight, as do incentives tied to policy compliance and well-judged punitive measures against violators. While risk management is no longer in opposition to line management, it is still passive much of the time, acting mostly as a check of line activities. A better alternative is for risk management to take a proactive stance in helping the line units to make their businesses work. As we'll see in the next section, this partnership approach can be a powerful one for all concerned.

Partnership Model

In the partnership model, risk management is fully integrated into the business, as opposed to being a corporate oversight function. Line and risk management personnel work together to address risk/return issues not only when problems arise, but also in the front end of the business process when products are being developed and when pricing or investment decisions are being made. The relationship between line and risk functions becomes more like that of a client and consultant, where the line units seek to use risk management expertise to improve business performance. In this environment, the line and risk functions have individual performance targets, but also

some important shared performance measures, such as risk-adjusted profitability and portfolio quality. Given their shared performance objectives, line and risk units have incentives to work together to address risk management issues in the front-end business processes, and to respond to problems when they emerge.

The fundamental keys to making this model work are cultural and organizational. First, line management must recognize the role that risk management plays in supporting long-term performance and stop obsessing over its role in constraining short-term profitability. Second, the risk management unit must recognize the need to understand and respond to the line units' business needs, and resist handing down academic, impractical, and inflexible policies.

The first item can be dealt with by getting line management to recognize that risk and return are both inevitable parts of any business decision. Hence, it is a good idea to have someone who understands risk on-hand to provide advice and guidance when undertaking a new activity. Rather than applying risk management tools because they have to, the line unit clients should apply them because they want to; they should see the risk management unit as a value-added business partner that can help them to understand the underlying risk/return economics of their business, keep them out of trouble, and help them to achieve their business and financial objectives.

The second item should be dealt with by making sure that risk management sees itself as a consultant in a client-consultant relationship. That means it should be responsive to the needs of the business units and develop tools that can support business decisions, such as risk-based pricing models and scenario planning instruments. As such, the risk management function cannot live in an Ivy Tower, but must be decentralized in the business units. This can be accomplished by establishing risk management functions *within* the line units. Depending on the particular organization, this might be done by putting staff in each business unit in various geographical locations or other parts of the organizational structure that serves the operational needs of the business.

The main problem with the partnership model relates to the independence of the risk management function. As a business partner who participates in business decisions and problem resolutions, can risk management maintain its important role as a corporate oversight function? This is a similar challenge to the one faced by the Big Four accounting firms, whose independence as auditors has, in recent years, been brought into question by the growth and profitability of their consulting practices.

A likely resolution for the accounting firms is the divestment of the consulting practices into separate businesses—although this is not really an

option for a partnership risk management unit within a company. One answer is to mix up the models discussed in this section. As discussed earlier, the three models for line-risk relationship are not mutually exclusive. Many companies have blended the partnership and policy-and-policing models in order to maintain the independence of the risk management function. This hybrid approach establishes risk units with distinct but complimentary mandates.

For example, such companies have established operational risk consulting units to serve as business partners, but have maintained their audit function to maintain independence. Another example is the credit function at many commercial banks, where the origination versus credit approval model is replaced by a relationship management team that is fully responsible for sales and credit analysis, but a separate and independent credit review function is established to ensure compliance with credit policies.

KEY CHALLENGES

In aligning risk and line management, there are a number of key challenges that emerge from conversations with risk managers on both the line and risk sides of organizations:

- Conflict resolution between line and staff;
- The role of line risk management;
- Incentive alignment; and
- Non-financial risk measurement.

Conflict Resolution

The issue most often cited in conversations with risk managers is the adversarial nature of the relationship between line business managers and staff risk managers. While the three organizational models discussed above highlight ways to minimize potential conflict, there will inevitably be day-to-day tensions that need to be addressed. Usually, there is a straightforward, more or less open conflict between line business managers and staff risk managers. The form of the conflict most often concerns choices between business volume or revenue growth and risk control. At its most basic level, this is the conflict between perceptions of risk as opportunity for profit and risk as opportunity for loss.

This is a classic problem for businesses offering financial services, such as those that perform lending or insurance functions: as the business cycle

picks up and perceptions of risk start to fall, the supply of capital for lending and insurance products starts to increase faster than the demand for those products. As a result, a provider's business growth will suffer. In most of these cases, line managers will argue for lower pricing or relaxed underwriting standards in order to increase volume, whereas staff managers will argue for maintaining the same standards and keeping losses within planned levels.

Similar conflicts occur outside the financial industry. For example, line units may on occasion be required by a staff department to add additional product features; for example, to minimize environmental damage and hence reduce catastrophic legal risk. More generally, sales people will argue for marginal cost pricing to increase or maintain volume while finance will argue for full-cost pricing in order to increase or maintain profitability.

In these situations, there is the sense of an arms race between the staff functions and the line business units. In this process, the line seeks ways to avoid oversight by staff units, while the staff functions strive to unearth information on the line managers' activities so that they can be kept in check. Budgetary processes are often the focus of this game playing. This conflict tends to ebb and flow with the business cycle. In expansionary times, business development takes priority; in recessions, control is paramount. In light of this apparently inevitable conflict, the issue is usually framed as constructive conflict management rather than reconciliation, with a focus on structures and processes.

Line Risk Management

One response to the perception of unavoidable conflict has been for business units to install risk managers within their business units with increasing frequency—a parallel development, in some ways, to the trend for appointing CROs at the corporate level.

The appointment of a line risk manager gives strength to the partnership model described above: he or she can help the business unit to understand its risks in a way to ensure compliance with the consistent standards laid down by the ERM function. It works: while at Fidelity, I noticed that the quality of risk management at each of the company's 40 business units was directly correlated with whether that business unit had a dedicated risk manager.

In early models, the line risk manager reported jointly to the CRO and to the business manager. While this is perhaps the truest reflection of that person's role in the company, it is, in practice, highly ambiguous, which can create an uncomfortable atmosphere. The rest of the line staff may perceive

the line risk manager as part of the enemy while the ERM staff remains convinced that he is, at best, a double-agent working both sides to his own advantage! No wonder line risk managers often feel that they are walking a tightrope.

One solution is to have the line risk manager report to the head of the business unit and have a dotted line link to the CRO. This would make the business manager the line risk manager's boss, while ensuring that he or she must also keep the CRO in the loop—this helps to reduce some of the ambiguity described above. For some companies, the reverse structure will make more sense. Either way, the CRO should always provide a meaningful input in the performance review and incentive compensation of line risk managers, especially in the early stages of an ERM program.

Another increasingly common industry practice is the creation of communities of risk that cut across hierarchical levels and business units. These have been created in response to the perception that risk expertise and know-how are usually scarce in any given organization, but similar problems and opportunities are common. Successful organizations have built on these new positions and communities, changing their processes so that the individuals involved can operate effectively.

Incentive Alignment

It is clear that, in many cases, the adversarial nature of the debate stems directly from misaligned incentives. One side is seeking growth; the other is seeking quality. A notable part of the equation is line manager incentive structures that reward them based on a combination of business metrics, such as volume, revenue, profit, and return on equity. The other part of the equation is the structures in place for staff managers, which typically focus on minimization of losses, errors, or deviations from plan, with qualitative or subjective measures of performance (e.g., timely reporting, roll out of a system, enhancements to methodologies) layered on top.

In theory, perfect incentive structures could be designed so that both parties are facing the same objective function and, consequently, will act synchronously. However, in practice, it is difficult to design and implement the metrics required given the difficulty in measuring—or even obtaining solid data about—certain aspects of performance. In this area, most effort is being put into balanced scorecard initiatives, with some secondary emphasis on risk-adjusted performance measures. As such, the performance measurement and incentive systems are designed to incorporate corporate-wide performance metrics, as well as unit-specific metrics and non-quantitative criteria.

Nonfinancial Risk Measurement

A related, emerging issue is how to assess and quantify non-financial risks (business, organizational, and operational risks) and how to incorporate these measures into performance-measurement systems. As noted above, many management techniques that have risk measurement and management applications are found in other disciplines.

For example, many types of operational risk in primary industries and manufacturing have been addressed through total quality management (TQM) initiatives and business continuity planning. However, there is still plenty of debate outside manufacturing about how to define, let alone measure and control, operational risks, such as a poor service experience, a power outage, or an inadequately specified contract. The topic of operational risk management has been the subject of increasing attention in the risk management community (see Chapter 14 for more discussion on operational risk management).

BEST PRACTICES

As noted above, the relationship between line management and risk management is a critical factor to the success of any ERM program. To establish a healthy relationship, a balance must be maintained between effective corporate oversight and efficient line decisions. In order to achieve and maintain such a balance, the ERM program should strive to integrate risk management into business-management processes, including:

- Business strategy and planning
- New product and business development
- Product pricing
- Business performance measurement
- Risk and incentive compensation

Strategy and Planning

The business strategies and plans submitted by business units should include a full discussion of the risks involved, as well as the appropriate risk mitigation strategies. The business units should address six basic questions:

1. Which risk factors could prevent us from achieving our key business objectives?
2. How will we measure and track these risk factors?

3. How will we mitigate these risks through internal processes or external risk transfer?
4. What level or range of risk/return performance should corporate management expect?
5. What risk limits and tolerance levels should we recommend to corporate management and the board?
6. Who is responsible for measuring and managing the risks involved?

A company will obtain a number of benefits by ensuring that business unit strategies and plans address these questions. First, it focuses business units' attention on the key risk exposures in their operations, as well as on the necessary measurement and management strategies for containing these risks. A business unit that is unprepared to discuss its risks or its risk mitigation strategies should be an area of concern.

Second, it provides corporate management with timely and forward-looking information on the company's emerging risk exposures. For example, if many business units are planning to expand their businesses in Japan, then the treasury unit should plan on increasing its dollar/yen-hedging program. Third, it facilitates early discussions between line management and risk management to ensure that business and risk issues are identified and resolved. Risk management can be more proactive in developing and implementing risk policies given business changes, and can use the experience gained to develop best practices across more business units. This way, useful approaches can be shared within the company and can also help ensure that a mistake made by one business will not be repeated in another.

Fourth, the linkage between business strategy and ERM would support the development of risk limits and tolerances that the business units can recommend to corporate management and the board. These risk limits and tolerances should be linked to the corporation's statement of risk appetite. Finally, the integration of strategy and risk would enhance board and management reporting by tying together business objectives, key performance indicators (KPIs), risk-control self assessment, and key risk indicators (KRIs). Figure 6.1 provides an overall view of this process.

Product and Business Development

In addition to business planning, risk management should be a part of the development of new product and business opportunities. These opportunities should include new products, business and financial investments, market expansion plans, and mergers and acquisitions. When management pursues any of these business opportunities, it relies on a set of assumptions for the business, such as volume, price, costs, and technology. There are risks

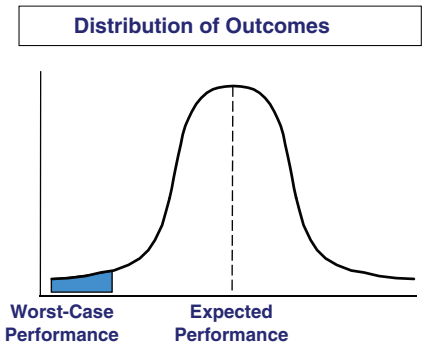


FIGURE 6.1 Integrating Strategy and ERM

associated with each of these assumptions. For example, actual volumes might fall below expectations, losses might exceed forecasts, and technology might not meet user expectations. It is important, therefore, to address these risk issues not only when the business opportunity is first considered, but also during regular business review sessions.

One of the best practices that I have seen first hand for integrating risk management with new product and business development was a business review process called Policy 6.0 at GE Capital. When a new business or investment is considered, the business unit must address all of the key business and risk management assumptions underlying the business opportunity. The business unit must discuss its expectations for each of these key assumptions. One particularly useful exercise was to set trigger points—the levels above and below expectations (i.e., plus and minus 10 percent) at which specific decisions or action plans are activated—or triggered. Individuals are then assigned to monitor and review business performance against these trigger points. If a business opportunity is not meeting expectations, the negative trigger points might initiate a plan to scale back the business, or even to exit altogether. If a business opportunity is achieving results that are above expectations, the positive trigger points might increase the company's investments and speed up the business-development timetable.

In order to assess the risks associated with new product and business development, many companies have established a risk committee (including

cross functional representatives from risk, legal, compliance, HR, IT, audit, etc.) that is responsible for reviewing and approving any new product or business prior to consideration by the executive committee or the board. This review process includes the introduction of a new or existing product into a foreign market. For a company that is expanding into a foreign market, understanding local business, compliance, and cultural issues is of the utmost importance. Global companies have made costly errors when selling their products in a foreign market. For example, it was discovered in a 2005 audit that Avon had paid bribes to officials in China while promoting their new products.[2] There have long been issues regarding Foreign Corrupt Practices Act (FCPA) compliance when it comes to business between the United States and China. Common business practices in China, such as treating officials to lavish dinners and other forms of entertainment, are not accepted in the United States under FCPA. The settlements and fines that Avon must pay for these violations have not been finalized, but the damage to the company's reputation has already been very significant. As another example, Mercedes Daimler AG had made more than $56 million in bribery payments to officials in 22 countries between 1998 and 2008 in order to obtain the necessary contracts for their vehicles. The company agreed to pay $185 million to settle these charges.[3]

Product Pricing

We discussed earlier how the pricing of a product or service should include the total cost of the risks associated with that product or service. More generally, the pricing of products developed and sold at the line level need to reflect the group-wide costs of risk that will otherwise go unrecovered. A company can only recover the costs incurred in managing risk by incorporating those costs into its product pricing. While many companies have established product-pricing models that incorporate operating costs and profitability targets, they often fail to fully consider the cost of risk.

The total cost of risk would include expected losses (from defects, errors, credit losses, etc.), the cost of economic capital (to absorb unexpected loss), the cost of risk transfer (insurance premiums and hedging costs), and the cost of risk management (risk professionals and systems). Without incorporating the cost of risk, companies will under-price their products and not get compensated for the risk exposures taken. Moreover, if a company is not using risk-based pricing and its competitors are, then it is subject to adverse selection, which results in a money-losing portfolio. For example, if an auto insurance company is under-pricing high-risk drivers and over-pricing low-risk drivers, then it will systematically get a portfolio over-weighted by high risk drivers but without the higher premium income to absorb the resulting higher losses.

The lack of risk-adjusted product pricing can also motivate adverse business behavior. For example, a bank would motivate business units to take interest rate risk if it does not incorporate the full cost of matched funding in its product pricing. With an upward sloping yield curve (where long-term interest rates are higher than short-term interest rates), a business unit can show higher profitability by funding long-term assets—say 30-year loans with short-term liabilities, or six-month deposits. However, note that such a strategy would expose the bank's earnings to rising rates and an inverted yield curve. This is what nearly bankrupted the U.S. thrift industry in the early 1980s.

Business Performance Measurement

The performance measures and goals for business units should include risk. Ideally, risk measurement and reporting should be integrated into overall business reporting. Given that a company takes risks to generate growth and profits, it only makes sense to include risk in the measurement of business performance. Having separate risk and business reports is equivalent to having separate revenue and expense reports. Just as management can only assess profitability by combining revenues and expenses, it can only balance risk exposures and business opportunities by integrating risk and business reporting.

Beginning in the mid 1990s, many companies have adopted the balanced scorecard as a way to integrate business and financial reporting for senior management. The traditional balanced scorecard defines business performance in terms of four categories: financial, customer, internal, and learning and growth. A good case can be made that the balanced scorecard (or any other business-reporting methodology) should include risk assessments. Only then will the balanced scorecard be truly balanced, with respect to the information needed by both the board and management. In the aftermath of the 2008 global financial crisis, balanced-scorecard practitioners have begun to recognize the need to fill this critical gap. Based on this acknowledgement, Robert Kaplan, the co-inventor of the balanced scorecard, conducted research and wrote extensively to augment the balanced scorecard with consideration of risk assessments.

Risk and Incentive Compensation

Beyond performance measurement, regulators and executives have realized the importance of aligning risk management and incentive compensation.

In 2009, the Securities and Exchange Commission (SEC) approved rules to enhance the information provided to shareholders so they are better able to evaluate the governance and risk management of public companies.[4] The SEC established these new rules to improve public disclosures regarding

risk and incentive compensation: "Good corporate governance is a system in which those who manage a company—that is, officers and directors—are effectively held accountable for their decisions and performance. But accountability is impossible without transparency," said SEC Chairman Mary L. Schapiro. "By adopting these rules, we will improve the disclosure around risk, compensation, and corporate governance, thereby increasing accountability and directly benefiting investors."

The 2009 SEC rule stated that, "In particular, the new rules require disclosures in proxy and information statements about:

- The relationship of a company's compensation policies and practices to risk management.
- The background and qualifications of directors and nominees.
- Legal actions involving a company's executive officers, directors, and nominees.
- The consideration of diversity in the process by which candidates for director are considered for nomination.
- Board leadership structure and the board's role in risk oversight.
- Stock and option awards to company executives and directors.
- Potential conflicts of interests of compensation consultants."

In 2011, the SEC further developed the above rule with respect to financial institutions. The SEC's proposed rules for financial institutions would:

- "Require reports related to incentive-based compensation that they would file annually with SEC.
- Prohibit incentive-based compensation arrangements that encourage inappropriate risk-taking by providing excessive compensation or that could lead to material financial loss to the firm.
- Provide additional requirements for financial institutions with $50 billion or more in assets, including deferral of incentive-based compensation of executive officers and approval of compensation for people whose job functions give them the ability to expose the firm to a substantial amount of risk.
- Require them to develop policies and procedures that ensure and monitor compliance with requirements related to incentive-based compensation."

As a result of this new rule, clawback provisions have become more prevalent at financial institutions. Some clawback policies look beyond the activities of an employee to include the responsible supervisor. For example, Goldman Sachs and Morgan Stanley have established policies regarding situations in which they are able to recover compensation from risk-taking

traders and their bosses. Both firms stated that managers could face clawbacks if their subordinates take excessive risk or exercise other misconduct.

Experts say that clawback provisions are becoming increasingly popular and are encompassing a wider scope of events and different types of compensation: "the number of Fortune 100 companies with publicly disclosed clawback policies grew from roughly 18 percent in 2006 to just over 84 percent last year."[5] Some feel that this is a sign of progress and increased accountability in the corporate world.

CHAPTER 7

Portfolio Management

It took seven years to persuade super-investor Warren Buffett to be the subject of *Nightline*, the ABC network's flagship news program. At that time, Buffett's Berkshire Hathaway investment vehicle had posted a succession of returns that put its competitors to shame; Buffett himself was known as "the sage of Omaha" and regarded by many as the world's shrewdest investor. To kick off the interview, the host, Ted Koppel, asked Buffett what he did for a living. Buffet reflected for a second and replied: "I allocate capital."

That short answer from one of the greatest investors of our times encapsulates an important lesson for all business managers. Capital allocation is a critical concept for *all* businesses: not just money managers, but also for other financial institutions, energy firms, and non-financial corporations. Capital is the link between risk and return; hence, a sound capital-allocation process is critical to business development and the creation of shareholder value.

Capital is typically allocated by evaluating a set of investment opportunities, then selecting those that meet a set of predetermined investment objectives. Over time, the investments aggregate into portfolios—a research and development portfolio, a securities portfolio, an asset/liability portfolio, and so on. In essence, a company should be viewed as a portfolio of businesses, each with its own unique risk/return characteristics.

In most enterprises, the various business portfolios have historically been managed by separate entities, which rarely coordinate their investment objectives with one another. This fragmentation implies that the enterprise-wide portfolio is unlikely to be optimized. How, then, should we manage the sets of existing investments and investment opportunities in order to optimize the aggregation of portfolios across the entire enterprise?

Since the ultimate goal of management is to maximize shareholder value, the over-arching principle for enterprise-wide portfolio management should be to manage the business portfolio in the same way that a fund manager manages a stock portfolio. In other words, business portfolio managers should strive to understand the links between risk origination

(e.g., business lines and trading units) and risk transfer (hedging and insurance) and make investment decisions that position the overall enterprise portfolio at the classic *efficient frontier* of risk/return—the highest return for the same level of risk or the lowest risk for the same level of return.

This process, as applied to money management, is widely known as *active portfolio management*, or simply *active management*. Generally, active managers implement a strategy or system designed to exploit mispricing or to manage risk. The alternative is to use a passive strategy, such as investing in a market index, or to make an alternative investment that requires minimum maintenance. Although both techniques have their merits when it comes to capital market investments, only active portfolio management theory is particularly relevant in evaluating capital-allocation decisions for a business.

THE THEORY OF ACTIVE PORTFOLIO MANAGEMENT

The theory of active portfolio management largely builds on the foundation established by Harry Markowitz in the 1950s, revolving around the measurement and management of risk.[1] As Markowitz himself said in a January 2000 interview: "Risk has been the same since the caveman. Modern portfolio theory has developed apparatus for risk evaluation and control. This apparatus, subject to further enhancement, will carry forward into the risk world of the future."[2]

The area in which the portfolio theory has been most enhanced is money management, where there is now a large body of theoretical work and empirical research. This is in part because return, volatility, and correlation information tends to be easier to quantify, and so it is more straightforward to construct sophisticated, technical models for portfolio management.

It is not as easy to do the same for business enterprises, but the precepts of active portfolio management can nonetheless prove useful, and the interested reader should investigate further on the subject. We'll confine ourselves here to discussing how even a basic understanding of the theory can have marked benefits for businesses.

Let's begin by considering the fundamental concepts suggested by the portfolio theory of Markowitz and his successors: risk, reward, diversification, leverage, and hedging.

Risk, in this context, is typically equated with volatility, a statistical measure of the uncertainty associated with future events. Risk is therefore indeterminate by definition (since we do not know what will happen in the future), but we can estimate the *likely* future value of a business or investment, with some range of variation around the value. In the stock market,

this is done by looking at the standard deviation of past returns, or by extracting the market's current expectations of risk from the prices of stock options.

The opposite side of the coin to risk is reward, or the gain that stands to be made from a risky investment. Like risk, the reward on an investment is indeterminate, but can be estimated in terms of its likely, or expected value. For example, the reward for investing in equity is the expected return of the stock or index over a given interval. More generally, an enterprise's reward for a new business venture is the gain that an organization stands to make by taking on a particular risk. Clearly, it makes sense that the anticipated reward should be commensurate with the risk involved. This is not always the case in practice.

Diversification is the concept of lowering the total risk of an enterprise by spreading risk among many distinct projects: the total risk produced by a collection of diverse risks is *less* than the sum of those risks considered in isolation. Diversification is a very common-sense concept, as expressed by the oft-quoted adage that you should not put all of your eggs in one basket.

Put more technically, diversification is a result of the fact that not all opportunities are affected by risk-driven events in the same manner. For example, an increase in the oil price costs cuts into airline profits, but benefits oil companies. As such, an investor who owned both an oil producer and an airline would be less affected in the event of a price rise than one that owned two airlines or two oil producers.

These situations allow diversification to reduce portfolio risk significantly when many different investments are combined. The more dissimilar the investments (the less correlated they are), the greater the level of diversification. However, while these offsetting effects reduce risk at the enterprise level, the expected return on the enterprise portfolio remains a simple weighted average of the individual returns.

Leverage is the effect of borrowing to increase the risk/return profile of a venture. Money borrowed at a flat rate can be used to finance new investments. This has the effect of substantially increasing the risk and return in an investor's portfolio. Since the investor only needs to pay back the loan amount, any profits made with the borrowed capital are his to keep.

Thus, an investor might think he has spotted a sure thing and invest $200, comprising $100 of his own money and $100 borrowed from the bank. If he achieves a 25 percent return on the investment, he will make $50; since he only has to pay back $100 (ignoring interest in this simple example), he is left with $50, amounting to a 50 percent return on his own money. Of course, had he lost money, he would have lost twice as much. Simply put, leverage multiplies the risk/reward profile.

Finally, hedging is the process of offsetting risk by entering into a market position that is negatively correlated with an existing position. This is similar to diversification, but is motivated by the desire to reduce the risk associated with an existing investment, rather than to add new investments in a way that reduces overall risk. In this sense, hedging is much like insurance, and should be treated as such.

For example, say that a newly hired CEO is given shares of company stock valued at $50, but is not permitted to sell them for two years. Having done a sterling job, the stock has appreciated to $100 a share at the end of her first year, but the business climate is changing and the CEO fears that the stock may drop again before she can sell her shares.

To hedge against this downside risk, she buys put options on the stock that allow her to sell the stock for $100 at the end of the two-year period. The options are not necessarily cheap, but this hedge guarantees that no matter what price the stock reaches, our CEO will be able to sell each of her shares for $100. The financial security allows her to stop worrying about college fees and enjoy life a little more.

Now let's look at how a consideration of these concepts can help in enterprise risk management (ERM).

BENEFITS OF ACTIVE PORTFOLIO MANAGEMENT

Instead of managing individual securities within an investment portfolio, the goal of ERM is to manage individual businesses within an overall business portfolio. Portfolio management supports ERM in four important ways, by:

- Unbundling risk origination, retention, and transfer
- Providing a risk-aggregation function across the company
- Setting risk limits and asset-allocation targets
- Influencing transfer pricing, capital allocation, and investment decisions

Unbundling

By definition, portfolio management goes beyond business management at the transactional level and manages the overall business as a whole. Ironically, one frequent result is the unbundling of the business in terms of risk organization, risk retention, and risk transfer. A company's management can consider its core competencies and risk/return economies, then decide which of these functions it wishes to compete in.

What does this mean in practice? This kind of disaggregation has been the norm in mortgage banking for nearly 30 years, where the primary

risks in question are consumer credit risk and mortgage prepayment risk. Companies can specialize in loan origination, loan funding and/or servicing, or loan securitization (packaging individual mortgages into pools for sale in the secondary markets as mortgage-backed securities).

In recent years, this portfolio-management approach has extended into the credit cards, auto loans, and more recently, commercial loan and junk bond markets. It is now becoming increasingly widespread among non-financial corporations. Energy firms, for example, increasingly adopt it when addressing their interests in exploration, transportation and storage, product development and distribution, and trading. The key point here is that by understanding the risk/return economies of the overall business, a company can decide where within the value chain it should compete.

Risk Aggregation

The overall risk portfolio represents the aggregation of all types of risk within a company, across different business activities and risk types. Management needs information on aggregated risk exposures, as well as how these exposures correlate with each other; these should be the basis for setting risk limits and allocation targets, as discussed below.

For some companies, the aggregation of risks is performed for measurement and reporting purposes, and the risk profile of the company is managed through corporate management processes such as strategic planning, capital allocation, limits setting, and so on. Other companies prefer to take a more dramatic approach to certain risks, in which all risk exposures are transferred directly or through a transfer pricing mechanism into a central function where portfolio management and hedging decisions are made.

For example, most large banks manage interest rate risk centrally, by providing each business unit with duration-matched funds transfer prices for all of their assets and liabilities. This serves two key purposes. First, the profitability of the loan-origination and deposit-gathering businesses can be measured without any earnings contribution from interest rate risk. Second, the interest rate risk of the bank can be aggregated into a central interest rate risk unit where hedging decisions can be made after considering the effects of portfolio diversification.

Non-financial corporations perform a similar function when they centralize treasury functions—funding and hedging—and charge hedging costs to business units by levying a transfer price for funds. These companies benefit from the aggregation of risks by tracking enterprise-wide risk exposures, incorporating the effects of diversification, and centralizing risk management decisions where appropriate.

Risk Limits and Asset Allocation

The manager of a stock portfolio can ensure a balance between diversification and performance by establishing risk concentration limits and asset allocation targets. For example, a stock portfolio's investment policy might indicate that the fund cannot have more than 5 percent of its assets in any company, or 20 percent of assets in any industry. These limits ensure appropriate diversification. Within these risk limits, the portfolio manager might set asset-allocation targets that would overweight industries that are deemed undervalued, and vice versa. Such targets seek to maximize fund performance within the constraints established by the risk limits.

A business can set similar portfolio risk limits and allocation targets. For example, a global business operating in 10 countries might establish an upper limit of 20 percent for revenue contribution from any single country. On average, each country contributes 10 percent to total revenue. But given its positive outlook for, say, India, it might set a revenue contribution target at the maximum limit of 20 percent. In this case, the higher revenue target for India based on optimistic management projections is kept in check by the country limits. Risk limits and allocation targets thus provide complimentary controls for achieving optimal risk/return for the business.

Influencing Transfer Pricing, Capital Allocation, and Investment Decisions

Corporate management can shape the risk profile of the business portfolio in several ways. For example, the global business in the above example can adjust its transfer prices for India by increasing income credits and/or lower transfer costs to that country in an effort to motivate aggressive growth.

Management can also allocate more economic capital to businesses and products that are expected to produce superior risk-adjusted return on that capital. An efficient capital allocation process should function as an internal capital market where funding is provided only to businesses with the best prospects for earnings growth.

In addition to profitability and growth objectives, the capital allocation process should also be driven by diversification goals. For example, the investment decisions for research and development (R&D) at a drug company can be viewed as a portfolio of options. As with options, each new drug has an option premium (R&D investment costs), current price versus strike price (project status against plan milestones), implied volatility (project uncertainty), and time to maturity (time to launch product). For the drug company, its market value is determined not only by the success of its existing products (those that are in-the-money until patent expiration) but also by the pipeline of promising new drugs (options in its R&D portfolio).

As such, the management of drug companies should pay close attention to managing the life cycles of existing products as well as those in its pipeline.

This dynamic approach to portfolio management can benefit all types of companies—especially those that deal with products that exhibit out-of-the-money option characteristics (e.g., venture capital firms, like drug companies, have many more failures than successes) or products with short life cycles (e.g., technology firms).

PRACTICAL APPLICATIONS OF PORTFOLIO MANAGEMENT

While the theoretical arguments for active portfolio management in the capital markets seem sound, there is no clear evidence that active management yields consistently higher risk-adjusted returns in practice. As a result, many proponents of index investing have argued that, given lower expenses, it makes more sense to invest passively in an equity index than to bet against the assumption that investors and markets are rational and efficient, or that a particular manager has extraordinary insight into potential investments.

Does this argue against extending those arguments to business enterprises, as we did in the last section? Actually, it doesn't, because the flaws in the theory don't necessarily apply in a business context. *Holding a market portfolio* means little for the managers of a company, and so there is generally no passive strategy. On the contrary, competent managers should be expected to have superior inside information about the portfolio of businesses that make up their company, and to make rational decisions about them. Given this, a diligent active portfolio-management approach can be highly effective for controlling return targets and risk limits.

Put another way, diversification can increase shareholder value, active management can keep risk within tolerable levels, and volatility can often be managed with existing financial instruments. It makes more sense to diversify and stay on the efficient frontier than to focus risk exposure in one arena and encounter more volatility than is necessary to achieve the same expected returns. If diversification through project selection is not an option, more advanced hedging techniques (such as options, futures, etc.) can be considered.

Now, let's put aside the theory, and instead consider two fictional case studies: an insurer concerned about a sharply increased chance of bankruptcy; and a manufacturer exposed to significant foreign exchange exposures.

Reinsurance

Although issuing insurance is the primary business activity of an insurance company, many insurance companies have publicly traded equity, and one

of their primary management objectives is ensuring shareholder satisfaction. Thus, when the risk profile of outstanding contracts goes beyond a defined tolerable level, many insurance companies will purchase reinsurance (insurance for insurers) from other insurance companies.

Consider the case of WindGuard, a fictitious Florida insurance company that specializes in providing homeowners with insurance against damages caused by natural catastrophes, such as hurricanes. WindGuard has historically performed very well, due to mild weather and well-priced contracts. The company has liquid assets, in the form of collected premiums, of $1 billion.

Insurance is, by its nature, a very risky business. The value of an insurance company is in its ability to forecast risk and price its contracts appropriately: if the risk can be accurately quantified, the leftover cash from the premiums becomes the profit. In WindGuard's case, a typical year results in a payoff rate of around 0.7 percent. That would mean that the company would pay out some $700 million of the $1 billion in claims and book $300 million as gross profit.

However, as Hurricane Andrew demonstrated in 1992, the effects of even one severe storm can be so financially devastating that an unprepared insurance issuer may be put out of business. Several small insurance companies actually were bankrupted in 1992, which stranded nearly a million policyholders.[3] And new proprietary studies indicate that the weather is becoming increasingly volatile, which translates to a greater chance of a payoff rate changing to anywhere between 0.2 percent and 1.2 percent of the face value of the contracts.

WindGuard's managers are concerned about this increase in loss volatility, and specifically about the $100 billion of disaster contracts it has already issued for the following year. They are afraid that if the next season is bad enough, there will not be enough money to pay the disaster victims. This could mean a catastrophe for the insurance company itself, as well as the unpaid victims.

From the portfolio-management standpoint, the insurance company still has the same expected return, $300 million—but the risk has reached a level where the company cannot afford to be exposed to it. One solution is to purchase reinsurance; this would reduce the net expected return for the insurance company (since the reinsurance protection has a price), but it would also significantly reduce risk. A reinsurance policy switches WindGuard's exposure from unpredictable hurricane risk to the more predictable, and presumably smaller, counterparty risk of its reinsurer(s).

The company decides that it should not take the chance of going out of business, and therefore finds a reinsurance contract from another firm that allows it to reduce its risk appropriately. The contract costs $150 million,

but covers all payoffs beyond $700 million. That leaves it with only $850 million in liquid assets, but guarantees that it will keep a minimum of $150 million of the premiums it has earned.

Although this is not necessarily the most efficient risk-return profile, it makes good business sense if WindGuard believes that $150 million and a lower chance of bankruptcy is preferable to $300 million and 20 percent chance of bankruptcy. Provided that WindGuard's management explains the risks and its response effectively, the company's shareholders will likely come to the same conclusion.

Currency Hedging

Stable revenue streams are extremely important to any corporation striving to maximize shareholder value. Volatile revenue streams imply a risky business environment and an uncertain picture of the future. Shareholders demand a higher rate of return for this sort of volatility, so they would rather put money in safer stocks that promise the same rate of return with less risk. As a result, the valuation of a volatile company is generally lower than that of its peers with more stable revenues.

Fortunately, a corporation often has more control than it realizes over this revenue generation risk. Consider the case of WidgetCo, a fictional U.S.-based company that has been manufacturing America's finest widgets for many years and has impressed shareholders with steadily increasing revenue and earnings growth. This year, however, much of its sales are originating abroad for the first time. Specifically, a craze for all things widgety in Japan has significantly boosted its orders there, so its anticipated U.S. sales of $50 million are matched by an anticipated 5,000 million yen in Japanese sales, which are also worth $50 million, at an exchange rate of 100 yen to the dollar.

WidgetCo management has never worried about its negligible foreign exchange risk in the past, but is now afraid that these large foreign orders are adding considerable uncertainty to the firm's future revenue flows. The company manufactures custom widgets, whose complex nature means that most orders take a minimum of three months to complete. Payment arrangements are finalized before production starts, although payment is only made on delivery. To make matters worse, WidgetCo's powerful Japanese customers are unwilling to assume any foreign currency risk exposure and will only pay in Japanese yen. Moreover, WidgetCo's suppliers and manufacturing operations are U.S.-based so there is no natural hedge between its yen-based revenues and the U.S. dollar expenses.

As such, WidgetCo is exposed to the risk that the value of the yen will change against the dollar between each order and its delivery, which means

that its Japanese revenues will translate into more (or less) than the $50 million nominal value of the order. Should WidgetCo hedge this risk, and if so, how?

WidgetCo could decide to do absolutely nothing about the risk. The expected revenue is still $100 million, albeit that the U.S. dollar value of the 5,000 million yen coming from Japan is at risk from fluctuations in the U.S. dollar-yen exchange rate. If nothing happens to the exchange rate during each of the three-month periods between orders and deliveries, WidgetCo will be able to exchange its yen for dollars at the 100-to-1 rate each time and achieve cumulative revenues of $100 million. This would make the shareholders happy and demonstrate that WidgetCo is still profitable and growing.

This is not very likely, however. If, as is far more possible, the exchange rate deviates at all over the three-month production periods, the cash flows from Japan will become uncertain. WidgetCo doesn't take a view on the direction of the yen, so it assumes that the exchange rate is just as likely to rise as to fall. That means it is equally likely to realize more or less than the nominal U.S. value of the Japanese order. For example, if the exchange rate becomes 80-to-1, the 5,000 million yen will become worth significantly more than the anticipated $50 million. In fact, they will now be worth $62.5 million, and WidgetCo's cumulative revenues will be $112.5 million. However, if the exchange rate became 125-to-1, WidgetCo's Japanese revenue would only be worth $40 million.

If both of these possibilities are equally likely, what should WidgetCo do? The answer lies in the shareholder's view of the company. The shareholders expect the company to increase its revenues and profits steadily, and would likely lose much confidence if revenues came in lower than expected. In the case where the exchange rate becomes 125-to-1, the $40 million revenue would force WidgetCo to report a loss for the year, and shareholders would definitely lose confidence in its earning potential.

So this uncertainty is best avoided. An upside surprise, though, would likely be unsustainable in the long term, since fluctuations in a foreign exchange rate should be random in the long term. WidgetCo's shareholders will realize this, and will likely discount such extraordinary profits. They also may realize that the unexpected upside this time could give way to an unexpected downside next time.

Although WidgetCo might be lucky enough to report a short-term gain, it cannot rely on a discernible increase in its longer-term expected returns. This makes it impossible to justify taking on greater risk, and so it becomes apparent that management would be remiss if it did not hedge against this kind of foreign exchange risk. Portfolio management theory espouses that risk should be as low as possible for a specific rate of return, and it certainly makes sense in this example.

After some deliberation, WidgetCo decides that its new policy will be to enter into forward contracts at the same time that each sale to Japan is signed—these forward contracts are arrangements with a third party to exchange a fixed amount of currency at a predetermined exchange rate. In this manner, WidgetCo's managers can rest assured that widget manufacturing will continue to be a solidly reliable business.

These last two examples illustrate how a business could decide whether or not to seek third-party protection against risk. In the next chapter, we'll look at the alternatives when it comes to actually carrying out a risk transfer strategy.

CHAPTER 8

Risk Transfer

Put simply, risk transfer is the act of moving risk from one entity to another. In more precise terms, it is the deliberate exchange of probabilistically different cash flows. Either way, it is most often taken to mean the movement of some of a company's risk to an external party—but it can also mean the shifting of a given risk to a different part of the same company, or the creation of a new subsidiary within that company for the specific purpose of managing that risk.

The most traditional way in which companies transfer risk is through the purchase of various kinds of insurance, with the three most common types being workers' compensation, general liability, and property/casualty insurance. When a business buys an insurance policy, some or all of the risk associated with any event covered by that policy is effectively transferred from the business to the insurer. The concept of insurance has been around for a long time: a form of marine insurance is mentioned in the Code of Hammurabi, written some 3,800 years ago.

The second common risk transfer mechanism is through derivative products such as futures, forwards, swaps, and options. Strictly speaking, a derivative transaction alters the characteristics of a company's cash flows through a financial obligation in a way that may adjust the nature or amount of risk to the company. Unjustly maligned as dangerously volatile transactions for hardened speculators, largely due to their involvement in a number of disaster stories in the 1990s, derivatives actually have a pedigree comparable with insurance and have been safely used to manage risk at many corporations.

Risk transfer revolved around either insurance or derivatives for many years—in fact, for centuries. Since the late 1980s, however, there has been a proliferation of risk transfer products that combine the features of both. These products are known collectively as *alternative risk transfer* (ART) products. While they have yet to realize their full potential, they hold the promise of risk transfer rationalization that we cited as a major benefit of ERM back in Chapter 4.

Insurance and derivatives may at first seem an unlikely pairing. People generally (inaccurately) associate insurance with risk reduction and derivatives with risk enhancement. The blending of elements from both categories into new financial instruments is therefore an uncomfortable idea for many. A more accurate perspective is to think of insurance as a source of capital that becomes available if some event occurs (*contingent capital*) and derivatives as a means of *risk manipulation*.

The combination of capital reserving and risk manipulation can allow companies to change their risk profiles in powerful ways. Modern corporations are coming to realize that by outsourcing risks that they had once regarded as a normal part of business operations, they can reduce their risk management expenses, simplify their administration, and even increase shareholder value.

A BRIEF HISTORY OF ART

Alternative risk transfer has no formal definition, but can be broadly understood as a range of non-traditional risk transfer products. Most of these can be placed into one of two categories: unconventional vehicles used to cover conventional risks, and vehicles based on instruments from the capital markets. A selection of these products is given in Table 8.1.

The ART market has its roots in a deeper trend: the convergence of the capital markets and banking industries. ART products cannot be created without a high degree of interaction between the insurance industry and the capital markets, which has traditionally been in short supply. Prior to the 1970s, insurance companies were banks' customers, and vice versa. There were few firms that offered any kind of integration of insurance and capital markets techniques.

Signs of change emerged during the early 1980s, as large companies began to seek alternatives to costly traditional insurance. An increasing number began practicing self-insurance through Self Insured Retentions (SIR), Risk Retention Groups (RRG), captives, and rent-a-captives. It should be noted that self insurance is not the same thing as no insurance; a self-insuring corporation explicitly assumes a given risk and establishes reserves for negative contingencies. Companies practicing self-insurance typically use it to cover well-defined, high-severity, and low-frequency events. Rather than pay premiums to an insurer over several years, they save the money in their captive, to be disbursed against the occasional catastrophe—saving themselves the insurer's margin. Technically speaking, this is risk financing rather than risk transfer, but it is often referred to as an ART practice because it is used as an alternative to conventional insurance.

TABLE 8.1 ART Products

Unconventional vehicles used to cover conventional risks:
Self-Insured Retentions (SIR)—retentions of capital set aside for use under negative contingencies.
Risk Retention Groups (RRG)—self-insurance capital pooled by a number of small-to-medium sized companies.
Captives—subsidiary companies set up solely to insure to the parent company. These are often located offshore to exploit tax advantages.
Rent-a-Captives—captives shared among several medium-sized companies; funds are managed centrally.
Earnings Protection—policies triggered by a specified earnings shortfall within a given financial period.
Finite Insurance—insurance policies extended over a multi-year time period in order to smooth profit and loss. This kind of insurance often involves very little risk transfer, but has the effect of reducing capital requirements and/or taxes.
Integrated risk and multi-trigger policies—policies covering a basket of different risks, some of which are not conventional insurance risks; sometimes called insuratization.
Multi-Trigger Policies—policies triggered only if a number of different specified events occur within a given timeframe.
Multi-Year, Multi-Line Policies—policies covering a basket of different risks, spread out over a specified number of years.
Vehicles based on instruments from the capital markets:
Insurance-linked bonds—bonds whose interest and/or principal are wholly or partially forfeit if a specified event occurs. These are most popular as a way of transferring natural catastrophe risk from reinsurers to the capital markets.
Securitization—the process of packaging risks into debt or equity instruments that can be traded in financial markets.
Cat-E-Puts—(Catastrophe Equity Put Options) options allowing a company to issue and sell equity at a predetermined price in the event of a specified catastrophic event.
Contingent Surplus Notes—notes providing access to capital to their holders in the event of a loss event.
Credit Default Swaps—derivatives under which the buyer pays premiums to the seller, who makes a payment to the buyer in the event of a credit default.
Weather Derivatives—policies triggered by specified meteorological events of predetermined magnitude.

The next step in the emergence of ART was largely the result of Hurricane Andrew, which caused a huge amount of damage to South Florida in August of 1992. Even though it narrowly missed hitting Miami, this hurricane was the most expensive meteorological event up to that time, causing an estimated $15.5 billion in overall losses. Insurers and reinsurers, with aggregate reserves estimated at less than $250 billion, were not well prepared for this event. Several went bankrupt, while those that survived had to raise the premium they charged dramatically.

The aftermath of Hurricane Andrew brought the idea of securitization to the forefront of risk transfer thinking. It became clear that a company did not need to cover its risks through conventional insurance or even through self-insurance: it could instead package its risks and sell them on the open market. Mortgage-backed securities had been traded since the late 1970s, and items such as auto loans, home loans, and credit cards were securitized not long after. These instruments transferred financial risks—mostly retail credit risks—away from product providers and into the hands of capital market investors.

The possibility of doing the same with insurance risk was now a serious consideration. While the claims associated with Hurricane Andrew were huge, they represented only a tiny fraction of the multi-trillion dollar value of capital markets. Securitization also provided a way for large single risks (such as natural catastrophe risks) to be split up and spread among many investors, who could hold the individual pieces of the risk in a more diversified portfolio than a single insurer could.

A number of vehicles aimed at facilitating this transfer sprang up in the mid-1990s. In 1995, the Chicago Board of Trade, one of the world's largest derivatives exchanges, began to market futures on Property Claims Services' indexes of catastrophe insurance losses. The same year, the Catastrophe Risk Exchange, a bulletin-board enabling insurers and reinsurers to swap units of risk of different types and from different geographies under standardized contracts, opened for business. Two years later, the United Services Automobile Association (USAA) kick-started the market in catastrophe-linked bonds, whose repayments change in amount and/or timing if a catastrophic event occurs. USAA obtained $400 million in coverage by issuing hurricane-linked bonds to investors. Seven years later, a total of more than $3.5 billion worth of insurance risk had been sold in capital markets.

The implied threat to the traditional insurance business went largely unheeded. The kinds of risk involved in early securitization deals—those associated with massive natural catastrophes—were risks that most insurers didn't have enough capital to take on. If anything, they presented a way for them to offer coverage in markets that hadn't previously been viable. Many insurers also assumed that securitization would be a passing fad, and thus

was not worth worrying about. However, the volume of ART transactions has continued its upward climb. In 2012, reinsurance sales in the capital markets rose above $190 billion.[1]

Furthermore, ART deals offered protection for non-catastrophic risks that could conceivably have been covered by insurance. For example, weather is a major contributor to the volatility of earnings for companies in many varied industries, ranging from clothing to tourism to agriculture. Until recently, it was a risk that companies typically just had to live with. From the mid-1990s onward, however, companies began to write insurance against weather based on average temperature (e.g., average degree days) or other weather-related measures. One early success for the market was a substantial policy that Boston's Logan Airport bought as protection against snowfall of greater than 44 inches—an amount that would significantly impact airport revenues. That policy paid out to the tune of some $2 million following the winter of 1995 to 1996, when snowfall totaled 107 inches.

Although the Logan Airport case was not the debut of weather insurance, its outcome did much to increase demand for such coverage. Predictably, other companies hoped to benefit in the same way, which drove up demand for weather insurance for the winter of 1996 to 1997. This increased demand was countered by the insurance companies' newly raised premiums. That helped to spawn the popularity of capital markets alternatives—notably, weather derivatives, which also served to provide protection, but did not rely on a single, capital-rich provider.

To the surprise of those who predicted a swift demise for the emerging ART market, groundbreaking deals continued to be struck over the course of the late 1990s. In July 1998, Honeywell purchased an unusually comprehensive integrated risk policy, covering substantial financial and insurance risks. In October of that year, British Aerospace purchased an innovative earnings protection policy, which effectively guarantees that there will be no shortfall in the company's expected $3.9 billion of leasing income over the next 15 years.

Since then, ART has continued to develop at considerable speed, and it is probably fair to say that the majority of industry executives today are of the opinion that more and more ART transactions are likely to occur in the near future. This further growth of ART will be supported by a convergence of banking and insurance that goes beyond risk transfer instruments; the industries as well as the instruments are uniting. During the 1980s, large insurance and reinsurance companies such as AIG and Swiss Re developed significant capital markets and derivatives businesses. In April of 1998, the high-profile merger between Citicorp and Travelers highlighted the business potential for such combinations.

The integration of banking and insurance businesses, either through mergers and acquisitions or expansions, will likely result in more supplier resources for the ART market. These companies possess the essential competencies required for ART transactions: the insurer's skill at quantifying the likelihood and magnitude of a risk, together with the bank's experience in packaging, underwriting, and placing securities. They also have the advantage of greater capitalization than most insurers, which enables them to take on some of the risk. This can prove key in getting complex deals off the ground.

ADVANTAGES OF ART

So what does ART have to offer, besides an alternative for companies that don't like insurance? The answer, as suggested earlier, is the rationalization of risk transfer across the organization—a fundamental benefit of ERM. The traditional management of risk in silos, where different risks are managed by different organizational units, has resulted in risk transfer programs that have not been rationalized either from the point of view of corporate policy or of economics.

From a policy perspective, a typical company might have in place a very conservative (and expensive) program for eliminating currency risks, but have no risk transfer strategies for other risks such as computer outages, which could potentially be more significant. Even within companies where these functions are part of the same department, these policy decisions are generally made independently. This is largely due to the decentralization of risk transfer, with little or no policy coordination from senior management.

The financial objectives of these risk transfer activities are also distinct from an economic perspective. For example, a company's treasurer may want to use financial derivatives to eliminate all exposures to currency movements and to minimize the cost of issuing debt. The credit risk manager might prefer to reduce the company's credit exposure to emerging markets, and the insurance risk manager would focus on reducing premiums paid while maintaining the same coverage for general liability and property damage.

The key problem with this approach is that risk transfer activities will likely be inconsistent from a policy perspective, which may lead to insignificant risks being over-hedged and critical exposures going unremarked. Enterprise risk management enables companies to measure, manage, and transfer risks on a much more integrated and rational basis. With specific reference to risk transfer, ERM is useful for:

- Establishing more consistent risk transfer policies, such as prioritizing risk exposures that have the greatest impact on the company's earnings volatility. This ensures that the most important risks receive the most immediate attention.
- Incorporating the full effects of diversification, so that only the company's *net* exposures are considered in risk transfer. A company that transfers out *gross* exposures without considering diversification is bound to over-hedge.
- Establishing an economic framework in which the costs and benefits of various risk transfer strategies can be evaluated. As a rule, the company should only transfer out risks if the cost of risk transfer is lower than the cost of risk retention, unless it deems the retention of certain risks to be entirely unacceptable.

Table 8.2 provides a simple example of how enterprise risk management can rationalize a company's risk transfer strategies. In this example, the company's economic capital requirements for credit, market, and operational risks are $50, $30, and $40, respectively. Diversification benefits amount to $20, resulting in a total economic capital of $100. If the cost of capital is 15 percent, the total cost of risk retention is $15.

Now assume that the company is considering an ART strategy that can reduce its risk levels by half. That is, the ART strategy will reduce the economic capital required by half and reduce the cost of risk retention to $7.50. If the risk transfer costs only $5, there will be a reduction of $2.50 in the net cost of risk. That suggests the ART would be a good move.

Such a decision framework captures all of a company's sources of risk on a consistent basis, incorporates the effect of diversification, and evaluates

TABLE 8.2 Cost-Benefit Analysis

	Economic w/o ART	Capital w/ ART
Credit Risk	50	25
Market Risk	30	15
Operational Risk	40	20
Diversification Effect	–20	–10
Total Economic Capital	100	50
Cost of Risk at 15%	15	7.50
Risk Transfer Cost	0	5
Net Cost of Risk	15	12.50

the cost-benefit of risk transfer. The same framework can be used to evaluate risk transfer using traditional insurance and derivative products as well as ART, and so is useful for comparing and contrasting their various effects.

ART has other advantages, too: focus; customization; cost reduction and simplified administration; coverage of non-traditional risks; and earnings stability. Let's briefly consider these.

Focus

An emerging business paradigm is that a company should do what it knows how to do best, and outsource the rest. The average company, for example, does not manufacture its own computers or build its own office furniture, unless it happens to be a computer manufacturer or furniture maker. It follows that, since most companies are not in the business of managing financial and insurable risks, they would be wise to transfer risk to an outside party. This selective delegation of risk translates to more efficient use of capital for the business as a whole.

Customization

An ART policy is to a traditional insurance policy what an over-the-counter (OTC) derivative is to an exchange-traded derivative. ART deals are company-specific and made to order, unlike more standardized insurance policies. Thus, a company buying an ART product is not obliged to purchase coverage that it is unlikely to need, and can easily arrange for extra coverage in areas in which it has unusual levels of vulnerability.

This is particularly helpful for companies with unusual portfolios of risk that might not be adequately covered by traditional insurance. For example, a company that wishes to transfer some or all of its lending risk, counterparty risk, operational risk, or settlement risk can only do so through one form of ART or another. Given the recent focus on operational risk management, companies will likely identify more non-traditional risks that they want to transfer out.

Cost Reduction and Simplified Administration

If a company uses integrated risk policies or multi-line insurance, it may be able to use the natural hedges created by non-correlated risks to reduce the overall cost of the policy, in comparison with the aggregate cost of the same kinds of insurance purchased separately. A multi-line policy covering both currency and catastrophe risks will typically cost less than the combined prices of a stand-alone currency policy and a stand-alone catastrophe policy,

since the occurrence of natural disasters is usually largely uncorrelated with fluctuations in exchange rates.

Another advantage of using an integrated risk policy or a multi-line finite policy is the reduction in insurance-related administrative duties. If all coverage is purchased from the same company, there is less paperwork, fewer contacts to be dealt with, and no need to compare multiple policies for overlaps.

Earnings Stability

We've already noted that shareholders and analysts have become increasingly sensitive to earnings volatility in recent years. Given the choice of two securities that perform similarly over the long term, investors will pick the one that exhibits less variation in periodic earnings. Earnings can be smoothed to some extent by more conventional hedging, but it would typically take a great many separate (and costly) hedges to achieve the same degree of homogenization as ART products can.

PITFALLS OF ART

Despite these many benefits, ART is not a panacea. In particular, ART cannot completely eliminate risk any more than any other form of risk transfer can. As noted in *Global Institutions, National Supervision and Systemic Risk*, the landmark 1997 report[2] produced by the Group of Thirty (G30): "Of course, there is no way to eliminate risk or failure completely. The business of market intermediation is to accept an appropriate amount of risk and manage it effectively. A financial system that attempts to eliminate risk rather than managing it well would be costly and inefficient."

This holds equally true for the companies working within that system: they cannot eradicate all risks without greatly hampering their operations and financial performance. There are limits to the utility of risk transfer, whatever form it may take. Even if a company *could* transfer out most of its credit, market, and operational risk does not mean that it should. The transfer itself would generate new risks: most obviously counterparty risk to the provider of the risk transfer service. The amount of risk that a business should transfer, and the means it should use to transfer that risk, are largely dependent upon the specific needs and characteristics of that company.

Though most companies hold at least some conventional insurance, many have yet to use any ART vehicles. The usual rationale is inertia; if one's company has done fairly well with conventional insurance coverage,

there is little incentive to try ART. Some executives have chosen not to consider use of ART on the grounds that it is new and therefore risky.

Certainly, there is a degree of truth to this. ART does not yet have a long history, and so some of its methods inevitably need to be refined. Some risks are impossible to quantify with precision, and so insurance-linked bonds may be needlessly expensive to issue or provide insufficient coverage for a given event. There are also potential cost issues. An ART product may require a larger initial outlay than a conventional insurance policy, though this is not always the case. The complexity and customized nature of ART instruments may also make the deal-making and legal documentation processes somewhat lengthier than companies are used to.

The greatest barrier to ART adoption, however, is largely cultural: the purchase and effective utilization of ART may require a company's employees to drastically alter the ways in which they define, measure, and manage risk. Although such a paradigm shift is ultimately in the best interests of the company as a whole, the adjustment process will take time.

If a company comes to the conclusion that ART would be a good solution, there is a certain amount of education that its executives would be wise to acquire before proceeding, including a basic understanding of the product, the seller, and the regulatory and legal environment.

Understand the Product

The nature of the ART market means that the majority of ART products are still much less standardized than conventional insurance policies. Though this can be a great advantage, in terms of customizing an instrument to the individual needs of the buyer, it can also make it difficult to determine fair prices and reasonable terms. Moreover, the insurance contract needs to be developed to facilitate the efficient processing of potential claims and settlements. To make sure that an appropriate product is purchased at an appropriate price, the following questions must be answered:

- How exactly does this product work? How are the triggers determined? What would the payoff be, given a range of contingencies?
- What is the net impact on the company's economic capital requirements with this product?
- Have similar deals been transacted in the past? If so, how were they priced? Have their purchasers been satisfied with the results?
- Would it be possible to obtain the same coverage through conventional insurance? Would it cost more or less? Would there be tax or regulatory advantages to choosing one over the other?

Know the Seller

Most ART providers were founded in the mid- to late-1990s, and have thus had relatively little time to establish expertise or reputations for themselves beyond those inherited from their parent companies. Even the more established providers are unlikely to have experience setting up all the available variations on ART, due to the great diversity of existing products. It is therefore prudent to make a careful assessment of the capabilities of any potential ART counterparty. Some illuminating questions include:

- Has this entity transacted any ART deals in the past? If so, were they similar to the one currently under consideration? How have these previous deals performed to date?
- Are there former or current customers of this provider who might be willing to offer informed assessments of the entity's skill in ART?
- If this company has not packaged ART deals in the past, does it possess the competencies necessary to put such a policy together? In particular, does it have the experience necessary to bridge both insurance and capital markets?
- How does this company measure and assess risk? What methodologies and models does it use? Does it outsource the risk measurement underpinning the protection it writes? If so, how reliable is the company to which the risk measurement is outsourced?
- Does this company possess sufficient capital and/or reinsurance to reimburse claims that may arise? Are its reinsurers, if any, also capable of sustaining potential losses?

There may be many additional questions to ask, depending on the circumstances of both the company and the risk transfer market. As a rule, the more that is learned about the prospective deal, the less chance there is of making a costly mistake.

Regulatory and Accounting Standards

One of the more salient problems with ART is the confusion regarding its regulation. Capital markets, banks, and insurance companies have traditionally been governed according to more or less separate, and frequently mutually exclusive, sets of rules and guidelines.

It was the breakdown of the barriers between these various markets and institutions in the 1990s that allowed ART vehicles, which exist at their intersection, to proliferate. A single ART transaction may be brokered by

an insurance company, packaged by an investment bank, and placed with investors in the capital markets; this means it may be subject to scrutiny by three regulators and one accounting standards board.

In fact, the treatment of ART products is generally convoluted, with multiple regulatory, legal, and accounting standards coming into play for any novel product or application. Some ART techniques (such as self-retention or captives) are well established. However, many others, such as earnings protection and catastrophe bonds, are still in their infancy, and it is likely that more new products will join them over time. Dealings in such products must be undertaken with an unusual level of expert legal and accounting advice.

A LOOK TO THE FUTURE

It is hard to tell what will happen to ART in the years ahead. Although a large number of major players, in both the insurance industry and the capital markets, are firmly convinced that ART is the wave of the future, there also remain many who believe that ART is a craze—an overly complex solution to a simple problem which will pass within the next few years. The key issue appears to be whether ART products can be executed more cost efficiently than conventional insurance.

Let us paint an optimistic picture. A harder insurance market than that of the 1990s increases the premiums charged for conventional coverage and makes ART look inexpensive by comparison. Companies adopting ERM programs turn to ART as the most efficient means for risk transfer. Their use of these products leads to impressive returns and earnings stability, encouraging other businesses to try out similar products. Increased demand encourages expansion of existing ART practices, and new banks and insurers enter the ART market, some in joint ventures between insurers and banks. Large corporations that own both banks and insurance companies realize that ART offers them much greater opportunity than simple cross-selling does.

The increased use of ART creates a need for standardized legal treatment, and both national and international governing bodies adopt guidelines for straightforward ART regulation. Even as the market for today's ART products grows, the older ART providers begin offering new vehicles, securitizing a greater variety of risks than ever before. Investors, made newly aware of the need for hedging created by increased capital markets volatility, become increasingly eager to purchase these products to diversify their portfolios. ART becomes standard practice for companies in virtually every industry.

This view is largely based on the impressive growth of the ART market in the 1990s, even in the midst of an unusually soft market for traditional insurance. The trend toward enterprise risk management should further support the development of integrated risk transfer products. It only makes sense that as companies take an enterprise-wide approach to managing their risks, they will look for new integrated risk transfer solutions that will help them meet their risk management objectives.

Furthermore, it is likely that demand for ART will increase as the field of risk management matures. Companies will increasingly come to understand that managing risk does not necessarily mean eliminating risk. They will also learn to differentiate between risks that are at the core of their business competencies, and risks that can be more efficiently transferred out. When they reach this point, businesses will finally be able to devote all of their attention to their true task: doing business.

In the last decade, the advancement of the ART markets has resulted in a proliferation of new products and services. For instance, consider the rise of finite risk products, which are, typically, multi-year contracts that allow clients to reduce the cost of capital with more stable earnings. As such, they are powerful tools for managing loss volatility—the ability to control loss volatility is important, because it allows firms to more accurately allocate cash flows and other resources. Insurance is a particularly useful approach to the management of loss volatility because it allows for the distribution of losses over time, as well as among those insured. Popular finite risk products include: loss portfolio transfers; spread loss covers; adverse development covers; and time and distance covers.

Finite risk products are generally more expensive than more traditional methods of insurance, but for good reason—they help to protect against those black swan events that are normally excluded from other types of insurance because they have little historical precedence, which makes loss projections very difficult to calculate. According to Kate Westover, vice president of Alternative Risk Transfer Services at Innovative Captive Strategies, Inc., "finite risk methodology is a necessary alternative to traditional insurance rating techniques."[3]

Another notable product is contingent capital, which is a bond—debt, essentially—that turns into equity when certain triggers are set off, or in the case of a defined event. In the short-term, contingent capital helps to keep the cost of capital at low levels, because it is generally classified as debt, but, like finite risk products, also serves as a cushion against black swan events. In this manner, contingent capital can go quite some way in helping to mitigate the too-big-to-fail problem by allowing banks and other financial institutions to re-capitalize without needing to touch taxpayer funds.

CASE STUDY: HONEYWELL

In February 1997, Honeywell Inc. took an "intrepid step forward transferring its risks"[4] by blending its property and casualty exposures and foreign exchange translation risks in a single policy insured by American International Group and brokered by J&H Marsh & McLennan. "Our objective was to significantly reduce our overall cost of risk, as well as our administrative costs," says Larry Stranghoener, Honeywell's CFO and vice president.[5] Mr. Stranghoener was looking for a policy that would limit the volatility of Honeywell's financial results under the assumption that, as was discussed earlier in this chapter, stock markets punish earnings volatility with sometimes significantly lower stock prices.

By taking an integrated view of their risk exposure and using alternative risk transfer methods, Tom Seuntjens, director of risk management at Honeywell, estimates that Honeywell was able to save more than 20 percent over its traditional risk management practices. It was able to cut the number of insurance carriers it used from 17 down to 10, and noted real savings in staff time and overhead because of simplified transactions.[6]

Honeywell has been pleased with the policy's performance thus far, and is now considering adding a weather risk transfer element to help offset the risk of mild winters on sales of its thermostats. Honeywell is also evaluating the possibility of adding interest rate risks and foreign exchange transaction risks to the mix.[7] Furthermore, it is deliberating movement in the direction of full enterprise risk management. "We believe it makes sense from a risk management standpoint to evaluate our total risk profile, not just hazard and financial risks, but also our operational and strategic risks. Once we do that, the next logical step is to find a comprehensive way of mitigating those risks. It's still too early to say if we will go this way, but I think we already have the reputation for being aggressive and innovative in this area."[8]

CASE STUDY: BARCLAYS

In an effort to meet the higher required levels of contingent capital, British banking giant Barclays has recently rejuvenated its ART strategies by offering a wave of 10-year contingent capital bonds—in 2012, it sold $3 billion worth of these products to investors across Asia, Europe, and the United States. The attractiveness of the bonds can be attributed to its 7.6 percent interest rate, which is remarkable in today's historically low rate environment.

Still, this higher yield comes attached with a corresponding higher risk; should Barclays incur losses that bring its core Tier 1 equity ratio to 7 percent or lower, the value of the contingent capital bonds drops to zero,

and investors lose all their money. Potential investors are concerned by this stipulation, worrying about the asymmetrical risk/return profile of these bonds. Robert Montague, of ECM, notes how "some investors prefer getting written off to being converted to equity. . . . These instruments share the same downside risk as equity, but none of the upside."[9]

While some banks have followed in Barclays footsteps—including Credit Suisse and UBS—many have instead turned to other forms of ART products. While regulators are encouraging banks to engage more with contingent capital, Barclays' current shareholders hold mixed views of it; in the case that these bonds are converted into equity shares, the ownership interests of existing shareholders will inevitably be diluted.

It is too early to tell whether Barclays' latest move will prove to be a success or a failure. However, what is obvious at this stage is the fact that increased regulatory capital requirements and an uncertain economic climate have driven banks to be more innovative in their risk transfer strategies, which has pushed the growth of ART applications to a much higher level.

CHAPTER 9

Risk Analytics

In risk management, as in many other business disciplines, you manage what you measure. As discussed in Chapter 3, risk measurement is one of three components of the basic risk management process—the other two being risk awareness and risk control.

Risk measurement analytics are therefore an invaluable part of the risk management process. Trying to manage risk without appropriate analytical tools is like trying to fly a plane without instrumentation—while the weather is good, everything is fine and the organization may not experience substantial losses. But in bad weather, the organization can be put in grave danger without any sense of where it lies.

Increased awareness of the challenges of ERM has therefore led to increased development of advanced analytical and reporting tools. Since the early 1990s, volatility-based models such as Value-at-Risk (VaR) have been applied to the measurement and management of all types of market risk within an organization. Value-at-risk can be defined as the maximum potential loss that a position or portfolio will experience within a specific confidence level over a specific period of time. In market risk management, the use of VaR models has become standard practice for estimating potential loss and establishing risk limits.

Similar models, along with models of corporate default, have more recently been applied to credit risk management; some companies have even begun experimenting with the application of these techniques to operational risk management. This has supported the quantification and management of credit, market, and operational risks on a more consistent basis.

The same techniques can also be used to evaluate the merits of risk transfer products such as derivatives, insurance, and ART products, as well as in the quantification of risk exposures and risk-adjusted profitability. Take risk transfer—a company's management can increase shareholder value through risk transfer if the cost of transferring out a given exposure is lower than retaining it. For example, the all-in cost of risk transfer might be 12 percent

and the cost of risk capital 15 percent. Alternatively, management might want to reduce the company's risk exposure from a VaR of $300 million to a VaR of $200 million. Risk analytics can be used to determine the most cost-effective way to do that.

Various analytical tools are available for managing risk at the enterprise level. Each of these can be grouped into one of two broad categories. The first focuses on risk control. These are designed to ensure that the risks being taken by an enterprise conform to its overall risk appetite. The second category is oriented around risk/reward optimization. These analytics are intended to support the enterprise in determining which risks it should take (i.e., identifying those that offer a high return relative to their risks) and which it should avoid (i.e., low returns relative to risk).

RISK CONTROL ANALYTICS

We will review three major forms of risk control analytics: scenario analysis, economic capital, and risk indicators (early warning systems).

Scenario Analysis

One of the most fundamental techniques of risk control is scenario analysis. A scenario analysis is a top-down, what-if analysis that measures the impact that a certain event (or combination of events) will have on the enterprise. An example of a scenario analysis would be to assess the financial impact of market and economic conditions similar to the 2008 global financial crisis. A stress test is a form of scenario analysis focused on specific risk factor(s). Stress testing should be implemented in combination with regularly performed risk assessments, as well as on an as-needed basis. Stress testing should be tailored to the institution's unique combination of size, business model, and risk/return characteristics, and should be regularly evaluated to ensure its effectiveness and relevance.[1]

The stress testing framework should address the possibility of specific negative outcomes, including those resulting from severe turmoil in the capital markets and macroeconomic conditions. By incorporating a range of sensitivity and scenario analyses, and reverse and enterprise stress testing, stress tests can assess the risk impact of given scenarios on the capital and liquidity of the entire institution.

Stress tests are an important supplement to other risk management tools because they can help institutions to identify underestimated or previously unconsidered areas of vulnerability and risk. In order words, they allow institutions to quantify tail risks or loss estimations beyond those provided

by probabilistic risk models. They are meant to capture the impact on the enterprise given changes such as:

- The effects of interest rate movements (e.g., what impact might a 300-basis-point upward shift of the yield curve have on the enterprise?)
- Changes in the default rates in a portfolio (e.g., what happens if loan defaults increase by 20 percent?)
- A decrease in liquidity (e.g., what happens to our liquidity position if we have limited access to wholesale-funding markets for 90 days?)
- Changes in unemployment (e.g., what happens if unemployment rises to 10 percent?)
- Credit downgrade (e.g., what is the financial impact, including collateral requirements, if our credit rating is lowered two full notches?).
- The effects of movements in commodity prices (e.g., what happens if oil prices increase by 20 percent?)
- Changes in gross domestic product (GDP) (e.g., what happens if GDP falls by 5 percent?)

The results of stress testing are consequential enough for it to be a significant part of new regulations mandated by the Federal Reserve as well as the Dodd-Frank Wall Street Reform and Consumer Protection Act.

For example, the Comprehensive Capital Analysis and Review (CCAR), an annual process by which the Federal Reserve performs analysis of the capital adequacy of "U.S.-domiciled, top-tier bank holding companies (BHCs) with total consolidated assets of $50 billion or over," specifically requires stress testing as a part of capital analysis.[2] During the CCAR process, participating BHCs must submit proposals to the Federal Reserve which outline their plans for managing capital, adhering to specific minimum capital ratios, and meeting basic Basel III requirements (further details in Chapter 12). Should the Fed reject the BHC's plans, the BHC must then produce a revised version within 30 days, which is subject to further approval by the Fed.

In return, the Federal Reserve will supply the BHCs with stress test scenarios that include a broad collection of variables to assess the BHC's losses and resulting capital ratios. One such scenario comprises of a recession over a nine-quarter forecast period. Using past recessions as a basic model, this stress test forecasts the BHC's performance in the case that, for example, domestic and foreign GDP and house prices decrease by more than 20 percent, asset prices fall, and unemployment rises, among other stressed assumptions.[3]

The Dodd-Frank Act provided the legislative framework for the stress testing requirements discussed above. Enacted in October of 2012, the Act calls for both annual supervision by the Federal Reserve, as well as

semi-annual stress tests to be conducted by BHCs themselves (among other chosen financial institutions with more than $50 billion in assets).[4] To increase the comparability of the stress test results, the Federal Reserve requires all participating BHCs to project their earnings and capital ratios in three possible macroeconomic scenarios—a baseline, an adverse, and a severely adverse scenario. All three scenarios outline trajectories of real GDP growth, inflation, foreign exchange rate, interest rates, and asset prices for a total of 26 variables that determine economic conditions and activities over a nine-quarter forecast period.

For example, the severely adverse scenario details a decrease in real GDP by 5 percent, an unemployment of 12 percent, and a fall in home values by more than 20 percent.[5] BHCs are required to forecast their net income and equity capital for the specified time frame to assess their own capital standing under these specific conditions.[6] With a minimum tier 1 common ratio of 5 percent, all of the BHCs (save for Ally), passed the stress test, as demonstrated in the graph below (Figure 9.1).[7] The Federal Reserve also provides other shock scenarios for the BHCs deemed more susceptible to counterparty risks (such as those with heavier involvement in derivatives and other types of inter-bank leading and trading).

The results of these stress tests are meant to provide transparent information regarding the capital and liquidity resources of each institution to assess their ability to weather harsh macroeconomic shocks. However, it is important to note that scenario analysis and stress testing are not meant to

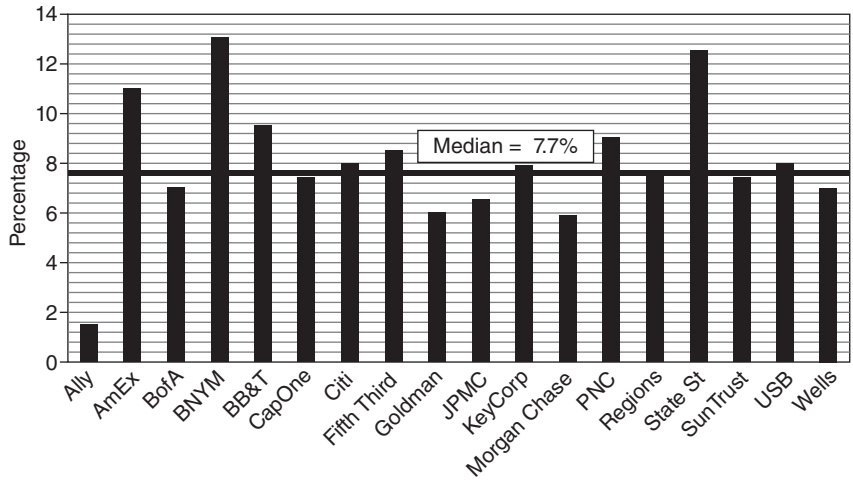


FIGURE 9.1 Stress Tested Tier 1 Common Ratio

capture the absolute worst that might happen (things can *always* get worse). Rather, they focus on the most severe events that seem plausible in the minds of senior management.

One of the shortcomings of stress testing is that it focuses on extreme, adverse events and does not capture the impact of less extreme, but more probable, adverse events. One analytic approach that addresses this problem is the simulation of a range of scenarios for a particular risk factor or set of risk factors, such as interest rates.

A specific and common form of simulation is Monte Carlo simulation. A computer performing Monte Carlo simulation is basically a machine for generating what-if scenarios—random scenarios based on parameters specified by the user. For example, a Monte Carlo simulation of interest rate movements could be constructed by using the historical interest rate volatility to parameterize each scenario. Monte Carlo simulation has been used in the measurement of a variety of different types of risk, including credit, market, insurance, and operational risks.

Economic Capital

Another common risk control measure is *economic capital*. At the enterprise level, economic capital represents the amount of financial resources that the institution must theoretically hold to ensure the solvency of the organization at a given confidence level and given its enterprise risk profile. Economic capital is therefore a function of two quantities: the organization's so-called solvency standard and its risk.

The solvency standard is the desired creditworthiness of an organization and can be inferred from its (desired) debt ratings. For example, an institution that has a target solvency standard of 99.9 percent would default, on average, only once every 1,000 years. This is roughly equivalent to an institution awarded an A rating by Standard & Poor's credit-rating service.

A higher solvency standard implies that more economic capital is held for a given level of risk: put the other way, the greater the risk that an institution bears, the greater the financial resources it must have in order to maintain a given solvency standard. A widely accepted theoretical framework for relating the amount of capital a financial institution needs to hold against a given level of risk is based on Robert Merton's model of default,[8] which essentially says the following:

- A company's shareholders own the right to default on payments to debt-holders, and will do so if the value of the firm's equity (net assets) drops to zero;

- Debt holders charge shareholders for default risk by demanding a spread over the risk-free rate on the funds they provide; and
- The probability of default is a function of the *current* level and potential *variability* (the probability distribution) of a firm's net asset value.

The calculation of an organization's economic capital is generally done bottom up. That is, the economic capital is calculated separately for each type of risk, and then aggregated, taking into account the effects of diversification, to come up with the overall economic capital for the entire enterprise. The basic process is as follows:

- Generate stand-alone distributions of changes in the enterprise's value due to each source of risk;
- Combine the stand-alone distributions, incorporating diversification effects;
- Calculate the total economic capital for the combined distribution at the desired target solvency standard; and finally
- Attribute economic capital to each activity based on the amount of risk generated by the activity.

Risk Indicators

A third form of risk control analytics is risk indicators, or early warning systems. These are designed to give timely information about changes in risk conditions to allow management to take appropriate action to mitigate risk. Early warning systems can use either external market data or internal data.

External systems make use of market and economic data to indicate changes in the amount of risk to which an institution is exposed. Data commonly used this way include interest rates, foreign exchange rates, credit spreads, unemployment rates, changes in GDP, the volatilities of these factors, and so on. This information can be monitored with respect to their levels and trends, as well as translated into the economic impact on an organization, such as increases in funding costs.

Internal systems make use of institution-specific data to indicate changes in risk levels. The risks that are being measured may be either tied directly to the bottom line (e.g., credit card default rates) or associated less directly with an increase in risk levels (e.g., increased concentration in the lending book, or increased line utilization which may indicate higher probability of customer default). In either case, advance warning will allow management to establish policies and procedures to reduce exposure to the specific risks identified by the early warning systems.

RISK OPTIMIZATION ANALYTICS

The goal of risk management is not to reduce an institution's risk to zero, or even to minimize risk. Without risk, there is no return. Rather, it is to ensure that the enterprise is well compensated for the risk that it takes, subject to the constraint that the risks taken fall within the institution's overall risk appetite. The risk optimization analytics discussed below can be used to help maximize returns relative to risks.

Risk-Adjusted Return on Capital

Risk-adjusted return on capital (RAROC) can be calculated for an institution as a whole, or separately for each of its business activities (e.g., by product, customer, or business unit). Since the amount of economic capital that is required to support each of the enterprise's activities is proportional to the risk generated by that activity, economic capital can be used as a standard measurement of risk. Combining the economic capital required to support the risks of an activity with the activity's expected economic returns yields a ratio that represents the amount of return the institution expects per unit of risk it takes:

$$\text{RAROC} = \frac{\text{Risk–adjusted Return}}{\text{Economic Capital}}$$

The risk-adjusted return is based on net income or expected return. RAROC using net income provides an indication of actual profitability, while the use of expected return provides a measure of normalized profitability. This is particularly relevant when applying RAROC to credit risk-related activities, since expected losses are often used in the calculation of return, rather than actual losses.

The primary use of RAROC is to compare the risk/return of different, and potentially quite diverse, business activities. This is particularly useful when capital is scarce and an institution needs a way to choose between investments. In addition, an institution can evaluate its RAROC against its cost of equity capital (Ke), to identify business activities that are adding shareholder value (RAROC is greater than Ke) and those that are destroying shareholder value (RAROC is less than Ke).

Economic Income Created

One disadvantage of RAROC as a performance metric is that it does not capture the *quantity* of return that an activity generates. For example,

suppose that a business unit currently has a RAROC of 25 percent, well above the parent institution's hurdle rate of 15 percent. If RAROC were the primary performance metric, the unit would not want to generate additional business that did not meet or exceed its current RAROC of 25 percent, as the additional business would move the average RAROC below its current level. This is obviously problematic, as the institution's management would like the subsidiary unit to pursue all opportunities that return the corporate hurdle rate of 15 percent or more.

It would therefore be desirable to use a metric that captures the quantity of return that a unit or activity generates in this case. Economic Income Created (EIC) is a risk optimization tool that can be used as just such a metric:

$$\text{EIC} = \text{Risk–adjusted return} - (\text{Hurdle rate} \times \text{economic capital})$$

Any business whose return on marginal economic capital is greater than the hurdle rate increases EIC. EIC is thus a better mechanism for setting performance targets and executive compensation payouts, as it clearly encourages business managers to pursue all above-hurdle, marginal growth opportunities (whereas RAROC targets can have the adverse effect of discouraging growth in businesses with high historical RAROC performance).

Shareholder Value and Shareholder Value-Added RAROC and EIC

Shareholder Value and Shareholder Value-Added RAROC and EIC are measures of performance in a given period of time. While they give a sense of performance in the current period, they do not directly measure the economic value of businesses over the longer term. Shareholder value modeling provides the translation from these annual measures to measures of the *intrinsic* economic value of a business as an ongoing concern.

Shareholder value (SHV) models must capture the full economic value of a transaction or business activity, which is to say the *present* value of all future cash flows. Shareholder value-added (SVA) measures the degree to which shareholder value exceeds the value of the capital invested. Borrowing from the popular dividend discount model for equity analysis, formulas for these two measures are shown below:

$$\text{SHV} = \text{Discounted Value of Cash Flows}$$

$$= \text{EC} \times \left(\frac{\text{RAROC} - \text{g}}{\text{Hurdle} - \text{g}} \right)$$

$$\text{SVA} = \text{Discounted Value of EVAs}$$

$$= \text{EC} \times \left(\frac{\text{RAROC} - \text{g}}{\text{Hurdle} - \text{g}} - 1 \right)$$

The new factor introduced by SVA analysis is the measurement of the future growth prospects of a business, *g*. This is inherently difficult to estimate, particularly for time horizons well into the future. While it would be more useful, and accurate, to use detailed cash flow projections for each unit, most organizations employ a medium-term horizon of three to five years in determining the growth rate. Note that the ratio involving RAROC, hurdle, and growth (*g*) in the SHV equation is conceptually similar to a market-to-book ratio and can thus be benchmarked externally.

SVA is designed as a decision-support metric. At the firm-wide level, SVA analyses are generally used to support decisions about internal resource allocation, as well as decisions on acquisitions, divestitures, and joint ventures. SVA employs many of the same conceptual factors that are used in the construction of the performance metrics described above, but differs from them in that it captures both tangible and intangible changes in value.

For example, changes in regulation or competition that may affect the long-term growth prospects of a business may not affect its contribution in a recent period (as measured by EIC). However, they will alter its value contribution to the firm over a longer time horizon (as measured by SVA). So much for the models applicable at the enterprise level. Let's now review the models used in the evaluation of market, credit, operational, and insurance risks. Once again, volumes have been written about the technical details of these models. We will confine ourselves here to sketching out the properties of the various analytics, though the interested reader is strongly recommended to explore these subjects in more detail.

MARKET RISK ANALYTICS

Interest Rate Models

Broadly speaking, there are two uses for interest rate or term structure models: pricing interest rate-dependent instruments and interest rate risk management. In particular, such models are useful in predicting the

dynamics of cash flows that are contingent on interest rates. Such cash flows are often path-dependent (that is, they vary according to the behavior of interest rates, not just their level); a classic example is prepayment of mortgages.

Value-at-Risk Models

Value-at-Risk (VaR) is one of the most common forms of market risk measurement. There are three broad approaches to calculating VaR, each with its own strengths and weaknesses: the *parametric* approach uses volatilities and correlations of risk factors; the *Monte Carlo simulation* method uses a simulation model to generate a large number of possible outcomes; and the *historical simulation* technique uses previously observed price and rate movements.

The primary advantage of parametric VaR is that it can be calculated quickly and is computationally simple, which makes it useful when analyzing portfolios with many different assets and risk factors. However, it assumes that asset returns are linearly related to risk factor returns, and that the risk factor returns are normally distributed. Thus, parametric VaR ignores non-linear price sensitivities, such as gamma for options and convexity for bonds. In addition, parametric VaR models (usually) assume that price movements are normal. Both of these factors cause underestimations of the potential future volatility of portfolios.

Monte Carlo VaR, on the other hand, does not make the assumption that asset returns are linearly dependent on price. In calculating portfolio profit and loss, Monte Carlo simulates normally distributed future scenarios, with the variances of risk factor returns as a parameter, and uses them to re-evaluate the portfolio. More complex versions fully reprice the portfolio assets. As a result, Monte Carlo has some disadvantages; it is generally the form of VaR that takes longest to calculate, and it still assumes that risk factor returns are normally distributed.

Historical simulation VaR is the only method that removes both the assumptions of normally distributed risk factor returns, and asset returns that are linearly dependent on price. Under historical VaR, the daily fluctuations actually observed in risk factors in the past are used to simulate the impact on the valuation of a portfolio of assets. In doing so, historical VaR produces better estimates of the actual distribution of risk factor returns, using full repricing; however, it repeats the exact returns observed over some historical period. This means the model's predictions are based solely on market fluctuations that were actually observed and take no account of those that are possible (and potentially important) but have not actually happened. As such, historical VaR is not practical

for new securities or securities that have not been observed in stressed markets.

Asset/Liability Management Models

VaR models are suitable for portfolios that are composed of liquid instruments. However, illiquid portfolios and structural positions (such as a bank's natural asset/liability mismatch position) have some characteristics that make VaR models (particularly parametric VaR models) sub-optimal for risk measurement. These characteristics include longer liquidation periods due to low liquidity, non-linearity of customer behavior, and embedded options within the assets and liabilities.

Asset/Liability management (ALM) models represent an improvement over VaR for illiquid portfolios for several reasons. First, they allow more sophisticated interest-rate and foreign-exchange modeling. Monte Carlo and parametric VaR permit very unusual yield curve movements that are unlikely to occur in reality. Historical simulation may or may not suffer from this problem, depending upon how the simulation is constructed. ALM models generally use more sophisticated mechanisms for capturing yield curve behavior, such as inversion between short-term and long-term rates, and are therefore more likely to yield accurate results.

ALM models also offer better accounting than VaR for long holding periods. VaR models use a very short holding period and volatility measurement period (generally either a one- or 10-day holding period, with volatility measurement done daily). This approach makes sense for short-term trading exposures. However, there are long-term relationships between risk factors that may not manifest themselves in the short term. Issues such as the mean reversion of interest rates or covered interest rate parity for foreign exchange mean that the risk factors do not necessarily change in a purely random or independent manner. ALM models are generally parameterized over a longer horizon and are therefore more likely to capture the effects of long-term relationships between risk factors.

A final advantage of ALM models is better treatment of embedded options and path-dependent products. The bulk of traded products have relatively simple relationships to risk factors such as interest rates and foreign exchange rates. Illiquid portfolios, particularly the structural balance sheets of banks, may include asset and liability positions with complex relationships to risk factors. For example, assets such as U.S. residential mortgages effectively bundle prepayment options with debt, and as a result, have a relatively complex relationship to interest rates. ALM models are designed to capture this complex behavior and appropriately value the change in assets and liabilities due to changes in risk factors.

CREDIT RISK ANALYTICS

A large variety of analytics are available for supporting credit risk measurement. Most of the available tools focus on estimating the components of expected loss for individual credit exposures. These analytics include:

- Credit-scoring models, which estimate the expected default frequency of a borrower or counterparty at a point in time.
- Credit migration models, which focus on how the credit quality of exposures changes over time.
- Credit exposure models, which estimate the Loan Equivalent Exposure of credit transactions.
- Credit portfolio models, which assess the risk/return profile of a portfolio of credits and take the impact of diversification into account.

Credit-Scoring Models

One of the key inputs when measuring credit risk is the likelihood that a given credit exposure will default over a given period of time—this is often called the expected default frequency (EDF). The most common analytical tool used to perform this estimation is a credit-scoring model. There are three basic types of credit-scoring models: empirical models, expert models, and Merton-based models.

Empirical models are constructed by analyzing the historical default experience for similar credit exposures. For example, an empirical model might be based upon an analysis that uses income, outstanding debt, and length of employment to predict the default frequency of a credit card customer. Fair Isaac's FICO score is an example of an empirical model applied to a consumer borrower base.

Expert models attempt to capture the judgment of credit experts in the form of a model. In most cases, credit experts are senior individuals within the organization who are seen as having strong credit assessment skills. These models tend to be employed when the credit assessment process is considered to be complex and difficult, and/or when the analysis of a vast amount of quantitative and qualitative information is required.

Finally, Merton-based models use finance theory and market information to develop implied default rates of companies. Credit Monitor, a product developed by the KMV Corporation (now part of Moody's), is an example of a credit-scoring tool that falls into this category. The basic finance theory used by such models is the Merton model of a firm's capital structure described above: a firm defaults when its asset value falls below the value of its liabilities. A company's default probability then depends

on the amount by which assets exceed liabilities and the volatility of those assets.

Market information (such as the volatility of a company's stock price) can be used to estimate the volatility of a company's assets. By making some assumption as to the shape of the distribution of changes in asset value (assuming that they are normally distributed), we can estimate the probability that the value of a company's assets will be lower than the value of its liabilities. This probability is then used as the basis for assessing the probability that the company will default.

Credit Migration Models

The credit grading models described above are useful for developing a point-in-time estimate of the default frequency of a company or entity. However, credit quality can and does change over time. If an institution has long-term credit exposures, it is essential to understand how credit quality can change in the future.

The problem of estimating long-term default probabilities is complicated by the reality of credit migration—the fact that companies' fortunes and creditworthiness will very likely change from one year to the next. Thus the EDF, per annum, of a long-term exposure is not necessarily equal to the one-year EDF. It would only be the same if creditworthiness remained constant. Similarly, very short-term credits may also have different EDFs than one-year exposures.

The primary objective of credit migration models is to attach cumulative default probabilities over a number of years to internal grades. There are several ways of doing this, just as there are several ways to tackle the EDF-based calibration of a credit grading scale. These methods can be classified into three categories according to the way that the relevant data are used and/or sourced: the cohort study approach, the migration matrix approach, and the benchmarking approach.

Under the cohort study approach, the credit portfolio is divided into cohorts based on origination year, geography, and risk grade. Then, multi-year EDFs are estimated by using the multi-year cumulative default rates actually observed historically for different grades of credit. This is similar to the historical method of calibrating the one-year EDF, and suffers from a similar problem: there is frequently not enough reliable data. This is particularly true for longer time periods, as many grading scales have not been used consistently for very long. Nonetheless, the cohort study approach is often used by credit card and mortgage lenders because marketing programs and product features vary each year. These variations can have a material impact on the credit performance on each cohort.

Another way of estimating multi-year EDFs is through the use of migration matrices. The main idea is to avoid having to measure default rates directly by observing the rates at which grades change—in other words, the rates at which credits migrate between grades. Migration rates are much higher (and thus, easier to measure accurately) than default rates, particularly for higher-quality credits. Together with the previously calibrated EDFs for each credit grade, a table of migration probabilities implies a complete series of long-term EDFs.

This process is most easily described by example. To find the two-year EDF for an A+ borrower, for instance, we would first measure the probability that, within a year (or some other period), an A+ company will remain an A+ company (e.g., 85 percent). In addition, we need the probability that it will become an A (10 percent), the probability that it will become an A- (4 percent), and so on. The probability of default in the first year will be the two-basis point characteristic of an A+. The second-year default probability, however, will be the weighted average of the EDFs associated with each of the different grades to which the credit *might* migrate. The weights are assigned according to the probability that an A+ company will change to that grade in a year.

There are two approaches when it comes to going further than the second year. One is to repeat the same kind of analysis over longer time horizons (that is, to compare the current grades with the potential grades two or more years from now). Another is to develop a migration matrix that provides information on the probabilities of a borrower having a certain grade a year later, given its current grade. Neither approach is technically simple, but both can achieve satisfactory results.

Counterparty Credit Exposure Models

The trading of financial instruments, such as foreign exchange forwards, forward rate agreements, and swaps, often generates *potential* credit risk exposure. The credit risk is generated when market conditions move in one party's favor, and so the contracts that it has engaged in have a positive mark-to-market value, or replacement cost. If the other party to the trade (the counterparty) defaults and cannot honor its side of the contract, the first party is exposed to the current mark-to-market amount.

Because this exposure is contingent upon the default of a counterparty, a credit risk framework is usually used to evaluate the risk. However, unlike the many forms of credit risk where the exposure is known (such as term loans), the exposure to a counterparty is in this case driven by *market* risk factors such as interest rates or foreign exchange rates. Analytical models are needed to estimate potential exposure to a counterparty.

The simplest approach is to use a percentage of the notional value of a contract as the expected exposure for calculating credit risk, potentially varying by type of contract and term of contract. This approach is generally too simplistic, and can substantially misestimate risk. An improvement is to use the present market value of the contract, although this does not take into account the potential for greater (or lesser) exposure in the future. Fortunately, potential credit exposures for most (but not all) instruments can be calculated using formulas that take as inputs the volatility of the value of the contract and the maturity of the contract.

These formula-based approaches work well for single-payment contracts, such as foreign exchange forward contracts or forward rate agreements. However, they generally do not work well for multiple-payment contracts such as interest rate swaps. In these cases, a Monte Carlo simulation approach would be more accurate; in using a Monte Carlo approach, the expected and maximum credit exposures can be estimated given a large range of potential rate and price movements.

CREDIT PORTFOLIO MODELS

The credit risk analytic models we have described thus far in this chapter are focused on the assessment of individual credit risk exposures. In addition, credit portfolio models are used to aggregate the credit risk of individual exposures, and to determine how losses behave at the portfolio level. There are three general approaches to modeling credit portfolios: financial models, econometric models, and actuarial models. We will provide an overview of these models.

Financial and Econometric Models

Financial models such as the RiskMetrics Group's CreditMetrics and KMV's Portfolio Manager rely on the Merton model of a firm's capital structure. As described previously, this assumes that a firm defaults when its asset value falls below the value of its liabilities. A borrower's default probability then depends on the likelihood that the value of assets will drop below the value of liabilities, which in turn is a function of volatility of the value of those assets.

The asset value is usually modeled as lognormally distributed, which means that changes in asset value are normally distributed. The default probability can then be expressed as the probability of a standard normal variable falling below some critical value, representing the point at which the value of liabilities exceeds the value of assets. The distribution of possible losses on the portfolio is estimated through Monte Carlo simulation.

Econometric models such as McKinsey & Company's CreditPortfolioView attempt to model the default rate for a borrower (or group of similar borrowers) in terms of the behavior of macroeconomic variables. To put it simply, the default rate of each sector (representing a group of similar borrowers) is determined by changes in macroeconomic variables such as interest rates, gross national product, and so on. The portfolio loss distribution is again calculated by Monte Carlo simulation.

Actuarial Models

The CreditRisk+ model developed by Credit Suisse Financial Products makes use of mathematical techniques that are commonly used for loss distribution modeling in actuarial (insurance) literature. CreditRisk+ is based on an analytical, closed-form formula for default risk—in other words, a formula which takes average default rates and volatilities as inputs and provides a distribution of credit portfolio losses as the output. As such, it requires relatively little data and can be evaluated very quickly compared with the computationally intensive and slow Monte Carlo simulations used by the financial and econometric models. The main problem with this approach is that it assumes that the bank already has useful default data, which is not always the case.

It has been shown (by Ugur Koyluoglu of Oliver, Wyman and Company and Andrew Hickman of ERisk) that these models are largely equivalent—provided that their assumptions and input data are phrased in compatible ways. In practice, however, the models' incompatibility is not easy to overcome. A user might end up with quite different risk results when the same portfolio is analyzed using such dissimilar models. This can, in fact, be a useful way to pin down the real risks of the credit risk portfolio by quantifying its loss sensitivity to different parameters and assumptions.

OPERATIONAL RISK ANALYTICS

There are two basic approaches to estimating operational risk: top down and bottom up. The top-down approach generally applies to the entire enterprise, while the bottom-up approach analyzes operational risks generated at the activity level, which are then aggregated to determine a measure of operational risk for the enterprise. Let's examine these individually.

Top-Down Approaches

There are two different techniques that are employed in the top-down approach. The first is the use of analogs—a technique which first strips away

all specific risks that can be identified, such as business risk, credit risk, or market risk, while classifying any remaining risk as operational risk.

This estimated operational risk is then benchmarked against public companies whose operations are comparable to that of the enterprise. Since these public companies are often selected for their nature as pure play analogs of the business operations of the enterprise, the amount of equity necessary to support operational risk (adjusted for size differentials) can be based on these external benchmarks. For example, the equity required for the IT function can be estimated by benchmarking the equity levels of pure IT companies.

The second technique uses historical loss data to provide an empirical distribution of operational risk losses. A loss database is used as the basis for parameterizing this loss distribution, and is then scaled up or down to suit the size of the enterprise's operations.

Bottom-Up Approaches

One bottom-up technique for estimating operational risk is through self assessment. This is basically a business- or expert-based risk assessment of a particular activity, as it includes estimates of probability, severity, and control effectiveness. Risk assessment will be discussed in more detail in Chapter 23.

Another bottom-up technique is to build a model of the cash flows of an activity or operation. The inputs to the model are risk factors that affect the profitability of the activity, and Monte Carlo simulation could be used to generate a distribution of value for the activity. These types of models are effective in situations where business relationships can be explicitly tied to external market risk factors. An example of a business for which this bottom-up approach works well is mortgage origination, where the amount of volume that is generated by the business unit can be directly tied to changes in interest rates.

GRC SYSTEMS

The Sarbanes-Oxley Act of 2002 (SOX) has its roots in the Enron and WorldCom disasters—both of which inspired scrutiny of federal securities laws, financial reporting practices, and internal controls at an unprecedented level.

Essentially a corporate-fraud bill, SOX places much stricter guidelines on corporate self-assessment measures in an effort to bolster the public's failing confidence in the corporate governance and financial systems of

publicly traded companies. President Bush, who signed the Act into law on July 30, 2002, deemed it "the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt."[9] Notably, SOX requires that a regulatory board be given the power to monitor the accounting industry with the aim of rooting out corrupt executives.

As part of the effort to meet these stringent new measures, many companies have developed governance, risk, and compliance (GRC) systems that integrate organization processes to capture a more holistic view of core and supporting functions. Section 404 of SOX mandates that public companies provide information in their annual reports with respect to the internal control structure and procedures for financial reporting. GRC systems support these internal control requirements by recording all material transactions from beginning to end, which ensures a certain level of transparency across business and financial activities.

The key feature of a successful GRC system is that it provides a large database of information with respect to business processes, financial accounting and reporting procedures, regulatory and policy requirements, and other documentation. As such, GRC systems can be useful in supporting the following processes:

- SOX compliance testing
- Internal audit planning and reporting
- Risk-control self-assessments
- Development of key risk indicators
- Enhancing operational risk controls, such as cyber security

The popularity of GRC systems has escalated since the inception of SOX, so much so that it has its own market; many vendors now provide advanced software products that automate governance, risk, and compliance functions. A recent report by Gartner outlines the basic capabilities of typical GRC system products:[10]

- *Controls and policy mapping*. GRC systems help organize the various policies and controls into a cohesive library that compares current company data with industry standards and regulations. The most useful aspect here is that the vendor provides the external information on the industry, which can save and time and resources for the client.
- *Survey capabilities*. This also includes vendor-supplied content on industry trends, to provide companies with a basis for comparison when using the GRC system in conducting internal surveys. Companies may find this handy when considering policy distribution and control assessments.

- *GRC asset repository.* Similar to the controls and policy mapping capability, GRC systems are able to organize information technology (IT) assets into systematic categories based on the business functions that they support. GRC systems also allow companies to extract data from external asset repositories.
- *Workflow.* GRC systems generally come equipped with vendor-provided workflow templates—though they also have workflow designing functions, to allow companies more flexibility.

In order to support the analytical models and systems discussed in this chapter, institutions need to establish the appropriate data and technology infrastructure and capabilities. This is the subject of the next chapter.

CHAPTER 10

Data and Technology

As discussed in earlier chapters, organizations of all types—both financial and non-financial—have, in recent years, become much more appreciative of the importance of risk in all its various incarnations. Quite apart from the arguments for risk management as a good thing in its own right, it is becoming increasingly rare to find an organization of any size whose stakeholders are not demanding that its management exhibit risk awareness.

Faced with this pressure, but also with a discipline whose successes are frequently intangible and non-intuitive—for example, reduced probability of a significant loss—management often turns to one of the few aspects of risk management that is easily measured in dollars and cents: investment in risk management technology. Chairmen hailing the benefits of such investments have for some years been a staple feature of financial institutions' annual reports; the trend is now repeating in the non-financial sectors.

This heavy investment is at least partially justified. We noted in Chapter 2 that it is critical to balance the yin and yang—soft and hard issues—if risk management is to be truly effective, and the hard side of risk management is inextricably intertwined with technology: for carrying out the analytics described in the last chapter, for gathering the data required as inputs to the analytics, and for reporting the data produced as their outputs.

But it is also easy for investment in technology to become an end in itself. Less emphasis has been paid to the value for money achieved in risk management technology projects—even though, in some cases, hundreds of millions of dollars have been spent with little to show for it. In this chapter, we'll consider the evolution and components of risk management systems and the keys to a successful implementation.

EARLY SYSTEMS

The first implementations of risk management systems were, in many ways, steps into the unknown. The boom in trading during the 1980s and 1990s led to sharply increased demand for systems that could price

instruments like bonds, equities, and derivatives quickly and accurately. The next stage was for systems that could carry out risk modeling of those individual instruments and trading portfolios—in other words, systems that implemented stress test, simulation, and value-at-risk (VaR) models described in Chapter 9.

Project managers were faced with the task of building these systems using huge amounts of data covering the terms and conditions of each of the instruments being analyzed, live market data, time series data for the construction of scenarios, and limits against which exposures might be compared. Most of this data was scattered, inconsistent, and error prone. The toughest to manage was the terms and conditions data: traded products are hugely variable and complex, especially when non-standardized products such as swaps and structured products are considered. All of this complexity is reflected in the terms and conditions that describe these contracts.

Project managers typically had to choose between two main data sources when gathering terms and conditions data. The first source was the accounting system, in which all of the holdings of the bank could be found. However, this typically stored only a subset of the attributes required for risk calculations. The alternative source was in the front office trading systems. All the attributes for each deal could be found here, but the deals were typically split over a proliferation of position-keeping systems and spreadsheets.

In general, in the earliest projects, decisions were made to extend the data stored in accounting systems to include all the attributes required for risk management, and then to source risk data from the back-office system. Conceptually, this approach makes sense. Why rebuild multiple interfaces to trading systems when the majority of the data is already available in a single location?

Unfortunately, this method hit two major problems. First, the process of extending the accounting system was often far more protracted than had been estimated, resulting in significant project overruns. Second, each time a new instrument type was traded, that instrument had to be implanted in the front-office system and mapped into the back-office system. Finally, the data model of the back-office system had to be extended and mapped into the risk management system—a lengthy process during which these new risks go unmeasured.

The basic problem was that project managers had tried to take advantage of the existing interfaces that had been built out of front-office systems. These interfaces had been designed for accounting purposes rather than risk management purposes, and so adapting them to risk management was a complex, extensive process. A new approach was required.

DATA MANAGEMENT

Data warehouses had achieved considerable success in the retail sector in the 1980s, where they had been used for a number of purposes, including the storage and management of customer information. The application of data warehouses to risk engine integration is conceptually appealing, a factor which helps to explain their significant, if short-lived, success.

The idea was as follows. Rather than extend the back-office system and all of the interfaces into the back office to transform risk data, why not simply build new interfaces into a custom-built database from which the risk engine could extract data for analysis? There were other clear advantages to this approach. By aggregating high-quality, clean, and comprehensive data into a single database, it would be possible to link other applications to the same database, such as performance measurement systems, customer relationship management systems, and even profit and loss (P&L) engines.

However, the need to aggregate all risk data into a single location was partly driven by the technical inadequacy of the risk engines. The novel nature of risk management meant that risk engines were typically built by financial engineers whose understanding of mathematical finance was, in general, considerably greater than their understanding of technology.

As a result, the risk engines were often structured so that all of the data had to be mapped into a single batch and the risk analysis carried out in a single run. Such applications have been described as monolithic black boxes. A more logical approach would have been to recognize that a risk analysis could be split into multiple components, each analyzing a subset of the book using consistent assumptions, with a final component aggregating the results.

Many financial organizations embarked on extremely ambitious warehousing projects, to the delight of software vendors and implementation consultants. The vast majority of these projects failed to live up to expectations; some of them just plain failed. There were three main reasons for this.

First, these projects were often technology-driven, with business users providing very little, if any, direction. In many cases, the projects had no clear business objectives. As a result, they consumed significant budget and corporate resources without producing tangible results. A second major problem was the time required to build and maintain the many interfaces with source systems. The third problem was the sheer ambition of the projects. Ultimately, the data types required for risk management are extremely complex and varied, and are not conducive to being stored in a single database.

The failure of data warehouse projects prompted some critics to liken the approach to boiling the ocean. An obvious reaction to the cost and time overruns in many data warehouse projects was to change the scope of the warehouse project. Rather than having a single warehouse attempting to hold all of the risk data in an organization, teams realized that a more effective approach was to implement a series of data marts, each of which resembled a mini-warehouse. Each data mart could then specialize in the data required for a single area of functionality.

Thus, rather than attempting to consolidate all data in a single location, a series of data marts would be set up containing subsets of data. One might hold market risk-relevant data from the trading room, for example, while another would hold credit risk information. A third would be set up to hold extracts from each of the two source marts to enable enterprise-level calculations. This approach reduced the scale of the database implementations to more manageable levels, although the extensive duplication of stored data magnified the scope of the reconciliation problem in many cases.

Data marts effectively solved the problem of warehouse projects overrunning due to lack of specific, clearly defined business objectives. They did nothing, however, to deal with the time taken to develop interfaces and to reconcile the data stored in the marts. Nor did they solve one of the essential problems of any risk system implementation (or indeed, any technology implementation). Namely: garbage in, garbage out.

Time series data, for example, typically contains a small amount of bad data. Corruption or poor data entry can result in the price of a stock that typically hovers around $45 being recorded one day at $450. This kind of error can cause significant problems in risk calculations, and so data-cleansing algorithms must be implemented to search out and fix such errors. These algorithms work either by comparing price data from multiple sources or by comparing a given value against historical ranges within user-defined tolerances.

Another example of the need for data cleansing is found in counterparty data. Most financial institutions store information about counterparties using a huge variety of names and codes. For example, Chase Manhattan Bank might be recorded in systems as Chase, Chase Manhattan, Chase Manhattan Bank, and a variety of other versions. In order to aggregate exposures to Chase Manhattan, the risk engine must understand that Chase and Chase Manhattan Bank are the same entity.

Several partial solutions have emerged to deal with data cleansing. The first class of solutions takes the form of clean data sources. These range from Interactive Data or Asset Control, who can provide cleaned and comprehensive databases of terms and conditions, through to vendors such as Olsen & Associates, Reuters, or Telekurs, who provide clean historical or live market

data. The second class of solutions comprises algorithms or interfaces for cleaning specific data types, for example, HMD Risk.

INTERFACE BUILDING

The majority of the time and effort expended on a reasonably planned risk management system implementation project goes into interface construction. If the risk data is being extracted from front-office trading systems, it will be necessary to build interfaces from each of the trading systems to the risk engine. In many of the early implementations there were few tools or packaged interfaces available to developers, so each had to be coded manually.

Each interface was made up of a number of distinct stages. First, a customized extraction program pulled the data out of the trading system—many trading systems do come with such extract interfaces, but these may need modification to provide all the data required for risk analysis. Second, the risk data must be transformed into the format required by the risk engine. While a coupon rate may be stored as "7% ANNU ACT/365" in a trading system, the same data might need to be reformatted to "0.07ANNACT-365" for a risk system. The rules for such a transformation have to be specified for every attribute of every piece of data going into the risk system.

Clearly, each interface is specific to a particular trading system and a particular risk system. If either is updated or replaced, the interface will have to be rebuilt. Similarly, if an organization starts trading instruments not previously coded into the interface, it will have to be extended. Problems arose because many early interfaces were poorly documented, so although they might have been well designed and understood by the original developer, they were often completely incomprehensible to anyone else.

In situations where the original interface builder had left the organization, interface modifications became extremely time consuming. To solve these problems, vendors of risk management systems started to sell mapping tools alongside their principal offerings. Simultaneously, many integration consultants began offering experienced resources and similar tools to aid the process.

Mapping tools typically provide several features to their users. First, and most importantly, they make interfaces transparent, so that it is relatively simple for future developers to extend an interface. Each of the rules required to transform a given attribute of a given instrument from a given source system is stored in a database and clearly documented. It is simple to locate, understand, and modify all of the individual rules. Second,

mapping tools can make interfaces reusable, since the transformation rules are specific to a trading system-risk system pair. Integration consultants have led the efforts to develop and resell such interfaces. Still, even with the support of mapping tools, risk management implementations still typically take many months, and sometimes years.

MIDDLEWARE

Another focus of efforts to reduce implementation time was a reduction in the total number of interfaces required. In a typical trading organization, there are a number of front office trading systems and a number of systems that require extracts from the front office. These include the risk systems, the accounting systems, management information systems, performance measurement systems, and more. The number of interfaces that must be built between each of these systems is obviously a function of the number of systems that provide data and the number that consume data. Once there are two or more providers and two or more consumers, it becomes more efficient to implement messaging-oriented middleware (MOM) between the consumers and providers.

MOM, of which Tibco and MQ Series are prominent examples, uses a variety of models for inter-process communication and offer significant benefits for enterprise risk management, including guaranteed delivery and interface transparency and robustness due to rule-based routing, error logs, and audits.

Conceptually, it seems reasonable that implementing MOM will save time and effort when there are two or more consumers and providers of data, since fewer interfaces will need to be built. In many cases, however, MOM projects did not enhance risk management projects, since there is often only one consumer for any given type of risk data. Even looking at the broader picture, where there are many consumers of front-office data, the implementation of MOM is still not always the most practical move. This is because the consumers of data usually require different data from each other so, in essence, the implementation of MOM falls victim to the same factors that sank many warehouse implementation projects.

Given that MOM provides more reliable delivery than other channels, it does ensure that the data in a risk system is generally more consistent with the data in the source systems. Ultimately, however, this is not perfect, and reconciliation will still be required as long as duplicate data is stored, or functionality duplicated, in two locations. Eliminating the need to reconcile the two sets of data requires a further advance: distributed architecture.

DISTRIBUTED ARCHITECTURES

Advances in application design during the 1990s made it feasible to build distributed software applications. These shift the processing from centralized application servers (which require the relevant data to be extracted from the source and moved to the server) to an environment where processing is moved out to the source data. This is achieved by using enabling technologies that hide the location of distributed objects from the application servers, which in turn allows the implementation of much more modular and scalable solutions. The implementation of these frameworks usually delivers many network services (e.g., security), which overcome the additional overheads of working within the distributed environment.

Component-based software models are nothing new but the ability to deploy applications rapidly in a distributed environment using these technologies is. It allows the development process to concentrate on solving the business problem rather than the complexities of implementation. These software tools effectively facilitate the encapsulation of source data with its processing logic into distributed objects that exist throughout the enterprise. This results in a single transaction—an insurance policy, for example—having a single point of persistence throughout the enterprise, rather than multiple ones with all the associated reconciliation issues.

Leaving the data management in the source system and moving the functionality there removes the need for complex data-reconciliation processes and changes the problem into one of synchronization: the need to ensure that data is viewed at the same time point and object version if the results are to be accurately aggregated.

An example of this would be a pricing component that produces a distribution of values for a set of transactions in a set of trading systems under a given set of scenarios. In order to aggregate these distributions correctly, one must ensure that the scenarios, the transactions included and the pricing algorithm are consistent across all the pricing calculations. These challenges can be addressed with standard technology components, rather than the bespoke business logic required in the centralized approach.

With distributed object technology, the implementation of the data-specific functionality is hidden from the application server processes. This delivers great scalability to the architecture, which can grow with the organization. Risk calculations, as we have learned, tend to be computationally intensive. The ability to distribute the additive components of a calculation across not only processors, but also machines, opens up whole new vistas of performance.

This architectural model implicitly requires the development of an enterprise-wide object model, but not an enterprise data model. From a data-centric view, we are still left with the business object mapping tasks that are specific to each source system. This may sound like a return to the cumbersome point-to-point interfaces of ancient times, but the interfaces here are not between applications but between source data and business object. These are usually less complex to implement and do not need to be forced into a single representation which meets all requirements.

KEY FACTORS FOR A SUCCESSFUL IMPLEMENTATION

The development and implementation of risk management systems to analyze enterprise-wide risks require substantial resources, yet they are a requirement for any enterprise risk management program. A successful effort can provide management with important information to help them control risks and make better business decisions. A failed effort can result in not only wasted money but also wasted time and organizational resources. There are key success factors that can increase the probability of success, including:

- Appointing a seasoned risk professional as the project leader, as opposed to leaving it to the technical staff
- Clearly defining the user requirements, including a prototype report that lays out the functionality and reporting specifications
- Establishing consistent standards for data and programs so that the risk management systems can communicate with other systems both inside and outside the company
- Using structured and modular programming techniques so that the risk management systems are scalable with new products and new methodologies
- Developing a clear project plan with specific responsibilities, milestones, timing, and expected performance
- Applying chunking methodologies where the project is broken into individual components that can be developed and tested
- Making the appropriate changes in personnel, vendors, and approach based on how the project is executed relative to expectations

One clear reason for the failure of many risk management projects is that they attempted to modify systems to address business problems that fall outside their intended core functionality. Examples include the misguided data warehouse projects and attempts to extend back-office systems to be a single repository of all risk data.

In many cases, this is because vendors have oversold the systems. Apart from the clear economic incentive, vendors often underestimate the tasks associated with extending their systems beyond their core competencies. The overselling process often takes the form of promised functionality that is in development. Potential buyers of such systems should pin down the core functionality offered by each system and discount future development. If the core competence of a system is market risk management for a trading room, then it should not be applied for enterprise level risk management, and vice versa.

Also, many businesses have chosen and attempted to implement systems that are inappropriate for their size, sophistication, and resources. Most risk management systems are designed for a specific group of target organizations—insurance risk management systems, for example, are very different from trading risk management systems.

Similarly, the systems designed for the large, multinational finance powerhouses who can dedicate a team of dozens to the implementation project are different from the systems and application service providers (ASPs) dedicated to smaller players with more modest budgets. Early on, the choice was between buying an off-the-shelf system from a vendor or building one in house. Typically the largest institutions built in-house while the majority bought vended systems. That choice has now evolved into a buy-and-build versus ASP choice. The largest players have the budgets to buy sophisticated risk engines, which come equipped with toolkits that allow limited amounts of extra development. The majority of financial and non-financial institutions may attain superior service in a fraction of the time by leveraging the implementations already carried out by ASPs.

Another critical factor is that a risk management system is unlikely to succeed unless it has the backing of senior management. Risk management systems by their very nature touch on a large number of businesses. Such systems are politically sensitive, since the performance measurement and remuneration methods of many institutions are linked to parameters set in the system. As such, it is essential to secure the support of senior management.

Fortunately, this is relatively simple. It is fairly straightforward to provide approximate risk results from relatively little effort—the first 20 percent of the implementation venture can yield enough information for senior managers to make informed strategic decisions. That opens the way for further, more detailed work.

CHAPTER 11

Stakeholder Management

In order to appreciate the significance of good stakeholder management, we need only reflect on the high turnover rate of customers, employees, investors, and other stakeholders at a company. On average, U.S. companies lose half of their customers over five years, half their employees over four years, and half their investors in less than *one* year.[1] These high turnover rates have an enormous impact on a company's profitability.

When people think about a company's stakeholders, they often think only about those who hold its equity, and perhaps those who hold its debt. However, a truer picture is that any group or individual that supports and participates in the survival and success of a company counts as a stakeholder. The obvious stakeholders are employees, customers, suppliers, business partners, investors, stock analysts, credit analysts, and special interest groups. Regulators should also be included if regulatory approvals and examinations are critical to an organization's business success—as, for example, in the financial, energy, and pharmaceutical industries.

Stakeholder management should involve providing key risk information to these stakeholders. The board of directors and regulators need to be assured that the company is in compliance with internal policies and external laws and regulations. Stock analysts and rating agencies are increasingly asking for risk management information on a company's investment and derivatives activities. For financial institutions and other complex organizations, they may even request line-of-business information with respect to profitability and risk. Institutional and individual investors need financial and risk information to make the appropriate investment decisions. The informational needs of key stakeholders are becoming more complex, and management must respond to improve risk transparency to these groups.

In stakeholder communication, it is important to bear in mind the unique needs of individual groups during the development of risk management presentations and reports. For example, boards of directors need summary information that highlights key risk information about the

company's compliance with regulations and board-approved policies. Stock analysts are more concerned about return on equity capital, so they need risk-adjusted profitability information—ideally by line of business to help facilitate comparisons with their own models. Rating agencies require information about capital plans and underlying risk exposures (particularly risk concentrations) in order to determine the relationship between a firm's risk taking and capitalization. Regulators are tasked with ensuring the safety and soundness of regulated entities in the context of the entire industry, which means they should be supplied with information about economic capital, risk management controls, and proper disclosure.

Each of these groups is essential to the success of the company, so the company must communicate relevant information to each group and ensure that it is taking steps to make sure that their particular needs are being met. According to a 2013 PwC global survey, 80 percent of CEOs said that customers and clients have the most significant influence on business strategy.[2] This was followed by government and regulators (50 percent), industry competitors and peers (45 percent), creditors and investors (38 percent), and employees (36 percent). It is clear that key stakeholders have a significant influence on business strategy. By extension, they should have a significant influence on risk management.

The needs of boards of directors and investors are discussed in more detail in Chapter 5 on corporate governance. In the rest of this chapter, we will discuss the risk management requirements of six key groups of stakeholders—employees, customers, regulators, rating agencies, shareholder service providers, and business partners.

EMPLOYEES

Employees should be viewed as major assets of a company, especially in those that depend heavily on intellectual or human capital. A company seeking to extract the maximum value from its employees must carefully manage both upside and downside risks throughout the duration of an employee's tenure with the firm, beginning with recruiting and ending with the employee's retirement, termination, or resignation.

Companies stand to gain more than warm feelings if they get it right. In 2011, *Fortune* magazine found that firms listed in its "100 Best Companies to Work for in America" outperformed their peers in cumulative stock returns by around 229 percent over a span of 14 years, starting from 1998.[3] As such, effective employee management not only saves unnecessary cost due to employee turnover, but also generates value for the company and its shareholders.

Employee turnover is no longer just a question of hiring and firing. Companies today have to manage an increasing number of free agents—individuals who see themselves less as employees and more as hired guns. These free agents may or may not be on the payroll; what is important is that their incentives are not automatically aligned with those of the company. These individuals are having an increasing impact on today's working world. In 2011, more than 40 percent of the American work force—at least 63 million people—consisted of free agents, defined as those who work for themselves, or could if they wished.[4]

Finally, companies operating in unionized industries have to face additional risks specific to unions—strikes, wage contracts, and morale issues. Union strikes upon contract renewal have become more prevalent in recent years, particularly in the airline and auto manufacturing sectors. Such incidents are both disruptive and costly, since strikes not only disrupt a firm's operations, but are also likely to destroy workers' morale and damage the company's image. For example, the 54-day strike of General Motor workers in 1998 caused plants to shut down and halted production; the strike cost GM $2.2 billion in lost sales, and may have taken an even greater toll over the long term, due to losses in market share and reputation.[5]

It is important to acknowledge that employees' needs and employers' desires do not necessarily match. Since employees have a high impact on business profitability, it is important to manage them effectively. This might seem obvious, but Peter Drucker succinctly captures the difficulties of this concept:

> All organizations now say routinely, "People are our greatest asset." Yet few practice what they preach, let alone truly believe it. Most still believe, though perhaps not consciously, what nineteenth-century employers believed: people need us more than we need them. But, in fact, organizations have to market membership as much as they market products and services—and perhaps more. They have to attract people, hold people, recognize and reward people, motivate people, and serve and satisfy people.[6]

We can consider employment as a series of stages:

- Recruiting and screening
- Training and development
- Retention and promotion
- Firing and resignation

There are different needs at each of these stages, and different employee management strategies are therefore required.

Recruiting and Screening

First, companies face the challenge of hiring the right employees. Employees' skills, experience, attitude, and potential determine their performance and productivity, and hence their contribution to the profitability of the firm. The risk of not hiring the right employees is tremendous. In an extreme case, such as that of a rogue trader, one mistake in hiring can bring down an entire company. For many years, companies such as Fidelity Investments and Disney have instituted background checks as part of their pre-employment screening process. Today it has become standard practice for even small to midsize firms.

Many companies would benefit from putting more resources and emphasis into recruiting. As the job market has become more competitive, companies have had to take more time and effort in hiring the right employees, who spend less and less time at any given company. The logical conclusion of this is the rise of the free agent, who may be integral to a company's operations, but may work for a number of different employers in quick succession, or even simultaneously. Not surprisingly, compensation is often cited as the top incentive for employees; however, other benefits should be considered as appropriate, and can make a real difference in hiring where cash alone cannot.

Training and Development

If hiring the right employees is important, keeping them is crucial. Employee turnover is costly; not only may valuable people, skills, and information be lost, but they may be lost to competitors. Then, of course, there is the cost of recruiting and training new employees. According to one study, the cost of replacing a worker is somewhere between 1 and 2.5 times the salary of the open position; the more sophisticated the position, the higher the cost.[7]

Training offers value to both employees and employers. In addition to on-the-job training, Andersen Consulting (now Accenture), the world's largest consulting firm, spent around $600 million, that is, 3 percent of net revenue, on formal continual learning programs for its consultants in 2012.[8] Some firms go beyond job-related learning programs. The grocery chain Wegmans Food Markets offers lifestyle and wellness programs to its employees, engaging more than 2,000 employees in a free smoking-cessation program that was first implemented in 2009.[9] Career development is also important. It provides a direction that an employee can follow and a goal for which he or she is motivated. With proper implementation, such programs can improve retention, productivity, and morale.

Retention and Promotion

According to *Fortune Magazine*, "swimming pools and surging pay may give employees a lift, but continual training and humane treatment get the best ones to stick around."[10] In addition to the training and career development discussed above, companies have to value and recognize their employees. This may include a culture of professionalism among co-workers and subordinates, appropriate delegation of responsibilities and project ownership, and awards and public announcements.

In the words of former General Electric boss Jack Welch, "you have to get rewarded in the soul and the wallet."[11] Promotion has to be based on meritocracy and not bureaucracy. The talent pool at GE is constantly refined by promoting the best performers and weeding out the worst. Talented executives are also nurtured in a rigorous meritocracy, where performance is lavishly rewarded and failure mercilessly punished.

Firing and Resignation

Massive layoffs reduce company morale and increase employee resignation. Managed firing, on the other hand, can increase employee motivation and improve company performance. At GE, for example, the company gets rid of the least effective 10 percent of its workers each year.[12] Leading consulting firms are increasingly adopting the up or out practice. If employees do resign, companies should find out why, by use of tools such as exit interviews. While negotiating with departing employees in order to retain them is a highly desirable goal, a number of studies have suggested that the use of counteroffers often do not yield the expected benefits. Therefore, companies should leverage information gathered in exit interviews so they can identify and fix the root causes of employee discontent.

CUSTOMERS

People may be a company's biggest asset, but not many in business would claim that their prime focus was on anything but their customers. After all, a company cannot survive without customers; hence there is obviously a great need for customer management.

Despite this, customer turnover is extremely high in most industries: on average, U.S. corporations lose half of their customers every five years. At least part of the reason for this is that many corporations do not really embrace customer management as a central concern, and many CEOs still take a primarily sales- or product-driven perspective on their businesses.

This may not continue to be a viable approach as customer power increases—a trend that many pundits expect to be an inevitable consequence of e-commerce and social media.

There are numerous aspects and strategies of customer management. We will discuss some of the major ones relevant to risk management here:

- Acquisition and retention
- Loyalty and satisfaction
- Knowing the customer
- Handling crisis

Acquisition and Retention

It is essential that a business should attract new customers and even more crucial that it keeps them. Even small differences in customer retention can translate into large shifts in a company's competitive position—particularly when it can cost five times as much to acquire a new customer as to retain an existing one.[13]

Long-term customers are profitable for other reasons, as well. For instance, they buy more, are less price-sensitive, and bring in more new customers than recently acquired customers do. In some industries, reducing customer turnover by as little as 5 percent can increase profitability by more than 50 percent.[14]

Good customer management does not mean that a company should attempt to obtain *all* possible customers in an effort to maximize revenues. Rather, companies need to identify and retain the *right* customers, who will help the company to increase its overall profitability, and not necessarily total revenues.

Consider a supermarket chain—at first sight a volume business, if ever there was one, which makes winning customers seem all-important. However, not every customer is profitable to the store. In fact, even customers who buy a great deal are not profitable if they "cherry-pick"—seek out deeply discounted items. The supermarket doesn't particularly want to retain these customers' business and so it might, for example, increase its range of luxury goods to attract shoppers who do not mind paying a premium, and scale back discounting campaigns.

Loyalty and Satisfaction

Customer retention is one result of effective customer relationship management—or, to put it another way, of customer satisfaction. Not only does a company lose the business of dissatisfied customers (normally to

competitors) but it may also lose the business of the potential and existing customers that the dissatisfied customers warn off.

A 2009 survey conducted by Genesys states that "nearly two-thirds of consumers who have ended relationships turn to a competitor," which substantiates the importance of maintaining a high level of customer satisfaction.[15] In the United States, firms reported an aggregate loss of more than $80 billion as a result of customer disatisfaction.[16] The financial sector seems to be the most adversely affected industry, with a reported loss of more than $44 billion.[17]

Ensuring customer satisfaction is not just a question of protecting against negative consequences. On the contrary, customer satisfaction positively creates shareholder value. In 2007, researchers at the University of Michigan found, using data from the American Customer Satisfaction Index, that companies with the highest customer satisfaction ratings beat the S&P 500 by more than 106 percent in terms of stock returns.[18]

Unfortunately, customer satisfaction does *not* correlate well with customer loyalty: a customer may be satisfied but still leave. As many as 85 percent of customers who defect have nonetheless been satisfied by the prior relationship.[19] Clearly, it is not sufficient just to attain high levels of customer satisfaction. What's also important is whether customers feel they have received enough value to keep them loyal.

Consider the American car industry: while it has a general customer satisfaction index of about 80 percent, the customer repurchase rate is significantly lower, ranging from about 30 to 40 percent for industry leaders such as Toyota, Ford, and BMW.[20] Loyalty is better measured in terms of customer retention and rate of repeat purchasing. Delivering zero-defect products is not enough in today's business: understanding customers' needs and satisfying them are pre-requisites for success.

Know Your Customer

Know your customer is a variant on know your business, the first lesson learned in Chapter 2. Companies that know their customers and act strategically on that knowledge can improve customer satisfaction and retention. Listening to customer opinions through a consumer hotline or surveys is one way to ensure that customers' voices are heard; data mining is another.

Amazon.com, for example, collects customers' purchasing behavior, stores it in a giant data warehouse, and analyzes it to provide more personalized service to each customer. Comparison of multiple purchasers' orders allows it to recommend other books that customers may be interested in after only their *first* purchase at the web site.

Just as with other business issues, it is important to know how far to go. Privacy is becoming an increasingly significant issue; if information is used improperly or left unprotected, knowing customers *too* well may introduce the risk of unnecessary losses and lawsuits.

Handling Crisis

Crises can occur no matter how efficient a firm's risk management—this should not be a cause for despair. Every crisis contains within itself the roots of failure, but also the seeds of success.

Consider Johnson & Johnson's Tylenol poisonings in 1982 and 1986. Each of these incidents cost the company more than $100 million directly, and could have cost it much more in reputational damage. However, J&J's swift responses allowed the company to turn these tragedies into opportunities, including setting industry standards for safety features in customer goods packaging. Customers, along with the general public, regarded Johnson & Johnson more highly *after* the incidents.

The keys to crisis management are to make contingency plans in advance and to avoid compounding the problem by trying to cover it up or deny responsibility. If a crisis occurs, the company must act fast, be honest, and keep customers and the general public informed. Today, it is no longer realistic to believe that the truth will never come out, or that financial damage can be postponed indefinitely; attempting to cover up a debacle may result in greater reputational damage to the company than openly admitting any mistakes that have been made. The company's response should focus on long-term benefits rather than on minimizing immediate losses.

REGULATORS

One stakeholder group that has become increasingly important for firms across most industries is that of the regulators—especially after the financial crisis of 2008. Some argue that the fear caused by the most recent economic turbulence has caused a wave of overzealous regulation that smothers rather than protects, heavily burdening U.S. companies that are used to a more laissez-faire attitude in regulation. Others argue that the lack of regulation, or effective regulation, is what allowed the financial crisis to happen in the first place. Among the most highly regulated industries are financial services, pharmaceutical companies, healthcare companies, and energy firms (particularly those that deal in nuclear energy).

In the aftermath of the 2008 financial crisis, and the new regulatory requirements, boards are taking a much more active role in risk oversight.

Recent surveys have indicated that risk management has replaced accounting issues as the top concern for corporate boards. Moreover, boards are more focused on risk areas that may have not received sufficient attention in the past. For example, a study of CEOs conducted by PwC in 2009 revealed "70 percent of CEOs in the United States and around the world said their boards were more engaged in assessing strategic risks as a result of the crisis."[21]

The new regulatory requirements have mainly focused on risk management practices, executive compensation programs, capital requirements, and disclosure rules. Consider the 2010 updated SEC disclosure requirement, which mandates that companies disclose the role of the board with regards to risk management in their proxy and annual statements. This new requirement is an attempt to enhance market transparency into the governance and risk management practices of publicly traded companies. In addition, the SEC requires companies to provide a risk assessment of their compensation programs.

The Dodd-Frank Act, also of 2010, was designed to target the root causes of the financial crisis; namely, the lack of transparency, the taking on of excessive risks, and the too-big-to-fail conundrum. While its objectives are commendable, the document itself is an unwieldy 848 pages long. *The Economist* wryly quips that the only people who have ever read the document in its entirety are "[their] correspondent in New York" and the Chinese government.[22] The bulk and complexity of the Dodd-Frank Act, and similar regulations, highlight the tendency that some lawmakers seem to have in trying to establish a rule for all potential issues. Critics of rules-based regulations argue that they are costly and ineffective, and suggest that "principles-based" regulations (similar to those in Canada and Europe) are more useful.

Regulators have particularly scrutinized the banking industry—banks are now required to hold more capital and liquidity reserves, and are also subject to new regulatory bodies, such as the Consumer Financial Protection Bureau. Other new requirements for banks include more stringent stress testing and a living will requirement (essentially an orderly liquidation plan).

The new regulatory environment has created significant challenges for banks. From an enterprise risk management (ERM) perspective, the allocation of economic capital is one of those challenges. In the past, economic capital levels calculated by internal models were almost always higher than regulatory capital requirements, but now, we often see the reverse. What are banks to do? Do they continue to allocate economic capital as per their business needs, or do they allocate regulatory capital and simply treat the excess as cost of doing business? Another challenge is how to balance the need to fulfill regulatory requirements against what's best for the company

in terms of sound business practices. As discussed throughout this book, the rationalization of risk, audit, and compliance activities is one of the key benefits of ERM. This rationalization has become even more critical in the current regulatory environment.

The largest banks in the United States are further strained by the need to address too-big-to-fail concerns; after the financial meltdown of 2008, neither regulators, lawmakers, nor the general public want to see massive bank bailouts in the future. Interestingly, some banks are not waiting to see what the regulators will come up with, but instead are moving actively to shape regulation while it's still in the works. For instance, in May of 2013, a group of banks, including Wells Fargo & Co., Bank of America Corp, and Citigroup Inc., presented their own proposal on the amount of equity and debt they would be willing to hold against large bank failures. They would agree to holding "combined debt and equity equal to 14 percent of their risk-weighted assets."[23] Since this is a lower level than the 15 to 16.5 percent mandated by international requirements, it remains to be seen whether or not the regulators will concede to the banks.

RATING AGENCIES

The importance of ERM as a criterion for credit ratings from external rating agencies has become visibly more relevant over the last decade, particularly in the years since the financial crisis. This makes intuitive sense—a credit rating represents the probability of default or the relationship between capital and risk. ERM provides organizations with enhanced capabilities to protect its capital base from unexpected loss. Rating agencies and bond investors should be concerned not only about the accuracy of the credit rating but also the durability of that rating. In 2005, Standard & Poor's (S&P) developed a series of ratings criteria related to ERM practices. Through this ERM evaluation, S&P rates companies as (in order of superiority) "excellent," "strong," "adequate," "adequate with strong risk controls," "adequate with positive trend," or "weak."[24] This rating process consists of a comprehensive examination of the different aspects of an ERM strategy including "risk management culture, risk controls, extreme-event management, risk and capital models, and strategic risk management." The ratings of each subcategory are combined to estimate an overall rating on the firm.[25]

First, S&P examines the risk management culture at the firm. It looks for indications of how large a role risk management plays in the decision making process by evaluating the governance structure, the overall tolerance for risk, the role of a risk executive, and the caliber of the risk management professionals at the firm, amongst other aspects.[26]

When evaluating the risk control processes for a firm, the rating agency determines how well the firm identifies, monitors, and manages different types of risk, as tailored to each firm. These risk areas include credit, market, insurance, and operational risk.[27] In addition, S&P examines a firm's extreme event management in terms of their stress-testing framework, considerations of a wide spectrum of possible adverse events, any early-warning indicators, and a regularly practiced extreme-event management process.

Finally, during the examination of a firm's strategic risk management framework, S&P assesses the firm's methods for strategic asset allocation, product risk and reward, optimizing risk-adjusted results, determining necessary adjustments to dividend payments, as well as a retained risk profile. In addition, S&P considers a firm's approach to risks that are currently immaterial but could affect a firm in the future—these risk areas could arise, for example, as a result of changes in regulation.[28]

Did companies with higher ERM ratings from S&P perform better during the global financial crisis? S&P addressed this question by examining the stock price performance of 165 North American and Bermudan insurance companies that it had provided with ERM ratings.[29] Overall, companies with superior ERM ratings performed better in both 2008 and 2009. For example, the average stock price of excellent ERM firms dropped by about 30 percent in 2008, compared to an average stock price decline of about 60 percent for weak ERM firms. In 2009, the average price stock of excellent ERM firms recovered by about 10 percent, while the average stock price of weak ERM firms continued to decline by about 10 percent.

SHAREHOLDER SERVICE PROVIDERS

As individual and institutional ownership of companies expands, firms that provide professional advice and other services have emerged to cater to this vastly important group of stakeholders. Institutional Shareholder Services (ISS) is a global leader in the provision of corporate governance solutions, advising organizations that have shares in multiple companies (such as hedge funds and mutual funds) on how to cast their votes. CtW Investment Group, another such company, works with union-affiliated hedge funds and "[enhances] long-term shareholder returns through active ownership."[30]

Both companies have considerable influence in the companies whose shareholders they advise. As required by the Dodd-Frank Wall Street Reform and Consumer Protection Act, public companies must now hold "an advisory vote on executive pay."[31] This greatly enhances the powers of proxy advisory companies like CtW and ISS, so much so that when ISS

recommends "in favor of a proposal . . . shareholder vote for that proposal [increases] by 15 percentage points."[32]

In a specific case, in April and May of 2013, CtW put tremendous pressure on both Goldman Sachs and J.P. Morgan by pushing forward proposals to split the role of CEO and Chairman. These proposals were ultimately suspended after negotiation between CtW and the two investment banking giants. The roles remain combined for them, though CtW director Diet Waizenegger says that he does not mean to completely back down just yet.[33] Notably, CtW's proposal for J.P. Morgan was also supported by "two major proxy advisory firms—Institutional Shareholder Services and Glass Lewis."[34]

The actions of CtW, ISS, and Glass Lewis reflect the movement of U.S. corporate culture toward greater board independence—this shift is not, by any means, limited to the financial sector. After the death of co-founder Steve Jobs, technology behemoth Apple, which previously did not have a chairman position at all, created one that was distinct from the CEO role for Arthur Levinson. Similarly, in early 2012, Myron E. Ullman III, who had served as both CEO and chairman of J.C. Penney, ceded the role of chairman to Thomas J. Engibous, an outside board member.

The number of companies that have split the CEO/Chairman role has grown by 15 percent since 2006—a 2012 survey conducted by Russell Reynolds Associates demonstrates that 44 percent of S&P 500 companies "now have separate executives holding the chairman and CEO roles."[35] Board independence is enhanced significantly with separate roles for CEO and chairman that allow for greater transparency regarding the CEO's actions. An independent chairman is able to drive the board agenda and provide more independent monitoring of executive management performance. CtW and other companies hold a remarkable amount of sway over the nature of corporate culture, which makes it important for companies to maintain good relationships with them.

In late 2011, ISS expanded the factors it considers in recommending withheld votes (or votes against directors) to specifically include material failures of risk oversight. ISS's 2012 annual survey revealed that for issuers, the second biggest concern was risk oversight,[36] so in 2012, ISS then further updated its policy by adding risk oversight as a consideration with regard to when votes should be cast for directors, committee members, or the entire board.

As of early 2013, ISS is updating its scoring methodology for governance related risk to focus on quantitative measures that identify "correlations between governance factors and key financial metrics."[37] ISS will give firms a numeric score on their governance-related risk based on its corporate governance with respect to the "board of directors, executive compensation,

audit, and shareholder rights."[38] Considering ISS's significant influence over publicly traded companies, this adjustment greatly underscores the growing importance of the role of the board in ERM (see Chapter 22 for further discussion).

BUSINESS PARTNERS

Strategic alliances have become a critical tool for almost any company operating in today's fast moving, networked economy. An alliance can help a company to speed up product cycles, obtain access to a new market, share the financial risks of developing a new technology, or profit from economies of scale.

Many companies have jumped eagerly onto the bandwagon, with the number of strategic alliances growing by 50 percent in the past three years.[39] However, there are abundant risks inherent in striking alliances. Consider that 40 to 60 percent of alliances ultimately fail to achieve their goals[40] and 70 percent of joint ventures end in a sale by one of the partners.[41] Failed ventures waste a company's resources, causing them to fall behind competitors and sometimes lead to reputational damage. There are other perils to the alliance approach, too, including the risks of loss of intellectual capital, conflicts of interest, and legal disputes over intellectual property rights.

How can the potential pitfalls of strategic alliances best be avoided? Careful attention must be given to risk management at each stage of the alliance process:

- Evaluating the pros and cons of an alliance
- Finding the right partner
- Monitoring progress as time goes on

Evaluating an Alliance

All alliances should be formed with a specific, value-creating goal in mind. They should never be born of desperation. For instance, some alliances are executed in the hope that a stronger company can be used as a crutch; this is likely to lead to the weaker company being bought out by the stronger at an unfavorable price. Others link one weak company with another weak company in the hope of magically becoming more competitive, which is likely to turn into a case of the blind leading the blind.

Of course, all of these goals can be achieved by means other than strategic alliances, including internal development, market-based transactions,

or vertical or horizontal integration. Hence, not only must the goal be achievable through a strategic alliance, but it must be *best* achieved through a strategic alliance.

In general, an alliance is suitable in cases where a considerable amount of control is needed (which could not be achieved through market transactions), but where internal development would be expensive or difficult. Alliances, for example, allow potentially incompatible partners to work together without the integration risks of a full-blown merger.

On the other hand, they also carry the potential for loss of intellectual capital. Alliance partners may be very close in one area of their business, but this may be a temporary or narrow arrangement. Before entering any alliance, a company should assess the degree of risk involved in sharing information with their prospective partner, which will vary depending on the nature of the intellectual capital, the capabilities of the alliance partner, and the nature of the alliance.[42]

An example of an instance where an alliance would likely be the best solution is the case of an auto manufacturer determining how it can best obtain the more than 15,000 parts needed to assemble a car. Building the parts internally, buying them in the open market, or buying up the part manufacturers would all be unwieldy, uneconomic, and impractical solutions. An alliance, however, allows the car and parts manufacturers to share information, where advantageous, and establish a reliable stream of transactions, while leaving the management of individual processes to the teams that understand them best.

Finding the Right Partner

Choosing an inappropriate alliance partner is a virtually certain route to a failed alliance. Since an alliance partner must be compatible in a large number of ways (from cultural fit to competitive position to legal status), it is crucial that the evaluation at *all* steps of the selection process is carried out by people who can appropriately screen potential partners on all of these dimensions. All members of the decision-making team need to agree on what the goals of the alliance are in order to make a coherent decision.

The first step is to determine a concrete set of criteria for evaluating potential partners, to ensure that important factors are not overlooked, provide support for the eventual decision, and screen out unsuitable candidates. Questions to ask in setting the criteria include:

- Do the two firms have similar interests and goals?
- Do they have complementary resources and skills?

- Are both dealing from positions of strength, or could one be exploiting the other? Do they have similar work-styles, cultures, and business practices?
- Can they trust each other?

The criteria should then be weighted to indicate those that are most important. The next step is to develop a ranked list of potential partners to meet with. Not all the criteria—work style, for example—can be evaluated in advance, but those that can be should be while plans should be developed for evaluating the others as soon as possible after contact is made.

After meeting with each company, *all* members of the selection committee should grade the potential partner on each criterion. This should be done immediately after each meeting, while it is still fresh in people's minds, not after an entire round of meetings. While it can be argued that the latter approach allows a better perspective on the relative strengths of candidates, in practice, any delay is likely to reduce the quality of the assessment.

While the selection discussion should begin with an examination of which company received the highest overall score, strong feelings on the part of team members should be taken into account. If the number one candidate is strongly supported by selection committee members except for a few members who hold strong reservations, while the second place candidate is universally accepted, but somewhat less enthusiastically supported, then the second place candidate may in fact be the better choice.

Monitoring Progress

The importance of regular status checks cannot be overemphasized, although it is forgotten surprisingly often. Indeed, in many alliances, it seems to be the case that more attention is given to the selection of an alliance partner than to maintenance of the subsequent relationship.

Realistically, however, there will be routine differences of opinion or reorientation of work efforts. It is also likely that major reassessments of alliances may be called for, since partners' goals and needs often change over the multi-year lifespan of most alliances.

Evaluating the success of the alliance is quintessentially a difficult task because the needs and goals of the alliance may sometimes conflict with the needs of either, or even both parent firms. While it is important to regularly evaluate the alliance and take corrective steps as soon as possible, one should not be overzealous. Like any relationship, alliances often go through growing pains, particularly once the honeymoon phase at the beginning of the alliance wears off.

What's more, alliance projects often break new territory, meaning that standard financial measures of success are usually inappropriate at the outset. Indeed, early on, any evaluation of the alliance should focus on the quality of the relationship, rather than the results; quality of the collaboration, equality in the relationship, productivity, and knowledge acquired should all be evaluated. If these are found to be lacking, concrete steps for improving them should be put in place.

Sometimes a company makes the mistake of viewing work on an alliance as a project of secondary importance, and assumes that if something more pressing comes up, a member of the alliance team can simply be staffed on the new project. This is a dangerous view because the intellectual capital and harmonious working conditions upon which an alliance depends are easily destroyed by the removal of the members who have created them. The alliance manager and the alliance team should be individuals who are committed to staying at the firm and with the alliance. A high turnover rate among the alliance staff is almost always a recipe for disaster for an alliance, just as it can be disastrous for a company.

While the key stakeholders for each company will differ, and this chapter discussed the requirements of six major groups—employees, customers, regulators, rating agencies, shareholder service providers, and business partners—management should explicitly address the risk management and reporting requirements for all key stakeholders.

Stakeholder management, perhaps more than any other aspect of ERM, requires cooperation at many levels, and in many departments of the organization. Top executives, business managers, risk managers, human resources, investor relations, marketing, and public relations must all be involved in ensuring that the company maintains good relationships with its stakeholders.

SECTION

Three

Risk Management Applications

CHAPTER 12

Credit Risk Management

The effective management of credit risk is a challenge faced by all companies, and a critical success factor for financial institutions and energy firms faced with significant credit exposures. Most obviously, banking institutions face the risk that institutional and individual borrowers may default on loans. Banks must therefore underwrite and price each loan according to its credit risk and ensure that the overall portfolio of loans is well diversified.

However, both financial and non-financial institutions also face credit risk exposures besides the default risk associated with lending activities. For example, the sellers of goods and services face credit risk embedded in their accounts receivable. Investors may see significant decreases in the value of debt instruments held in their portfolios as a result of default or credit deterioration. Sellers and buyers of capital markets products will only get paid on any profitable transaction if their counterparties fulfill their obligations to them. Furthermore, the increasing mutual dependence involved under arrangements such as outsourcing and strategic alliances exposes companies to the credit condition of their business partners.

Given this multiplicity of phenomena, there is obviously a need for a clear definition of credit risk. Credit risk can be defined as the economic loss suffered due to the default of a borrower or counterparty. Default does not necessarily mean the legal bankruptcy of the other party, but merely failure to fulfill its contractual obligations in a timely manner, due to inability or unwillingness.

A consultative paper issued in 1999 by the Basel Committee on Banking Supervision recognized that "the major cause of serious banking problems continues to be directly related to lax credit standards for borrowers and counterparties, poor portfolio risk management, or a lack of attention to changes in economic or other circumstances that can lead to a deterioration in the credit standing of a bank's counterparties."[1] While this quote focuses specifically on the banking industry, the need to establish sound credit risk management practices for customer receivables, investment activities,

and counterparty and business partner exposures is relevant to any given industry.

Credit risk management deals with the identification, quantification, monitoring, controlling, and management of credit risk at both the transaction and portfolio levels. Although the level and volatility of future losses are inherently uncertain, statistical analyses and models can help the risk manager quantify potential losses as input to underwriting, pricing, and portfolio decisions. Before we can do this, however, we will need to define some key concepts in credit risk management.

KEY CREDIT RISK CONCEPTS

Exposure, Severity, and Default

The credit loss on any transaction, whether a straightforward loan or complex swap, can always be described as the product of three terms:

$$\text{Loss} = \text{Exposure} \times \text{Default} \times \text{Severity}$$

Loss is the actual economic loss to the organization as a result of the default or downgrade of a borrower or counterparty—that is, as a result of a *credit event*. *Exposure* is the loan amount, or the market value of securities that the organization is due to receive from the counterparty at the time of the credit event.[2] This is the amount at risk. *Default* is a random variable which is either one (if the transaction is in default) or zero in the context of a single borrower or counterparty, but it may also represent the overall default rate of a portfolio. *Severity* is the fraction of the total exposure that is actually lost—the severity of a loss can be reduced by debt covenants, netting and collateral arrangements, and downgrade provisions.

Expected Loss

Another key concept is *expected loss* (EL), which represents the anticipated average rate of loss that an organization should expect to suffer on its credit risk portfolio over time. This is effectively a cost of doing business, and should thus be reflected directly in transaction pricing. The expected value of credit losses is equal to the product of the expected values of each of its components:

$$\begin{aligned} \text{EL} = \text{Expected Loss} &= \text{E}(\text{Loss}) \\ &= \text{E}(\text{Exposure}) \times \text{E}(\text{Default}) \times \text{E}(\text{Severity}) \end{aligned}$$

E(*Exposure*) is the expected exposure at the time of the credit event; it depends strongly on the type of transaction and on the occurrence of future random events. For loans, exposure is usually just the amount of the loan. Where a trading exposure to a counterparty is involved, the expected exposure must usually be modeled. For example, it is usually necessary to use a simulation model in order to find the expected exposures of long-dated transactions such as swaps or forwards.

E(*Default*) is the expected default frequency and reflects the underlying credit risks of the particular borrower or counterparty. It can either be estimated from the borrower's or counterparty's public debt rating or by calibrating the organization's own credit-grading scale. While each individual transaction is obviously either performing or in default—there is little middle ground between the two states—there is an expected frequency of default *within* an overall portfolio.

E(*Severity*) is the expected loss in the event of default. It is a function of facility type, seniority, and collateral. The severity is equal to the lost principal and interest, together with the cost of administering the impaired facility; it is expressed as a percentage of the exposure at the point of default. Since there is insufficient public data on recovery rates, and these tend to vary with the type of transaction, they must usually be estimated from the organization's own recovery data. Recovery rates for publicly traded bonds can be obtained from the major rating agencies.

The EL for a portfolio is simply the sum of the ELs of the individual transactions:

$$EL_{Portfolio} = \sum EL_{Transaction}$$

Unexpected Loss

Unexpected loss (UL) is a more important measure of risk than expected loss. EL is, as the name suggests, a reasonably predictable average rate of loss. Organizations do not have to hold capital against expected loss, assuming that they have priced it into the relevant transaction(s) correctly and have established the appropriate credit reserves. On the other hand, unexpected loss represents the volatility of *actual* losses that will occur around the expected level. It is the existence of UL that creates the need for a capital cushion to safeguard the viability of the organization if losses turn out to be unexpectedly high.

Statistically speaking, UL is defined as the standard deviation of credit losses. It is derived, mathematically speaking, from the components of EL:

$$\text{UL} = \sigma\,(\text{Credit Losses}) = \text{Var}^{1/2}\,(\text{Credit Losses})$$

If all transactions were to default at the same time, we would simply add up the UL of individual transactions to determine the overall UL of a portfolio. However, this is obviously extremely unlikely to happen, unless there are common factors driving the credit performance of all the transactions in the portfolio.

It's improbable, for example, that individual borrowers from different geographical locations would all default on their credit card debts at exactly the same time, although changes in the national levels of interest rates would likely be an important common factor. Similarly, a shared geographical location or industrial sector is likely to be important common factors for corporate borrowers.

The degree to which individual default behaviors are related is known as the *default correlation*. Broadly speaking, the more diverse (less correlated) the transactions in the portfolio are, the less likely it is that many of them will suffer a credit event simultaneously. Hence, the unexpected loss on a portfolio is dependent on its level of diversification as well as on the unexpected losses associated with individual transactions. This is measured in terms of the default correlations *among* transactions. Thanks to diversification, the unexpected loss on a portfolio will be less than the sum of the unexpected losses of its component transactions. In fact, it is:

$$UL_{portfolio} = \sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(UL)_i\,(UL)_j\rho_{ij}}$$

where $(UL)_i$ is the unexpected loss on the i^{th} transaction in the portfolio and ρ_{ij} is the default correlation between the i^{th} & j^{th} transactions in the portfolio. The higher the correlation between a new transaction and the portfolio, the more risk it adds to the portfolio. One of the key objectives for a risk manager is, therefore, to ensure that portfolios are sufficiently diversified—thus reducing the unexpected loss on the portfolio—by ensuring that credit exposures are not overly concentrated in any obligor, industry, country, or economic sector.

A word of caution on default correlation—as with general asset price correlations, default correlations increase significantly during market crises. As such, the benefit of credit portfolio diversification may not be realized during periods when it is most needed. Risk managers should stress test correlation assumptions (i.e., setting them at or near historical highs) to measure the sensitivity of UL to various levels of default correlation.

Reserves and Economic Capital

A credit loss *reserve* represents the amount set aside for expected losses from the firm's total portfolio of credit exposures. For example, bad-debt

provisions might be made to cover anticipated losses over the life of a loan portfolio. A reserve is a specific element of the balance sheet, while provisions and actual losses are treated as income statement items.

A firm must also earmark some capital to guard against large unexpected losses, however. This capital is known as *economic capital*, which is the amount that is required to support the risk of large unexpected losses. The amount of economic capital[3] required is determined from the *credit loss distribution*, which we will describe below.

Economic capital is an important concept for equity holders as well as debt holders. For equity-holders, economic capital can be used as a yardstick against which returns from different risk-taking activities can be consistently measured. For debt-holders, the economic capital can be viewed as the capital cushion against unexpected loss that is required to maintain a certain debt rating. It is determined in a similar way to the solvency tests applied by rating agencies, such as Standard & Poor's (S&P) or Moody's Investors Service, when assigning credit ratings.

For example, firms rated AA by S&P default with a 0.03 percent frequency over a one-year horizon. If a firm has a AA target-solvency standard, its economic capital can then be determined as the level of capital required to keep the firm solvent over a one-year period with 99.97 percent confidence. Since this is a probabilistic quantity, it will depend on the distribution of credit losses (see Figure 12.1).

Credit loss distributions are skewed because credit losses can never be less than zero. That would imply that borrowers pay back more than they owe when conditions are better than expected, which clearly does not

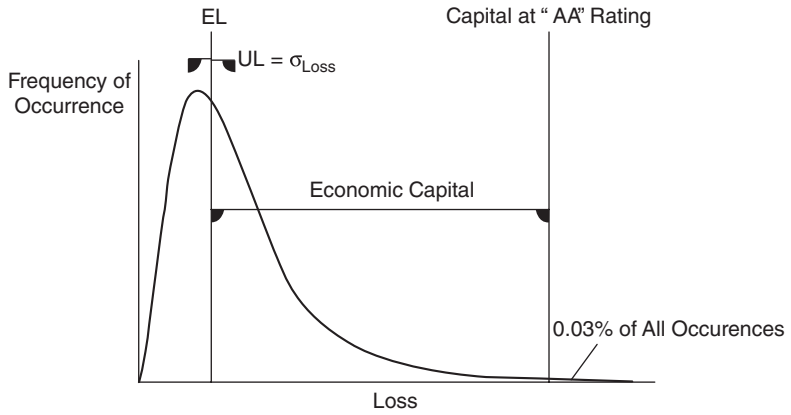


FIGURE 12.1 Illustration of Expected Loss, Unexpected Loss, and Capital Multiplier on the Loss Distribution

happen.[4] In most economic environments, one would expect relatively low levels of losses (at any competent institution, anyway). However, when times are worse than expected—for example, a recession causes a high level of defaults—credit losses can be much higher than average, and thus generate a longer, skewed tail. The distribution is *leptokurtic*, that is, the probability of large losses occurring is greater for a given mean and standard deviation than would be the case if the distribution was normal.

The loss distribution can be estimated by:

- Assuming that it conforms to one of the standard textbook distributions, such as the beta or gamma distribution, and parameterizing the distribution to match the portfolio's mean and standard deviation
- Analyzing publicly available information for peer firms, that is, their capital relative to their historical loss volatility (this requires some simplifying assumptions)
- Using numerical techniques or simulation to estimate and aggregate the yearly loss level of the portfolio over many business cycles.

Once the UL has been calculated and the loss distribution estimated, the desired debt rating (or target solvency standard) has to be factored into the economic capital calculation. This is done by introducing a *capital multiplier* (CM), which represents the number of multiples of UL required to create a capital cushion sufficient to absorb a loss at the confidence level implied by the institution's credit rating. It is determined from the loss distribution. As mentioned above, an institution that is seeking a AA rating must hold enough economic capital to protect against all losses except those so large that they have less than a 0.03 percent chance of occurring in any given year. Economic capital for credit risk is determined by:

$$Credit\ Risk\ Economic\ Capital = CM \quad \$UL_{Portfolio}$$

Off-Balance Sheet Credit Risk

When one thinks about credit risk, large loan losses come most immediately to mind. The dramatic and highly publicized credit crises of the last two decades include those associated with commercial real estate, less-developed country (LDC) debt, leveraged buyout (LBO) debt, Russian bonds, Long-Term Capital Management, energy trading counterparties, and the consumer debt problems that have plagued retail lenders (major mortgage write-offs in the early 1990s and sporadic credit card problems). More recently, the credit losses resulting from subprime loans and mortgage-backed

securities have reminded lenders and investors the importance of sound credit risk management.

However, as discussed in the beginning of this chapter, credit risk is not limited to banks and other financial institutions. In every market and every business, transactions with counterparties inevitably lead to credit exposures, which can result in economic loss and/or business interruptions. The most significant credit exposures faced by an organization may not even appear on the balance sheet; nowadays, organizations frequently assume credit risk from various off-balance-sheet financial instruments such as foreign exchange transactions, forward transactions, swaps, options, special-purpose entities, and financial guarantees. Two examples of off-balance-sheet credit exposures are provided below to illustrate how off-balance-sheet items can create credit risk exposures.

Credit Risk of Options A basic call option provides its holder with the right, but not the obligation, to purchase an asset at a predetermined price. Once the buyer pays the option premium, the seller of an option never has any credit risk exposure, because the buyer has no obligations to fulfill and there is therefore nothing to default on. The best-case scenario for the seller is that the option expires worthless and thus no future payment needs to be made.

However, the buyer of the option can be exposed to credit risk, since the seller is obliged to pay up if the option becomes profitable for the buyer and is exercised. As such, the buyer's credit risk exposure at any given time is the value of the option at that time, since that is the economic loss (or replacement value) that would be incurred if the option seller were to default. Options always have positive value until expiry (since there is always a chance that they will become profitable before the expiry date) and so the buyer of a basic option is always exposed to some credit risk until the option expires. The Black-Scholes option-pricing formula allows one to calculate option values, and hence the credit exposure.

Credit Risk of Swaps A swap is a financial agreement under which two counterparties exchange cash flows, based on one or more price indices. Let's use an interest rate swap to illustrate the challenges associated with the estimation of credit risk of derivative products.

There are two principal difficulties in estimating credit risk for interest rate swaps:

- There is little public information about severity in the event of default by swap counterparties. This is due to the paucity of defaults involving swap transactions. It appears that under U.S. bankruptcy law, swap

counterparties would have the lowest claim on the defaulted party's assets. However, the lower claim status of swap transactions is often mitigated by other credit protections, such as downgrade triggers and collateral requirements.

- The crucial element in the assessment of credit risk is the exposure amount or the mark-to-market value of a swap (which is usually close to zero at inception). Any exposure is generated later by the effect of price movements. The credit exposures of swaps and most other derivative transactions are indeterminate, in that they can be an asset *or* a liability, depending on movements in the underlying price or rate. For example, if interest rates fall, the party receiving a fixed rate in an interest rate swap has essentially acquired an asset, and they will then have credit exposure to the counterparty. If rates were to rise, however, the situation could easily reverse.

A number of different approaches have been taken with regard to the estimation of swap exposures. The most straightforward is the addition of a fixed percentage (add-on) of the swap's nominal amount to the current mark-to-market value. There are two difficulties with this approach. First, how should the add-on percentage be estimated? Second, the relevant exposure is not that of one particular swap but rather the total (net) exposure over all transactions with any given counterparty.

Sophisticated derivative dealers and users apply a simulation-based approach to the quantification of swap exposures. The basic concept behind simulation is that if we knew what the yield curve would be at the time of the counterparty default, we could value the swap and hence estimate the exact exposure amount.

Of course we have no idea when a counterparty might default, or what the yield curve might look like at that point in time. However, if we can model the possible evolution of the yield curve, we can generate a multiplicity of potential paths for interest rates over the remaining life of the swap and estimate the exposure for each separate path. We can then come up with an estimate of the most likely exposure and the potential variation in the exposure.

The success of this procedure clearly depends on the quality of the model used for the evolution of the yield curve. The basic procedure is indicated schematically in Figure 12.2.

Consider, for example, a plain vanilla swap with a notional principal value of $1 million, a maturity of five years, and a fixed-rate coupon of 6 percent. The short-term interest rate, which is also the floating coupon of the swap, starts out at 5 percent.[5] The results of the simulation procedure are illustrated in Figure 12.3, which displays the expected exposure and

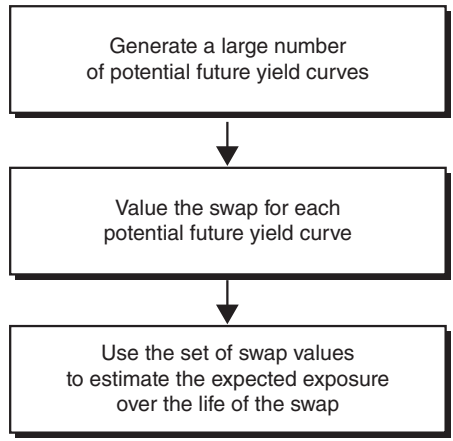


FIGURE 12.2 Basic Procedure

the 97.5 percent confidence bound on the exposure (the Maximum Likely Exposure or MLE).

Notice that the expected exposure rises until approximately the midpoint of the swap's term, at which point it falls back toward zero. On the final day of the swap the exposure will, in fact, be zero. A similar approach can be used for foreign exchange and commodity derivatives. In addition to the yield curve, a simulation model would estimate the price movements of the underlying price indices.

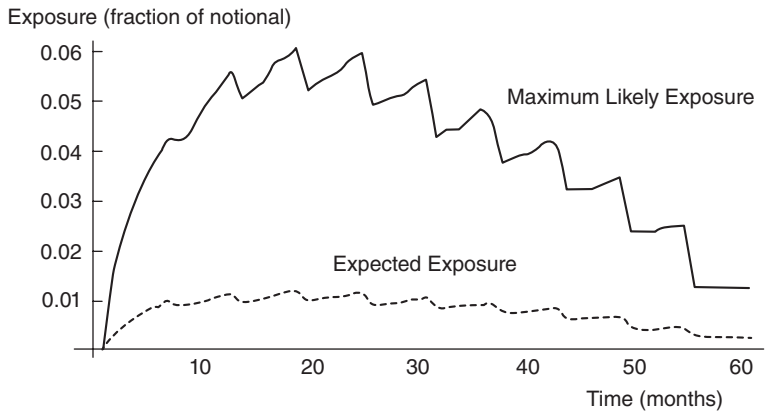


FIGURE 12.3 Exposure Simulation for a Plain Vanilla Swap

THE CREDIT RISK MANAGEMENT PROCESS

Figure 12.4 provides an overview of the credit risk management process. There are five stages: policy and infrastructure; credit granting; monitoring and exposure management; portfolio management; and credit review. Let's examine each of these in turn.

Policy and Infrastructure

This stage relates to the establishment of an appropriate credit risk environment; the adoption and implementation of credit risk policies and procedures; the development of methodologies and models, supported by appropriate systems; and the definition of data standards and conventions. It is the foundation on which management will build to ensure adequate controls are in place for managing credit risk.

An organization should have documented credit policies, methodologies, and procedures to ensure that credit risks are identified, measured, monitored, controlled, and regularly reported to senior management and the board of directors. These documents should reflect the firm's perspective on the prudent management of credit risks and take into account the nature and complexity of its activities, its business objectives, its competitive and regulatory environment, and its staff and technology capabilities.

Regulatory bodies take such policies very seriously. For example, the U.S. Federal Reserve System Trading Manual says:

"Credit risk management should begin at the highest levels of the organization, with credit risk policies approved by the board of directors, some form of credit risk policy committee of senior management, a credit approval process, and a credit risk management staff which measures and monitors credit exposures throughout the organization."[6]

There is no 'one-size-fits-all' structure in credit risk management, but generally credit policies should address such topics as:

- Credit risk philosophy and principles
- Credit analysis and approval processes

FIGURE 12.4 The Credit Risk Process at a Glance

- Credit rating systems and linkage to reserve and economic capital requirements
- Underwriting standards and risk-adjusted pricing guidelines
- Measurement of exposure of on- and off-balance sheet items
- Delegation of lending authority and exposure limits
- Target portfolio mix and use of risk transfer strategies
- Credit monitoring and auditing processes
- Exception and problem credit management
- Risk measurement and reporting activities

The policies adopted by senior management and the board need to be communicated to all employees involved in the credit process, implemented in a timely and consistent manner, and monitored to ensure compliance. They should be revised at least annually to take into account internal and external changes, such as new financial products, new markets and customers, and changes in regulatory environment.

Credit Granting

The second stage refers to the extension of credit to customers or counterparties. It encompasses credit analysis/rating of counterparties; credit approval by appropriate authorities; pricing and terms and conditions of transactions; and proper documentation.

An accurate, consistent system of risk rating is the essential underpinning of sophisticated credit risk management. A credit rating represents a firm's overall assessment of a given credit risk. It is the foundation for a set of critical activities—assigning loss provisions and risk capital, developing risk-adjusted profitability and pricing models, setting exposure limits, and managing the firm's risk/reward tradeoff.

Just as publicly available debt ratings are assigned by rating agencies (such as Moody's and Standard & Poor's) on the basis of data about the creditworthiness of a corporation, internal risk ratings summarize a firm's assessment of the probability of economic loss resulting from a credit-sensitive transaction. In developing the rating process, a firm should decide whether to rate the counterparty/issuer and/or to rate the specific transaction. The former would result in the same rating for all transactions related to one counterparty; the latter, in a rating that incorporates the characteristics of the transaction, such as collateral or guarantee. The latter approach is more refined, but the disadvantage is that it is more difficult to evaluate accurately. Some firms assign both counterparty and transaction ratings.

Risk rating systems should be designed so that it is possible to strike a balance between effectiveness (accuracy, consistency, and timeliness of

ratings) and efficiency (cost of assigning the ratings with a given frequency). Risk rating can be carried out on the basis of anything from pure judgment to deterministic modeling. In general, it will be a combination of both, including:

- Analysis of company financials, industry trends, and credit outlook.
- Use of a vendor-supplied or internal credit rating model.
- Use of external rating agencies credit ratings.[7]

A credit rating should be assigned to each on- and off-balance sheet credit exposure of the firm at origination. In addition, the system should be responsive to changes in credit risk characteristics of a counterparty/issuer/transaction. Exposures with deteriorating credit characteristics should be put on a credit watch list that is reviewed regularly by senior management and the board of directors.

A consultative paper issued by the Basel Committee on Banking Supervision in July 1999 outlines the factors to be considered in a bank credit-approval process.[8] These elements can be generalized to credit granting in general and would include an assessment of:

- The nature of the credit with respect to size, structure, maturity, and so on.
- The current risk profile of the borrower or counterparty and its sensitivity to economic and market developments.
- The borrower's repayment history and current capacity to pay its obligations, based on historical financial trends and cash flow projections.
- A forward-looking analysis of its capacity to pay obligations based on various scenarios.
- The reputation of the issuer or counterparty.
- The product knowledge and legal capacity of the counterparty to assume the liability.
- The proposed terms and conditions of the credit, including collateral and covenants designed to limit changes in the future risk profile of the counterparty (however, these should not be used to compensate for a lack of analysis or for poor information).
- Where applicable, the adequacy and enforceability of collateral or guarantees.

The credit-granting criteria listed above are obviously closely linked to the risk rating system, since they represent the basis for rating assessment. Granting credit involves accepting risks in order to produce profits, or transfer some risks to another party (for example, transferring market risk by entering into a swap agreement). With respect to loans, many banks

have found that they can significantly improve their ROA (return on assets) simply by setting pricing floors by risk rating.

The delegation of credit-granting authority should be designed to ensure an appropriate balance between the efficiency of credit operations and the effectiveness of credit review and approval. Lending authority is normally expressed in terms of notional transaction size, risk rating, and/or economic capital usage.

Monitoring and Exposure Management

Both individual and portfolio exposures should be monitored on a regular basis. Single-entity credit exposures should be monitored against established limits to prevent undue exposure to an individual counterparty. Moreover, aggregate exposures by industry, country, and economic sector should be monitored against limits to ensure appropriate portfolio diversification. Indicators such as credit spreads and stock price volatilities should be tracked for early warning signals of potential adverse credit events. Large individual and aggregate credit risk exposures should be reported to senior management and to the board of directors.

A basic requirement of effective credit risk management is updated credit exposure information. For example, a firm might have different transactions with a single counterparty that are conducted by more than one of its business units. In order for management to measure the current exposure to the counterparty, the individual transactional exposures must be aggregated. Exposure measurement of business activities in this way is important for a number of purposes; risk reporting; comparison with policy limits; and determination of required level of credit reserves and economic capital.

There are two types of credit exposure: current exposure and potential exposure. Current exposure is defined as the amount at risk today—it is the loss that would be suffered here and now if all the credit transactions were to be settled and all the credit assets were to be sold immediately. This definition should make obvious the fact that current exposure takes no account of any future changes in market prices.

Potential exposure, on the other hand, depends on the type of transaction and on the occurrence of future random events. For loans or receivables where there is no line of credit, potential exposure and current exposure are the same, absent any loan amortization or principal payment. For other transactions, such as swaps or credit lines, potential exposure needs to be modeled or estimated, since it is a function both of time to maturity and of the volatility of the underlying instrument. Furthermore, credit enhancements, such as collateral and third-party guarantees, downgrade triggers,[9]

and netting agreements[10] can be used to reduce a firm's counterparty credit risk. The calculated exposures should reflect these risk-reducing features if they are legally enforceable in the relevant jurisdictions.

Different approaches can be taken to exposure calculations. The calculation might be based on current exposure; maximum potential exposure; average expected exposure; or some rule of thumb, such as an add-on as a percentage of notional value. In addition, the exposure can be measured in terms of notional amounts, or in terms of economic capital requirements, with the latter being more representative of the risk involved in the transaction. Economic capital exposure is such that each dollar of economic capital represents an equal exposure to credit loss volatility. The selection of the appropriate exposure calculation(s) for a business depends on the level and complexity of credit risk, as well as the business applications for the exposure calculations.

The important concept to remember in exposure measurement is consistency. One challenge that a firm faces is the development of consistent measures for credit exposure throughout its portfolio. Since the exposures need to be aggregated in order to obtain a meaningful view of the total portfolio, and in order to compare exposures against approved limits, all transactional exposures must be measured in a consistent manner.

A concentration of credit risk is the single most important cause of major problems. One senior credit officer I met in the early days of my career put it succinctly when he said: "Concentration kills." Concentrations arise in a credit portfolio as a direct consequence of business specialization. It is this specialization that allows a firm to achieve market leadership and gain competitive advantage, and as such, concentration cannot be eliminated entirely. However, it can be controlled through the use of exposure limits.

The establishment of exposure limits is an important element of credit risk management that ensures appropriate diversification of a firm's credit portfolio. Limits should be defined for single counterparties, groups of connected counterparties, products, industries, and even for countries or geographic regions in which the firm currently holds, or could potentially hold, credit exposures.

Credit limits are useful in all areas of the firm's activities that involve credit risk. They should reflect management's appetite for a credit risk, and be meaningful constraints on business activities in order to mitigate risk. They should not, therefore, be so high that they are never breached, or so low that are breached too often. Actual credit exposures should be regularly compared with the established limits, and procedures should be in place for taking appropriate action within a defined period when limits are approached or exceeded.

Risk limits serve four main interrelated credit processes:

1. *Risk control:* The presence of limits prevents the firm from engaging in business activities that are too risky, such as extending too much credit to a single counterparty or industry. They ensure that the firm enters into new products and markets only once the proper risk management prerequisites are in place. Limits are also set to control activities in areas where the firm does not think it should be active because it is likely to be competitively disadvantaged. As such, the limits reflect not only a business judgment that the risk/reward tradeoff is inadequate, but also serve to manage operational risks. For example, smaller credit limits might be allocated in countries where business and contract laws are questionable.
2. *Allocation of risk bearing capacity:* Like any other scarce financial resource, credit limits must be rationalized across products and business activities. Limits should be set to reflect management's determination of the risk/reward tradeoffs made by potentially placing bets in a concentrated manner. A good example of the dangers of risk concentration is the case of the 1998 default of Power Company of America (PCA, a power-trading company). On June 24, 1998, a freak combination of factors led to power prices in the Midwest skyrocketing from their typical level of $30/MWh to an astounding $7,500/MWh. One of PCA's suppliers, Federal Energy Sales failed to deliver. PCA had to default as well, and was subsequently forced into bankruptcy by $236 million of outstanding claims. Had credit concerns stopped PCA from doing business with Federal earlier in 1998, as other companies had, its exposure to the company might not have been as lethal. An effective limit management process might have made for a very different story.
3. *Delegation of authority:* The credit limit system ensures that credit decisions are made by people with the requisite skills and appropriate authority. The delegation of credit authority is usually granted from the board of directors through the credit policy. From that point the firm's senior management may further delegate credit authority to the business units. This process may extend further still, with delegation to the individual personnel within business units. The delegation of credit authority through explicit credit limits ensures that central management retains control over credit risks, while providing business and risk-taking flexibility on a day-to-day basis.
4. *Regulatory compliance:* Regulators across all industries are increasingly focused on the corporate governance and audit procedures of the companies they monitor. For companies with significant financial risk exposures, the application of VaR measures has become an accepted

standard. For companies that are credit risk intensive, such as banks and brokerage firms, regulatory authorities can be expected to maintain close scrutiny of credit risk controls, including exposure limit management processes.

A credit risk reporting process provides relevant information to senior management and the board of directors so they can effectively perform their oversight and fiduciary function. Effective and timely reporting of the firm's key credit exposures helps to ensure that risk management objectives are met, and facilitates appropriate management decisions and actions.

Credit risk reporting should be prepared by the risk management function and should typically include information on portfolio trends, risk-adjusted profitability, large and complex transactions, aggregate credit exposures against policy limits, and key exceptions. In practice, the effectiveness of the firm's credit risk reporting process will be highly dependent on the quality of data resources and management information systems. In fact, the greatest challenge faced by most institutions will be the integration of various databases and systems to obtain a comprehensive credit portfolio perspective.

In July 1999, the Basel Committee on Banking Supervision published a paper: "Best Practices for Credit Risk Disclosure." According to this report, credit risk information should be:

- *Relevant and timely:* Information should be provided with sufficient frequency and timeliness to give a meaningful picture of the institution's financial position and prospects. To be relevant, information should also keep pace with financial innovation and developments in credit risk management techniques such as credit risk modeling.
- *Reliable:* Information should be reliable. Typically, it is more difficult to obtain precise measurements of credit risk than of market risk. This is because the estimation of default probabilities and recovery rates is usually less precise than the measurement of price movements in liquid markets. Moreover, credit ratings assigned to a counterparty usually include an element of judgment, which in turn depends on the quality of the credit staff.
- *Comparable:* Market participants and other users need information that can be compared across institutions and countries, and over time. As such, it is useful to apply industry standards for credit exposure measurement, as well as map internal credit ratings to those established by the rating agencies.
- *Material:* Disclosures should be adapted to the size and nature of an institution's activities, in accordance with the concept of materiality.

> Information is defined as material if its omission or mis-statement could change or influence an assessment or decision made by a user relying on that information.

Portfolio Management

Until recently, credit risk would typically stay on a firm's balance sheet until the settlement of transactions or the maturity/sale of financial assets. The introduction of active portfolio management, loan securitization, and risk transfer strategies has advanced the concept of credit portfolio management. With these tools, a target portfolio with optimized risk and return characteristics can be defined. The actual credit portfolio can then be steered toward this target by the use of portfolio management strategies. Such strategies may include the outright purchase or sale of assets; alternatively, part of the portfolio might be securitized or hedged through credit derivatives. Credit portfolio management can be used not only to optimize the risk/return of the credit portfolio, but also to free up scarce capital and credit limits in order to grow origination activities.

A portfolio management function should be responsible for optimizing the risk/return characteristics of the overall credit portfolio. The risk profile of a credit portfolio can be optimized through the use of origination targets, pricing, and risk transfer strategies. Origination targets determine which kinds of credit exposure the organization can safely take on, given the existing portfolio, while pricing can be used to ensure that it is adequately rewarded for taking on such exposures. Risk transfer strategies allow it to reduce or eliminate risks that are deemed undesirable and/or inefficient within the firm's portfolio, and also allow it to take on, or increase, desirable risks. The credit policy should document the financial vehicles that can be utilized—for example, securitization, derivatives, insurance products, sales of assets, and alternative risk transfer products. It should also specify the permitted transactions and applications of portfolio management and risk transfer techniques.

An innovative trend in wholesale banking has been the disaggregation of origination, portfolio management, and servicing activities. The rationale for this transformation in wholesale banking is nearly identical to the rationale underlying the same trend in mortgage banking a decade earlier. One part of this rationale is that corporate lending is generally a low-margin activity, and as such unprofitable unless bundled with non-credit transactions. The combination of poor economics, high capital consumption, and unfavorable tax treatment[11] conspires to suggest that these loans, if they are to be made at all, should be sold to investors. The packaging of loans into collateralized loan obligations (CLOs) and commercial mortgage-backed securities (CBMS) also

provides market discipline for three key components of a company's credit risk management process: underwriting, pricing, and documentation. First, the company's credit underwriting is confirmed as rating agencies review the creditworthiness of individual loans when they rate the various tranches of the deal. Second, investors will provide market feedback on appropriateness of the initial loan pricing when they bid on the supported securities. Finally, legal review will establish a check on the quality of loan documentation and collateral protection embedded in the loan contracts.

Credit Review

In order to ensure compliance with the established credit policies and processes, a formal credit review should be implemented as a separate credit risk process, or as part of the overall audit process. This involves a thorough review of a sample of transactions and documentation, testing of systems and data integrity, the enforcement of underwriting standards, and compliance with specific policies and procedures. The credit review group must be independent from the origination group; it may even be independent from the risk management function.

It is essential to define a disciplined process that ensures transactions are monitored and individual businesses comply with underwriting and credit standards. It also ensures appropriate checks and balances, as well as compliance with the organization's credit policies and procedures. Moreover, trouble indicators, such as unapproved limit excesses or double-rating downgrades, should be reported and addressed. An effective credit review process not only helps to detect potential credit problems, but also ensures the identification of exceptions or violations to credit policies and procedures.

The frequency of the reviews and specific actions to be undertaken for policy violations should be defined up front by the risk management function and approved by senior management and the board. These actions include re-rating the counterparty or transaction, revising the terms and conditions of the transaction, selling the asset to another market player, or executing a risk transfer strategy. It is good practice to document and report policy exceptions and establish a defined timeframe for resolution.

BASEL REQUIREMENTS

Regulatory requirements are a key driver of industry practices, and none more so than the capital adequacy system developed by the Basel Committee on Banking Supervision. The members of the Basel Committee, established

by the central bank of the Governors of the Group of Ten countries in 1975, are banking supervisory authorities. Today, the expanded group consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.

The Basel Committee's guidelines on capital allocation against credit risk have done much to shape the credit markets and the development of credit risk management. In 1988, the Committee introduced a capital adequacy system for banking institutions that stipulates an 8 percent capital charge against the risk-weighted exposure of all balance sheet assets. The risk weightings were assigned by asset class, ranging from 0 percent for U.S. Treasuries to 100 percent for corporate loans and bonds. The Capital Accord became a global benchmark for regulatory credit risk capital standards, and as such, a major driver for the behavior of banking institutions.

However, by the mid-1990s the Capital Accord was being disputed by a large number of practitioners who argued that it had some major pitfalls. For example, the risk weightings were seen to be too crude and arbitrary, with the effect that the Accord recognized no difference between lending to an AAA-rated corporation and to a double-B rated OECD country. Also, the Accord paid little heed to the term structure of credit risk. Consequently, a one-year loan was treated in the same way as a 20-year loan, despite the fact that there is clearly more chance of default over 20 years than over 12 months. Nor did the original Accord allow for the use of collateral or portfolio diversification effects.

To acknowledge the fact that the financial markets had changed significantly in the last decade, and that risk management tools had improved significantly, the Committee developed a new capital framework during the late 1990s. The new framework consisted of three pillars: minimum requirements, supervisory review process, and effective use of market discipline. To quote from the introductory report: "It is designed to improve the way regulatory capital requirements reflect underlying risks. It is also designed to better address the financial innovation that has occurred in recent years. . . . The review is also aimed at recognizing the improvements in risk measurement and control that have occurred."[12]

The Basel II framework motivated many financial institutions across the globe to adopt more advanced risk management tools for credit risk and other risks. Sophisticated banks were able to use internal models and ratings rather than public ones, subject to supervisory review and approval. Credit risk was only one part of the new capital guidelines, since the Committee had included capital charges for other risks, namely market risk and operational risk.

"The Committee believes that the Accord must be responsive to financial innovation and developments in risk management practices. The Committee's longer-term aim is to develop a flexible framework that reflects more accurately the risks to which banks are exposed."[13] Most risk practitioners agreed that, despite remaining technical issues, Basel II was certainly a step in the right direction.

The latest framework, Basel III, which was set for an early 2013 implementation in the United States—with a transitional period of up to 2019—was designed as a response to the weaknesses in financial regulation that were exposed by the global financial crisis. The updated requirements of Basel III include:

- An increase in the minimum common equity requirement from 2.5 to 4.5 percent
- A capital conservation buffer of 2.5 percent (total common equity requirements now up to 7 percent)
- A minimum tier-one ratio of 4.5 percent
- A countercyclical buffer of between 0 to 2.5 percent
- Higher capital requirements for trading and derivatives across the board.[14]

These key ratios are calculated as follows:

- *Common equity:* Common equity items include capital instruments and their related shared premium accounts, retained earnings and other significant accumulated income and reserves, and funds for banking risk.[15]
- *Capital Conservation Buffer:* These items include cash dividends, fully or partly paid bonus shares and other capital instruments, and repurchases of a firm's own shares and other capital instruments.[16]
- *Countercyclical Capital Buffer:* The individual countries participating in Basel III set countercyclical capital buffers.

As a result, Basel III will likely prove to have a significant impact on both individual banks and the financial sector as a whole. In today's harsh, already highly regulated business environment, it will be harder for some banks to meet the new capital requirements while simultaneously placing greater emphasis on meeting profitability and growth targets. These new capital requirements will also shift demand from short-term loans to long-term loans, which may restrict the banks' lending abilities.

Ultimately, full implementation of Basel III might create a capital shortfall of 577 billion Euros for banks in the Eurozone, as well as increase in risk-weighted asset holdings by 23 percent.[17] By 2019, the U.S. banking

sector will require $870 billion of additional Tier 1 capital, $800 billion for short-term liquidity and $3.2 trillion in long-term funding; as a result, ROE may decrease by around 3 percent in the United States and 4 percent in Europe.[18]

On the other hand, the implementation of Basel III should provide some important benefits to the financial industry. If the Basel III requirements are met on both the domestic and international levels, they will help to produce a more stable financial system, which will diminish the chance of a widespread banking crisis occurring in the future.[19] By fortifying the banking system so that it can withstand adverse shocks, Basel III aims to reduce the chances that disruptions in the financial sector will cause a global upheaval on the level of the most recent financial crisis. It also aims to "improve risk management and governance as well as strengthen banks' transparency and disclosures" in order to improve our ability to forecast—and thus, avoid—such disasters.[20]

Basel III also addresses concerns about systemic and counterparty risks. In order to be able to better absorb any potential losses, banks that are deemed "systemically important" are required to go beyond the minimum requirements. In addition to the minimum capital ratio, Basel III provides these banks with further provisions for leverage and liquidity standards as a means to reduce systemic risk. The minimum Tier 1 leverage ratio is 3 percent, which serves as an added protection beyond the risk-specific capital requirements.[21] U.S. banking regulators recently announced plans that will require the top eight banks to increase their minimum Tier 1 leverage ratio to 5 percent, while their FDIC-insured bank subsidiaries will have to increase their ratios to 6 percent.

Of the proposed reforms that address counterparty risk, some include the requirement that banking institutions should "determine their capital requirement for counterparty credit risk using stressed inputs."[22] Basel III creates further incentive for banks to manage counterparty credit risk by raising the capital charges for capital valuation adjustment value-at-risk (CVA VAR).

There also remain significant limitations to the Basel III framework, with regard to the extent that regulators can mitigate the risks inherent in the global banking system—much of this management must still be left up to individual banks.[23] Other criticisms of Basel III condemn it for not addressing the weaknesses of the preceding Basel II framework. Specifically, some believe that Basel III does not solve the issue of risk weighting assets, which requires institutions to hold more capital against riskier assets (determined by ratings given by ratings agencies).[24] Writing in *The Economist,* Noah Millman explains that the financial crises of 2008 and 2009 were not caused by "direct exposure to sub-prime loans," but by "exposure to

triple-A-rated debt backed by pools of such loans, debt which turned out not to be risk-free at all."[25] He claims that Basel III does not solve this problem, and that it might even cause further issues, since it "massively increases the incentive to find low-risk-weight assets with some return," and start another lending frenzy.[26] In the final analysis, regulatory frameworks such as Basel III represent necessary but insufficient standards for credit risk management. Banks and other credit-intensive companies must go beyond regulatory requirements and adopt industry best practices.

BEST PRACTICES IN CREDIT RISK MANAGEMENT

Best practices in credit risk management, as with other risk management disciplines, represent a moving target. What are considered best practices today will become industry standards in a few years. For credit risk-intensive businesses, a key challenge facing management is how to ensure that company practices are, at a minimum, consistent with industry practices, and ideally represent best practices. The following sections describe three categories of credit risk measurement and management practices:

1. *Basic practice* represents the minimum controls required for effective credit risk management
2. *Standard practice* represents the next level of credit risk applications in terms of sophistication
3. *Best practice* represents the most advanced credit risk applications adopted by leading institutions

It is important to note that a company does not necessarily need to establish best practices for all of its risk management areas. The appropriate level of sophistication in risk management processes really depends on the risk profile of the individual company. For example, a manufacturing company does not require the same level of investment in credit risk management as a commercial bank. Therefore, many companies have adopted what they considered to be best-in-class practices that incorporate the size, complexity, and risk profile of their businesses.

Basic Practice

A fundamental step in credit risk management is developing common definitions of risk and exposure measurement across business units. These definitions include items such as counterparty names used to identify the legal entities involved and the associated credit exposures; risk ratings, based on

consistent underwriting standards; and simple exposure measurement and aggregation methodologies such as loan and notional amounts. At the basic practice level, few risk ratings are established, and those that are installed are mainly used to accept or decline credits. The majority of credit exposures are often lumped into two or so ratings. The use of credit limits are focused on individual transactions, such as maximum amounts by obligor and risk rating, with few, if any, portfolio risk limits. The use of credit risk models is limited to simple spreadsheet models, ratio analysis, and credit bureau reports.

The credit risk management function is mainly a credit policy, approval, and monitoring function. It establishes credit policies and underwriting guidelines on how credits should be rated and what ratings are acceptable. Approval by a credit analyst or committee is only required for transactions above a certain size. On an ongoing basis, the credit function also identifies problem loans, maintains a watch list, and plays a central role in the workout process. The performance of the credit risk function is mainly determined by the level of charge-offs and delinquent loans.

Standard Practice

Building on the basic practices described above, standard-practice companies establish more risk ratings to better differentiate underlying credit risks, and explicitly link risk rating to pricing, reserve, and capital requirements. For example, a loan with a certain rating would be priced based on a pricing model or pricing matrix, and is then allocated a risk-adjusted level of reserves and capital. Formula-based exposure measurement and aggregation methodologies are used to translate on- and off-balance sheet exposures into loan equivalent amounts, while credit exposure limits are established by counterparty, risk rating, industry, and country. The use of credit risk models is limited to the credit risk management function, and may include both internally developed and vendor models. These models take into account detailed financial information, stock and credit spread volatility, and economic indicators.

The credit risk management function is more integrated with the loan origination function. Relationship managers or teams are assigned to institutional clients while product managers are assigned to retail products. These managers develop relationship and product plans that take into account both the profitability and the risks of individual transactions, as well as the overall portfolio. As such, credit analysts and loan originators work together to structure and price specific transactions and products in order to address both business and credit considerations. The performance of the credit risk management function is determined not only by the level of charge-offs and delinquencies, but is also influenced by how they contributed to the growth and risk-adjusted profitability of the business units.

Best Practice

Going beyond what has been discussed above, best-practice companies develop more advanced tools and applications in each aspect of their credit risk management. These tools and applications include:

- *Integrated credit-exposure measurement:* Monte-Carlo simulation models are used to calculate indeterminate credit exposures (e.g., swaps, forwards, credit lines) so they can be aggregated with loan exposures. This provides management with an accurate measurement of credit concentrations by counterparty name, industry, risk rating, country, and other defined credit segments. Aggregate credit exposures also incorporate the impact of netting and collateral arrangements. In addition to credit-exposure aggregation, the credit database can be used to identify unusual credit behavior or patterns.
- *Scenario analysis and planning:* Best-practice companies develop the ability to measure how adverse credit events and market changes would affect the institution's risk positions. It is important for management to assess the potential impact of multiple events. For example, how would a global stock market crash combined with a Mexican peso devaluation affect the institution's direct credit exposures to Mexican companies, and to other companies with significant economic ties to Mexico? Such scenario analysis is then followed by the formulation of risk mitigation plans and leading indicators so that the company can identify the emergence of various scenarios and take appropriate actions.
- *Advanced credit risk management tools:* These tools include credit scoring models that assist credit analysts in rating counterparties and tracking the probability of default over time; credit surveillance systems that provide early warning signals by monitoring stock and bond prices, credit spreads, company news stories, and other market and competitive data; credit migration models that help management to assess potential future credit losses and reserve and capital requirements, by projecting how current credit ratings would migrate over time under expected and stressed scenarios; pricing models that help relationship managers determine risk-adjusted product pricing and relationship profitability; and portfolio management tools that help management determine the optimal asset allocation based on business risk and return relationships.
- *Active portfolio management:* Based on the information and tools above, best-practice companies develop strategies to optimize the risk/return of the overall credit portfolio. This includes changing the institution's existing credit portfolio through loan sales, securitization, credit enhancement, credit derivatives, and other techniques, as well as

defining trigger points and exit strategies for the institution's current and/or projected credit concentrations. A centralized portfolio investment unit drives the active portfolio management approach. This unit sits between the bank's loan originators and the secondary market; it assumes ownership of credit assets, and exercises profit and loss (P&L) responsibility for the portfolio as a whole. The portfolio unit is intended to act like an asset manager—that is, to make decisions about what to buy and sell, and at what price, based on a portfolio assessment of risk and return. A significant virtue of the active portfolio management approach is its transparency. Individual functions are held accountable for the sources of value within their control—such as pricing and productivity for origination; credit returns and economic capital utilization for portfolio investment; and scale and cost efficiency for servicing. This added transparency goes a long way toward eliminating the cross-subsidies that often make credit a loss leader, and toward establishing pricing and underwriting discipline based on market developments.

Best-practice institutions are characterized by a credit culture where credit risks are managed at both the transaction and portfolio levels, and where there is an optimal balance between business and risk management objectives. This culture is supported by the appropriate credit training and incentive programs that reinforce the organization's credit policies. Building a best-practice credit risk management capability is expensive: it requires highly skilled staff and extensive systems investments. However, there are significant benefits. First, credit approval and pricing decisions are improved at the transaction level. Second, concentrations in credit risk at the portfolio level are controlled to prevent large unexpected losses. Third, more accurate projections of credit losses and reserve requirements result in smoother earnings. Fourth, advanced credit metrics and reporting help facilitate management decisions and actions before credit problems deteriorate further. And finally, active portfolio management and risk transfer strategies will help to optimize the overall risk and return of the credit portfolio.

Ultimately, the true test for a best-practice company is not simply the advanced models and methodologies that it employs, but the difficult management decisions that it needs to make in the face of earnings pressure. A good example is the large credit write-offs of telecommunication loans by the large banks in 2002. Many of these banks have developed very sophisticated credit risk models, but nonetheless built up significant credit exposures to the telecommunication industry because they offered huge investment banking fees and attractive growth prospects in the previous years.

Lenders beware: concentration kills.

CASE STUDY: EXPORT DEVELOPMENT CORPORATION (EDC)

EDC is a Canadian crown organization with a very important mission. Since 1944, EDC has been helping Canadian businesses grow and prosper through international trade and foreign investment. Export Development Corporation is accountable to the Canadian Parliament through the Minister for International Trade and operates as a Commercial Crown Corporation. EDC's purpose is to support and develop, directly or indirectly, Canada's export trade and Canadian capacity to engage in that trade and to respond to international business opportunities. EDC is the only Canadian financial services company devoted exclusively to providing international trade-related financial services in support of Canadian export.

Patrick Lavelle (chairman at the time this case was written) explains: "Overall, our results are a tangible reflection of our public policy mandate: to support and develop, directly or indirectly, Canada's export trade, as well as Canadian capacity to engage in that trade and to respond to international business opportunities. We do so by taking on trade risks in a financially sound manner, through credit insurance, bid and performance bonds and guarantees, and by making it easier for foreigners to buy Canadian through a multitude of financing options." Mr. Lavelle added: "As Chairman of EDC, one of my key objectives is to ensure that we can meet our public policy objective by striving toward best practices in risk management."

Lines of Business

With financial assets of about $25 CAD billion, EDC provides a wide range of financial products and services in support of its customers. The Corporation delivers its products and services through sector-based business teams. A cross-sector team dedicated to serving small and medium-sized enterprises and various centers of expertise provide in-depth industry and country knowledge in support of the business teams. EDC's financial products and services can be classified into five general categories:

1. *Credit insurance services:* protect EDC's policy holders (generally, Canadian exporters) against non-payment by buyers and/or banks, whether it is due to commercial risks such as insolvency, default, repudiation of goods, or termination of contracts, or to country risks outside the buyers/banks' control such as difficulty in converting or transferring currency, cancellations of export or import permits, or war-related risks.
2. *Financing services:* provide EDC's customers, and enable them to provide their customers in turn, with flexible, medium- and long-term financing using a variety of structures (lines of credit and protocols with

foreign banks and agencies, note purchase arrangements, direct buyer loans, long-term pre-shipment financing, leveraged lease financing, and project risk financing packages).

3. *Contract insurance and bonding services:* come into play in many international credit commitments, particularly for capital equipment and projects, where those who purchase from EDC's customers may require them to post bonds guaranteeing their bid, performance, or any advances received from the purchasers.
4. *Political risk insurance services:* to support EDC's customers with investments in foreign countries and to support lenders who finance transactions pursued by EDC's customers abroad. Political risk insurance protects the policy holder against transfer and convertibility risk, expropriation risk, war, revolution, and insurrection risk.
5. *Equity services:* provide equity and other forms of related investments in EDC's customers or their projects, or companies operating abroad or through participation in market- or sector-focused investment funds.

Credit Risk at EDC

Credit risk at EDC is broadly defined as the possibility of financial loss resulting from credit commitments within EDC's business activities. Credit risk generally manifests itself as the risk of a payment default resulting in a financial loss for EDC's direct credit commitments, or a risk event which could lead to a claim for EDC's indirect credit commitments. Depending on the type of credit commitment, credit risk may include: financial solvency risk, performance risk, industry risk, unwillingness to pay on the part of the obligor and/or related parties who may have an influence on the possible loss associated with the credit commitment, and country risk of the country in which the obligor and/or related party is domiciled.

Since the acceptance of credit risk is such an important component of EDC's policy mandate and long-term success, it is critical for senior management that best practices are in place. As such, in the summer of 1999, EDC began a major initiative to establish a credit policy framework that would represent industry best practices. Peter Allen, CFO, and W. James Brockbank, VP Risk Management (who was promoted to CRO in 2001), provided the executive sponsorship for the initiative, while Christopher Clubb, a senior member of the Risk Management Office, acted as the overall project manager. The key objectives of EDC's credit initiative included:

- Articulate and document the organization's credit philosophy and processes
- Make significant improvements in its credit policies and practices

- Shift the role of the Board of Directors from transaction approval to credit policy and portfolio management
- Develop a Credit Risk Policy Manual that will establish the overall credit risk management framework at EDC

This project represented a significant step for EDC in moving toward best-practice credit risk management. At the conclusion of the project, all parties involved felt that the project was highly successful in achieving its objectives. Several key success factors contributed to the positive outcome of the project. These key success factors include:

- *Board Involvement:* Members of the Board, in particular Patrick Lavelle, chairman, and Pierre MacDonald, chair of the Board's Risk Management Committee, took on highly visible, engaged, and supportive roles throughout the project. At times, their personal commitment and participation resulted in more aggressive development of EDC's risk management capabilities. In addition, Robert Holt, James Patillo, and Huguette Labelle, the other members of the Board's Risk Management Committee, played critical roles in reviewing with management the entire manual and recommending approval of the manual to the full Board of Directors.
- *Executive Management Commitment:* Ian Gillespie, CEO, and Peter Allen, CFO, were both fully committed to the project. To ensure compliance with the credit policies, a policy compliance and reporting procedure was put in place at the end of the project. As part of this procedure, Gillespie and Allen would sign a "compliance certificate" each month that assured the Board that they were monitoring EDC's credit activities against the policies, and that any exception was reported as required. Additionally, senior management agreed with the board to review the Credit Risk Policy Manual on an annual basis to facilitate ongoing improvement.
- *Executive Management Steering Committee:* The project evolved over the course of approximately six months. Over this time, the executive Risk Management Committee served as the steering committee in completion of the project. In addition, to Gillespie, Allen, and Brockbank, the committee is comprised of Eric Siegel, executive vice president medium long term financial services, Rolfe Cooke, senior vice president short term financial services, and Gilles Ross, senior vice president legal services and secretariat.
- *Stakeholders Management:* The Risk Management Office, led by W. James Brockbank and Christopher Clubb, paid significant attention to communication with key stakeholders. For both the Board of Directors and line management, they introduced each section of the Credit Risk Policy Manual in a phased approach to obtain buy-in. Additionally,

they held open house meetings with small groups of directors to further educate them about credit risk management objectives and practices.

- *Open Debate and Resolution:* There were no sacred cows during the project. All issues were open for debate and discussed until resolution was reached. In one defining moment for the project, Peter Allen put forth a number of critical issues regarding EDC's credit-approval process. These issues were fully debated until final agreement was reached on the appropriate policies for credit approval. This agreement alone resolved open issues that had caused confusion for many years.
- *Credit Culture Change:* This project resulted in real change in EDC's credit culture even before the Credit Risk Policy Manual was finalized. Credit risk considerations were integrated into senior management decisions at both the transaction and portfolio levels. Additionally, line management was increasingly seeking the guidance of the Risk Management Office.

EDC's Credit Risk Policy Manual

The following sections summarize the major components of EDC's credit risk policy manual.

Organizational Structure Patrick Lavelle: "Given that EDC is targeting higher-risk markets on behalf of Canadian businesses, as well as operating in an increasingly uncertain global economic environment, a Risk Management Committee of the Board has been established to ensure that the principal risks of the corporation's business have been identified and that appropriate systems are in place to manage our risk strategy."

The organizational structure for risk management at EDC is shown in Figure 12.5.

The Risk Management Committee of the Board was established in May 1998. Pierre MacDonald, an independent board member, chairs the committee. Its immediate focus was to ensure the appropriate credit policies were in place. It was also responsible for reviewing and approving business transactions, as well as monitoring the overall risk in EDC's risk portfolio. The Risk Management Committee of the Board consists of:

- The Chairman of the Board of Directors
- The President, and
- Four Directors appointed by the Board, including Pierre MacDonald.

The Risk Management Committee of the firm and the Risk Management Office, headed by W. James Brockbank, were established to provide a second and impartial perspective as to the acceptability of the assets and/or

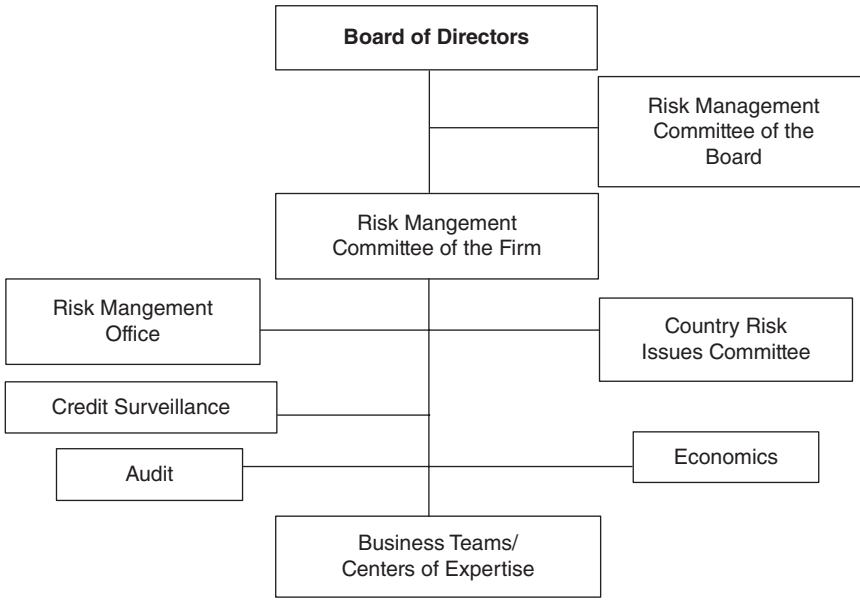


FIGURE 12.5 EDC's Risk Management Structure

exposures being recommended by the business teams. Their mandate is to optimize the corporation's capacity and appetite for timely origination of credit exposures consistent with corporate business plans and objectives.

Philosophy Statement As mentioned previously, a credit-intensive firm should have a documented credit risk philosophy that underpins the credit risk management framework. This statement presents the credit risk culture that exists within the organization and underlies the credit risk policies, methodologies, and procedures. EDC's statement was developed by senior management and is shown here.

EDC's Statement of Credit Risk Philosophy

Due to its unique business mandate, EDC's credit risk philosophy can be best described as follows:

- To fulfill our business mandate, we balance the dual responsibility of maximizing EDC's capacity to help create enduring prosperity for Canada while at the same time safeguarding the corporation's financial sustainability;

- We are prepared to originate/underwrite credit commitments that have a risk profile that may be higher than what would be present at other Canadian credit providers, and hold portfolios of credit commitments at higher concentrations than at other Canadian credit providers;
- At origination, we are committed to the appropriate level of due diligence to ensure that the risks of the credit commitment have been properly analyzed, fully disclosed to the authorizing and endorsing bodies, and appropriately characterized (e.g., rated). We apply leading-edge commercial principles to ensure the credit commitment has been appropriately structured, priced, and documented with the goal of maximizing, when applicable, the marketability of the credit commitment in secondary market activity. We price credit commitments with respect to market practices;
- When originating credit commitments, we recognize the differences between originating commitments within our financial services programs. Generally, the granting of credit within the credit insurance services and some of the contract insurance and bonding services concentrates on the risk/return of pools of credit commitments, while the granting of credit within other EDC lines of business concentrates on the risk/return of the individual credit commitment;
- We strive to manage credit risk and ensure financial sustainability in order to continue to grow and fulfill our mandate;
- We maintain reserve and capital levels adequate to absorb expected and unexpected losses;
- We establish corporate portfolio pricing and profitability objectives that balance EDC's commercial financial requirements and EDC's public policy mandate to provide value-added benefits for Canada;
- We establish credit limits (obligor, country, and industry) to manage portfolio concentrations; and
- We utilize risk transfer abilities to manage credit exposures within portfolio concentration limits and portfolio targets.
- We strive to incorporate relevant credit risk management best practices within EDC where appropriate.

The Credit Risk Policy Manual EDC recognized the need to have documented and approved policies and procedures to ensure that all credit risks are identified, measured, monitored, controlled, and regularly reported to the Board of Directors. The Credit Risk Policy Manual was developed in 1999 and describes EDC's perspective on the prudent origination and management of credit commitments of the corporation's portfolio. The manual is designed to help ensure that EDC will always be in a position to provide value-added commercial financial solutions to companies of all sizes by using its own internal financial resources.

The manual also serves to fulfill the Risk Management Committee of the Board's responsibility to ensure that appropriate policies are in place to maintain an acceptable level of credit risk to the corporation. Credit risk policies remain the oversight responsibility of the Risk Management Committee of the Board, for which Management is responsible for ensuring and reporting adherence.

The manual is divided into three chapters. The first chapter puts the manual and its policies into EDC's context by examining its mission, business objectives, credit risk philosophy, and credit risk principles. The second chapter presents EDC's Credit Risk Policies, each of which are structured as follows: executive summary, purpose, policies and methodologies, exceptions, and reporting to management and to the Board of Directors.

The Policies are as follows:

- Risk Rating Policy
- Credit Granting Policy
- Credit Exposure Measurement Policy
- Country Risk Limits Policy
- Industry and Obligator Risk Limit Policy
- Credit Loss Reserve and Capital Adequacy Policy
- Credit Monitoring and Review Policy
- Credit Portfolio Management Policy
- Risk Transfer Policy
- Management and Board Reporting Policy

The third chapter defines the organizational structure for credit risk management, roles and accountabilities of various departments and committees, and responsibility of maintaining the policies.

The Board of Directors approved the manual and its policies upon the recommendation of the Risk Management Committee of the Board of Directors and EDC management. Management will provide reports to the Board of Directors on a regular basis, evidencing adherence to the policies. The manual will be subject to review and revision on an annual basis to reflect changes in EDC's business environment and evolution in best practices in credit risk management. Management, the Risk Management Committee of the Board, and the Board of Directors acknowledge that full implementation may require several years. Accordingly, management will review the manual and its policies on an annual basis, and recommend any changes to the Risk Management Committee of the Board. All changes to the manual require the approval of the Board of Directors.

In developing the Credit Risk Policy Manual, EDC took a significant step forward in implementing best practices in credit risk management at the organization. This development involved the active participation of various parts of the organization. The Risk Management Office provided the technical resources in drafting the credit policies, as well as gaining business unit support and educating board members through a series of workshops. Senior management, led by CFO Peter Allen in this effort, engaged in healthy debate as to the appropriate credit philosophy and policies for EDC. The board of directors, and the Risk Committee of the Board, allocated significant time in reviewing and approving the credit policies. The EDC case study is a good example of the components of establishing a credit risk policy, as well as one of the key requirements for success—the active involvement of senior management and the board. In December of 1999, the Credit Risk Policy Manual was approved the Risk Committee of the Board, as well as the full Board of Directors.

CHAPTER 13

Market Risk Management

What is market risk? A general definition might be something like the following: Market risk is the exposure to potential loss that would result from changes in market prices or rates. All companies are exposed to some forms of market risk. The level and form of market risk exposure differs by industries, and by companies within an industry. The relevant prices or rates (sometimes called the market risk factors) might include equity or commodity prices, interest rates, and foreign exchange rates. For example, one form of market risk faced by a financial institution would be its exposure to changes in interest rates if the durations of its assets and liabilities are mismatched. Other market risks at financial institutions might arise from proprietary trading and market-making activities.

An international corporation, on the other hand, might be exposed to foreign exchange movements if its offshore revenues and expenses are denominated in different currencies. Even if these were denominated in the *same* currencies, foreign exchange risk would exist when it came to repatriating offshore earnings into the corporation's home currency. An energy firm is exposed to energy price movements if a change in an input price (the price of crude oil, say) is not matched by a change in an output price (the price of petroleum or jet fuel). Additionally, the value of an energy firm's reserves is directly linked to market prices.

While different industries face specific forms of market risks, there are some market risks that are faced by all companies. For example, the performance of a company's investment portfolio directly impacts its financial performance. All companies will only stay solvent by ensuring that all cash obligations can be met by a combination of investment liquidity, funding sources, and contingent liabilities. Another example of a common market risk is the obligation to fund pensions and other defined benefit plans. For example, three years after a period of restructuring in 2009, GM still had a pension fund shortage of $109 billion in mid-2012.[1] General Motors was not alone, as many large corporations have also recently announced large pension losses—in January of 2013, Ford announced an $18.7 billion shortfall.[2]

In this chapter we will discuss the various types of market risk, approaches to measuring and managing it, and best practices today.

TYPES OF MARKET RISK

There are three types of market risk—trading risk, asset/liability mismatch, and liquidity risk. Trading risk encompasses the risks that a company faces in its investment and trading portfolio(s) due to changes in interest rates, exchange rates, equity prices, and commodity prices. The exposures involved in trading risk are short term, and can typically be closed out or hedged over a period of several days. Trading risk is the major market risk faced by investment banks and dealers. Energy firms with market-making activities and non-financial corporations with a trading book would also face trading risk.

Asset/liability mismatch arises from a difference in the interest rate sensitivities of assets and liabilities held on the balance sheet. This interest rate risk is distinct from trading risk in that it is generally less liquid and can therefore only be adjusted or closed out on an infrequent basis, although it can be hedged and re-hedged more often. Asset/liability mismatch is the major market risk faced by commercial and retail banks, though insurance companies and investment banks are also faced with this type of balance sheet risk. For energy firms, the risk of mismatches between input and output prices can also be analyzed in an asset/liability management framework. The same can be said about managing the gap between pension assets and liabilities.

Liquidity risk is the risk that a company will be unable to obtain the funds to meet its financial obligations as they come due, either by increasing liabilities or by converting assets without incurring significant losses. As such, all corporations face this risk. Liquidity risk may occur even in a trading portfolio, when either a large position is unloaded on the market or when trading in thin markets (as commonly found in emerging markets, for instance).

Figure 13.1 illustrates how the three major types of market risk can be further subdivided into individual risk types, some of which overlap: interest rate risk, foreign exchange risk, commodity risk, equity risk, and basis risk. In addition, there will frequently be other (perhaps more complex) risks that arise from a change in a market risk factor.

- **Interest rate risk:** The risk of financial loss due to interest rate volatility. Losses could result from changes in level and/or shape of the yield curve.
- **Foreign exchange risk:** The risk of an adverse variation in return or cost resulting from changes in foreign exchange rates.
- **Commodity risk:** The risk of commodity price fluctuations.
- **Equity risk:** The risk of equity value fluctuations.

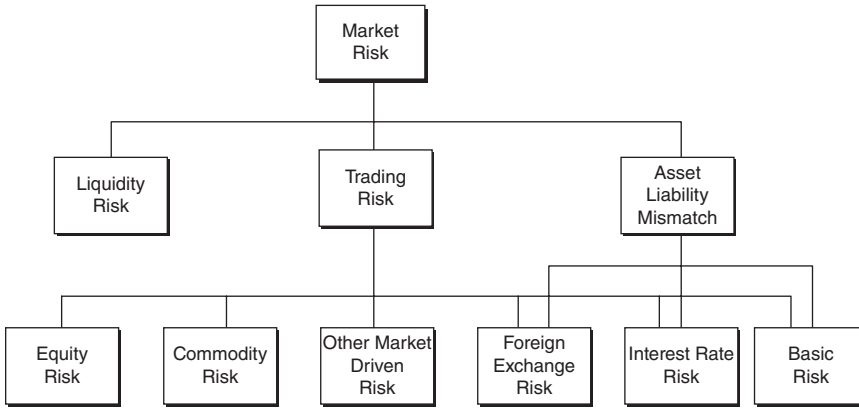


FIGURE 13.1 Types of Market Risk

- **Basis risk:** The risk of changes in the relative rates of two indices, that is, prime rate versus LIBOR.
- **Other market driven risk:** In addition to the most common market risk types listed above, there are other market risks, such as option risks (e.g., prepayment of mortgage loans and securities) and exposures to other market prices (e.g., real estate prices).

A key measure of market risk is Value-at-Risk (VaR), which measures the worst loss that might be *expected* over a given time interval, under normal market conditions and with a given confidence level. VaR is useful because it provides users with a standardized measure of market risk, expressed in terms of the money that might actually be lost. For instance, a bank might report that the daily VaR of its trading portfolio is $30 million at the 99 percent confidence level. In other words, there is only one chance in 100 that a daily loss greater than $30 million will occur, under normal market conditions; it also means in two or three days a year, losses would likely exceed $30 million. We will examine VaR and other useful and widely used techniques of market risk measurement.

MARKET RISK MEASUREMENT

Gap Analysis

Gap analysis is the most common and perhaps the best-understood technique for measuring interest rate risk, despite the limitations discussed below. It can also be applied in policy setting and risk limit definition.

Most large banking corporations present gap analyses in annual reports to discuss their interest rate risk exposures.

In gap analysis, the organization's assets and liabilities are grouped into time buckets according to when they will be re-priced. The difference between repricing assets and repricing liabilities is known as the gap. A negative gap would result if repricing liabilities are greater than repricing assets, indicating a risk exposure to increasing rates. Gap analysis, however, ignores mismatches that exist *within* the various time buckets. For example, repricing assets may equal repricing liabilities within the next year, but over the next month there may still be repricing mismatches. Additionally, gap analysis is usually not an effective measurement tool for more complex interest rate risk factors, including the treatment of accounts that don't have definite maturities (e.g., checking and deposit accounts), administered rate accounts (prime rate loans), basis risk (prime vs. LIBOR), and option risk exposures (mortgage loans and securities).

Duration

Duration is a fundamental technique in interest rate risk measurement, and determines a financial instrument's price sensitivity to changes in interest rates. Mathematically, duration is equal to the weighted-average time when all future cash flows are received, using the present values of such cash flows as weights. Duration captures the effects of differing coupon rates and market yields for debt instruments. An important property is that it is directly proportional to the percentage changes in asset prices that result from a change in market yields. For example, an asset with a duration of five years would drop by roughly 5 percent for every 1 percent increase in rates. Thus, duration can be used to calculate an investment's interest rate elasticity.

However, it only takes into account parallel shifts in interest rates: that is, those where all interest rates move by the same amount (so the three-month rate changes by the same amount as the five-year rate). In real life, shifts in the interest rate curve are often anything but parallel. To capture more realistic changes in the level and slope of the yield curve, other duration measures (e.g., key rate duration) are used to measure an instrument's or portfolio's price sensitivity to changes in various segments of the yield curve.

Value-at-Risk

The concept of Value-at-Risk has rapidly become the industry standard for measuring and reporting market risk in trading portfolios. It translates the riskiness of an entire portfolio into a common standard: the potential loss stated in a single currency, such as U.S. dollars. This simple common standard makes VaR appealing and powerful; it provides a consistent and comparable

measure of risk across all instruments, products, trading desks, and business lines. In 1995, the International Swap and Derivatives Association (ISDA) stated that: "The measure [of market risk] thought to be appropriate by most of the leading practitioners is some form of Value-at-Risk." (see Figure 13.2)

VaR is a measure of the likely loss of market value for a given portfolio over a predetermined confidence level and holding period. That is, there is some fixed probability (the confidence level) that any losses suffered by the portfolio over the holding period will be *less* than the limit established by VaR. There is also a fixed probability that the losses might be worse. The VaR limit does not, therefore, say anything about how bad losses could actually be, and definitely does not specify the worst possible loss—a common misconception. It simply suggests what loss might be suffered on a fairly bad day.

Another way of thinking about VaR is that it draws the line between everyday losses and exceptional losses. Clearly, this makes it useful for considering the everyday risks run by an organization. However, there is as yet no single industry standard for what constitutes a severe loss, and thus no industry standard for what actually constitutes VaR. The Group of Thirty, a think-tank that issued widely used standards for risk management, recommends the use of two standard deviations of daily market movement for calculating VaR, which corresponds to a 97.5 percent confidence level for normal distribution. Another widely used standard, RiskMetrics,[3] defines VaR as the 5 percent event (which corresponds with a 95 percent confidence level) while the BIS stipulates a 99 percent confidence interval. Individual institutions may choose other confidence levels; a level somewhere between 95 and 99 percent is most common. The institution's choice of a particular number is, by far, less important than maintaining a consistent level across the entire enterprise.

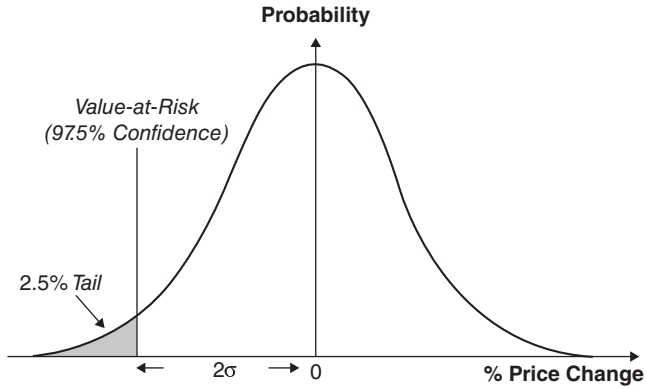


FIGURE 13.2 Illustration of Value-at-Risk

The BIS has developed specific guidelines for the parameters that determine VaR calculation for risk in the trading room (Table 13.1). These choices were determined by the needs of a regulatory agency rather than from the point of view of active risk management in a sophisticated trading operation. As such, the 10-day holding period is unreasonably long for all but the most illiquid securities. Similarly, the BIS-specified calculation method is simple and transparent, but less effective at predicting future volatility than the common approach where market behavior in the recent past is given more weight than the distant past. However, there is nothing to preclude any institution from calculating both a regulatory VaR and a management VaR for internal consumption—most leading players do, in fact, calculate both. Most commercially available VaR systems allow for such dual calculations as well.

The VaR methodology can also be applied to the measurement of balance sheet interest rate risk. A smaller set of risk factors than the trading risk VaR analysis is used, and is restricted to those associated with the yield curves that affect the pricing of the assets and liabilities on the balance sheet. Since the balance sheet represents a longer-term portfolio than those associated with daily trading, a modestly different approach is required. The main difference is that the changes in the risk factors are measured less frequently than the daily measure taken for trading risk measurement.

Calculating VaR

VaR is calculated as the product of three basic factors:

1. The size of the open position at risk, called the exposure amount.
2. The volatility of the price of the instrument, called the price volatility factor.
3. The time required to close out a position following an adverse price movement, called the liquidity factor.

TABLE 13.1 BIS recommended parameters for VAR calculation

BIS Guidelines	
Confidence Level	99 percent, one-tailed
Holding Period	10 days
Observation Period	1 year
Model Type	No particular one, so long as it captures all material risks

Source: Basel Committee, January 1996

The exposure amount is the net exposure of an open position. It is typically calculated for a business unit or for a portfolio that consists of related instruments. The process of marking positions to market is essential to the accurate measurement of exposure amount, and therefore, market risk. Proper aggregation is also crucial to the calculation of exposure amount (e.g., all exposures to changes in the U.S. Dollar/Japanese Yen).

The risk inherent in holding any market position is dependent on the volatility of the underlying market(s). The most important volatility measure is the price volatility factor, which is the best estimate of the future daily volatility of market prices. While historical volatility can be observed, future volatility can only be estimated using past data, judgement about the future condition of the markets, or the implied volatility from traded options.

If a company is dealing with a portfolio instead of just a single asset (which is usually the case), it should include the correlations between market movements, usually estimated by using the historical correlations between each pair of market prices. The company itself can do this, but it is also possible to obtain third-party correlation matrices that cover the most commonly traded market prices. Again, the correlation matrix is ideally a forward-looking measure, so it may be necessary to adjust historical results to reflect current market conditions.

The liquidity factor represents the time (in days) required to liquidate a position in an orderly fashion and in *adverse* market conditions. The fact that abnormally large positions and/or markets that can dry up will require more than a day to liquidate is often overlooked in VaR analysis. In order to incorporate the liquidity factor, the holding period should be adjusted according to the market liquidity of the various instruments.

Three Flavors of VaR

There are three main approaches to calculating VaR: parametric (also called the variance-covariance) approach, Monte Carlo simulation, and historical simulation. Each has its strengths and weaknesses; taken together, they give a more comprehensive perspective of risk. We will describe each of these approaches briefly.

The Parametric Approach This is the simplest approach to VaR. It makes two basic assumptions about price movements and the consequent changes in portfolio value:

1. Changes in risk factors are *normally distributed* and linearly correlated; and
2. The change in value of the portfolio resulting from a change in risk factor is *linear.*[4]

The first assumption simplifies the VaR computation dramatically, although it is not always true in practice. Operating under this assumption, all we need to measure and model is the variance and correlation between assets or instruments. We should then be able to predict the likelihood of severe market fluctuations and their impact on loss. The second assumption is true for some simple financial instruments, but is violated by many other instruments—particularly those with option characteristics. The VaR estimates produced by this approach will therefore be most accurate when the portfolio is mostly comprised of products with minimal optionality (or non-linearity) and price changes are approximately normally distributed.

Despite its limitations, parametric VaR is often a reasonable approximation of a firm's risk profile. For example, the portfolio that brought down Barings Bank was dominated by positions in Japanese government bond futures and Nikkei futures. Not only was this portfolio highly concentrated (there were only two instruments), but it also contained derivative products, albeit of the simplest variety. Nonetheless, parametric VaR would have revealed that rogue trader Nick Leeson had placed almost $1 billion at risk! His final loss amounted to approximately $1.3 billion. Given the unusually large drop in the Nikkei following the Kobe earthquake, the highly concentrated nature of the portfolio, and its high proportion of derivatives, this loss was still remarkably close to the parametric VaR estimate—a number that would have been very useful to senior management at Barings.

Monte Carlo Simulation This method generates a distribution of changes in portfolio value by revaluing the portfolio under a large number of scenarios. Each scenario represents one way that the portfolio's value might evolve over time, with the collection of risk factors changing in a different, randomly chosen way each time. The overall effect of these random changes on the portfolio value can then be found, using the volatility and correlation information described above. A combination of the portfolio values found under each scenario gives an estimate of its likely behavior.

Recall that the parametric approach to VaR rests on the two assumptions of normality and linearity. The Monte Carlo approach relaxes the assumption of linearity. To understand the distribution of changes in value for non-linear instruments such as derivatives, consider Figure 13.3.

Panel A describes the payoff function of an option as the value of the underlying changes; here it is non-linear. The next panel is the normal distribution of the underlying risk factor. Panel C combines the two by describing the distribution of value changes of the derivative product. In simulation, we generate the data for B randomly and re-compute the value of the derivative

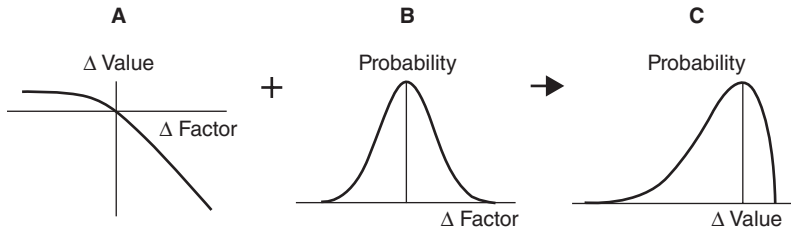


FIGURE 13.3 Non-linearity of Derivative Instruments

product using A to obtain C. Note that C looks rather non-normal even though B looks quite normal. This is because the non-linearity we see in A results in a non-normal distribution of changes in the derivative's value; only a simulation-based approach will capture this.

The Monte Carlo approach is, therefore, most useful when non-linear instruments represent a significant fraction of the total portfolio and where the underlying risk factors are normally distributed. For example, mortgage securities react in a non-linear manner to rate changes due to the prepayment option, yet changes in interest rates are normally distributed. In practice, Monte Carlo simulation is widely used to provide valuation and risk management for holders of mortgage securities.

Historical Simulation This approach to VaR uses historical data about actual price movements to generate scenarios, and then re-prices the portfolio according to these historical scenarios to generate the distribution of changes in portfolio value.

Historical simulation is therefore similar to the Monte Carlo simulation approach, except that the changes in the risk factors are determined by historical experience, not chosen randomly. The historical simulation approach allows the relaxation of both the linearity and normality assumptions of parametric VaR. In addition to the non-linear characteristics of Panel A in Figure 13.3, Panel B becomes non-normal in this case. A good example of a non-normal underlying risk factor is electricity prices, where there can be extreme upward spikes in prices.

Historical simulation is clearly the most generally applicable of the three approaches to calculating VaR, and there seems to be a move toward its use among the most sophisticated global trading houses. Its single main drawback is that we can only use information about market movements that actually did occur in the past—these may not include all the movements that are actually possible, or even likely. To overcome this shortfall, some sophisticated companies have developed a set of stressed scenarios to use in addition to historical scenarios.

Consider an example of a European call option on a futures position in a non-G7 currency—the Mexican peso, say—to compare the three approaches to VaR. The VaR estimates are summarized in Table 13.2. The result implies that the amount of non-linear risk in the position is U.S. $ 7,689 (Monte Carlo minus parametric), and the magnitude of non-normal risk is U.S. $ 3,414 (historical minus Monte Carlo). Note that relying on the computationally straightforward linear parametric VaR underestimates market risk by more than U.S. $11,000.

Estimating the Market Risk of Extreme Events

As we have already seen, VaR is good at describing the type of adverse events that occur perhaps three to four times a year (for an event that has a one-in-one-hundred chance of occurring under daily VaR). However, it is relatively poor at capturing the events that might happen once every five years but can wreak havoc on a portfolio.

There is therefore a need for a different kind of analysis that can tackle the potential impact of extreme events. This kind of analysis, which we will describe below, is called *stress testing* or *scenario analysis*, and is now required by regulators in most jurisdictions. JP Morgan Chase, for example, uses both VaR and stress testing as its principal risk measurement tools: "VaR measures market risk in an everyday market environment, while stress testing measures market risk in an abnormal market environment . . . This dual approach is designed to ensure a risk profile that is diverse, disciplined, and flexible enough to capture revenue-generating opportunities during times of normal market moves, but that is also prepared for periods of market turmoil."[5]

The terms stress testing and scenario analysis are frequently used interchangeably in the context of risk management. However, we will make a subtle distinction in their definitions here. We will consider stress testing as a bottom-up analysis, based on the effect of large changes (shocks) made to key risk factors. On the other hand, we will interpret scenario analysis to be more of a top-down approach, in which we begin by defining an alternate

TABLE 13.2 VaR estimate example

Technique	VaR Estimate
Linear Parametric	U.S. $24,935
Monte Carlo Simulation	U.S. $32,624
Historical Simulation	U.S. $36,038

state of the world (such as a crisis in southeast Asian financial markets), and then draw out the implications for portfolio value. In practice, there is sometimes no clear distinction between stress testing and scenario analysis, but equally, there is sometimes a very clear distinction. In any case, clear definitions will help to sharpen understanding of the issues involved.

Stress Testing

Stress testing quantifies the loss under extreme outlier events, without assigning any *likelihood* to such events or the consequent loss. Its goal is to provide insight on the portfolio behavior that would result from large moves in key market risk factors: What if the Fed announced a 50-basis-point increase in interest rates? Or what if the price of oil doubled? How would a 30 percent devaluation of the Thai baht affect portfolio profit and loss (P&L)? All of these events, although very unlikely under normal conditions, are certainly possible, and can quickly become more likely as conditions change.

The process of stress testing therefore involves identifying these potential movements, including which market variables to stress, how much to stress them by, and what time frame to run the stress analysis over. In general, stress testing involves the following steps:

1. Determine which variable(s) should be stressed and to what level(s)
2. Develop assumptions for price correlations within the portfolio
3. Measure the impact of the stress test on the portfolio
4. Develop alternative strategies that can be implemented
5. Evaluate the cost benefit of each alternative strategy

In 1995, the Derivatives Policy Group (DPG) published "A Framework for Voluntary Oversight" to address derivative activities by U.S. brokerage firms. Among other things, the DPG proposed standards for the stress-testing of key risk factors and their impact on P&L:

- Parallel yield curve shifts of 100 basis points (bp) up or down
- Steepening and flattening of the yield curves (2s and 10s) by 25 basis points
- Each of the four permutations of parallel yield curve shift of 100 bp concurrent with a tilting of yield curve (2s and 10s) by 25 bp
- Increase and decrease in all three-month yield volatilities by 20 percent of prevailing levels
- Increase and decrease in equity index values by 10 percent
- Increase and decrease in equity index volatilities by 20 percent of prevailing levels

- Increase and decrease in exchange value (relative to the U.S. dollar) of foreign currencies by 6 percent for major currencies and 20 percent for other currencies
- Increase and decrease in foreign exchange rate volatility by 20 percent of prevailing levels
- Increase and decrease in swap spreads by 20 bp

These analyses represent the typical stress tests that are carried out by various financial institutions. However, it is critical that companies develop a stress-testing methodology that is customized to their own portfolio and business environment, and not rely on standard tests.

Scenario Analysis

Scenario analysis typically goes beyond the immediate effects of predefined market moves and tries to draw out the broader impact that events may have on the revenue stream and business. It is meant to help management understand the impact of unlikely but catastrophic events, such as major changes in the external macroeconomic environment that will have an effect well beyond any immediate impact on the value of a trading portfolio. The crises triggered by the 1998 Russian debt restructuring, 1997 Thai baht devaluation, and 1994 Mexican peso devaluation are historical examples of extreme situations where the tried-and-tested assumptions made in the past simply ceased to apply.

The design of scenario analysis is a complex and difficult process that typically draws on the expertise of many people with diverse backgrounds in various departments. It is a very subjective way of assessing the long-term strategic vulnerabilities of a firm. The following are some guidelines for effective scenario analysis:

- **Defining scenarios:** The first step is to define a plausible scenario. There are two ways of doing this. The first is to consider historical situations (such as the 1987 stock market crash, 1994 Mexican Peso crisis, 1995 Kobe earthquake, and 1997 Asian crisis) and what would happen if something similar happened today. The second is to imagine entirely new circumstances that might be caused by catastrophic events (such as a natural disaster or war) or long-term changes in the macroeconomic climate (such as a U.S. recession or failure of European Monetary Union [EMU]). One way to generate such scenarios is to ask business managers or traders what the worst thing they could imagine for their business might be.
- **Inferring risk factor movements from the scenario:** Once a scenario (or set of scenarios) has been chosen, the second step is to identify all the

relevant risk factors that will be affected by the scenarios, and the magnitude of the effect that the scenario will have. For example, a crisis in the Middle East might be modeled in terms of a set of shocks to foreign exchange rates, to the yield curve, and to oil prices.

- **Responding to the results:** The next step involves defining the early warning indicators that would precede the scenario(s) and the management actions that should be taken in response. The scenario analysis reports should be circulated to line managers, risk managers, and senior management. Specific action plans and hedging strategies should be developed to address any high concentrations or exposures that are identified.
- **Reviewing the scenarios periodically:** Once a scenario analysis has been developed, the methodology should be reviewed periodically (quarterly, for instance) to see if it needs to be modified due to changing portfolio or market conditions.

Verifying the Measurements: Back-Testing

Back-testing is the practice of comparing results of valuation or risk models to historical experience to evaluate the accuracy of the risk analysis. In other words, if the analysis had been carried out at some point in the past, would it have provided useful information in the light of what actually did happen next? This process is a critical part of the market risk control. There are three key objectives of the tests:

- To test whether the software and database have been properly installed and implemented
- To test whether the modeled probability distribution (VaR) is consistent with experience
- To test whether the modeled P&L matches actual P&L

If actual results are materially different than modeled results, then risk management determines the underlying reasons, such as the methodology used by the model, the integrity of data and assumptions, or simply unexpected market behavior. Regulators also require back testing. For example, banks operating under the Basel Committee's 1996 rules on trading risk may be allowed to use their internal VaR models to calculate their capital requirements. If they do, they are required to review the accuracy of the model-generated estimates by back-testing its results at least quarterly. More specifically, the actual trading results over the prior 250 trading days are compared to the bank's daily VaR and the number of times that an actual loss exceeded daily VaR is noted. As shown in Table 13.3, the number of exceptions then determines the capital multiplier over 250 days.

TABLE 13.3 Back-testing results determine capital requirement

Exceptions in 250 Days	BIS Zones	Capital Multiplier
0		3.0
1	Green Zone	3.0
2		3.0
3		3.0
4		3.0
5		3.4
6	Yellow Zone	3.5
7		3.65
8		3.75
9		3.85
10 or More	Red Zone	4.0

Source: Basel Committee

This approach—to count the actual number of exceptions—is a simplified test, and financial institutions should consider developing their own criteria for back-testing. The audit function may be ideally suited to provide an independent test. The back-testing process must establish the appropriate time periods, variables (e.g., VaR, P&L), and acceptance levels. If back-testing reveals a failure of the risk analysis, there should be an immediate model and methodology review.

Conditional Value-at-Risk (CVaR) or Expected Shortfall

While VaR provides a consistent cross-business, cross-product measurement of risk, it underestimates asymmetrical and fat-tail risks. As an indication of this inherent weakness, actual losses can exceed 95 percent VaR levels about 5 percent of the time, which amounts to 12 days per year. Some firms even report exceeding VaR limits up to 30 days per year.

To address this issue, many firms compute conditional VaR (CVaR)—also known as expected shortfall, tail VaR, and expected tail loss—which represents the expected loss in a portfolio given that the risk event is occurring beyond the VaR confidence level. CVaR can be an effective tool to measure potential losses under extreme market conditions. Moreover, the ratio of CVaR to VaR can provide a useful estimate of the tail skewness of a distribution curve. Consider the two different risk distributions in Figure 13.4.

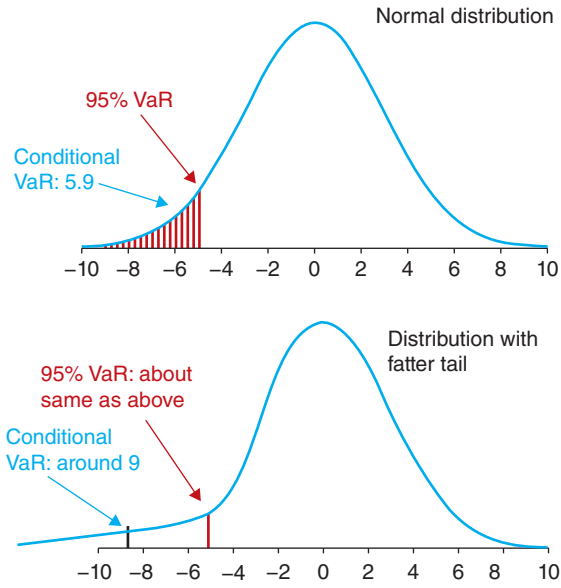


FIGURE 13.4 VaR and CVaR

The CVaR/VaR ratio for the top bell curve would be 1.2 (5.9 ÷ 5), while the ratio for the bottom bell curve would be 1.8 (9 ÷ 5); hence, we can see that a higher CVaR/VaR ratio reflects a fatter tail of an asymmetric loss distribution.

While VaR has been widely recognized as an industry standard of risk measurement since the 1990s, its credibility was greatly diminished during the financial crises of the late 2000s. This, rather unpleasantly, made us realize that stressed markets can cause devastating effects that are far beyond the scope of what we are capable of measuring and predicting with stress-testing models like VaR.[6] The VaR forecasts were so off the mark that the Basel Committee actually altered its regulatory approach in 2012 to replace VaR with expected shortfall, which "generates a diversification benefit"—a quality that VaR lacks.[7]

However, there are many who do not believe that this shift from VaR is a positive one. Jesper Andreasen, head of quantitative analytics at Danske Bank, asserts that there is no point to this change, because the problem of VaR lies in its "calculation methodology," which involves a "250-day boot-strapping of historical data." Switching out of VaR without changing this fundamental structuring will simply carry the issue into the expected shortfall framework, which does not help at all.[8] CRO of AQR Capital Management, Aaron Brown, further condemns the movement by claiming

that VaR is actually more reliable than expected shortfall, because people recognize what it stands for, know how to use it, and still trust it.[9]

Two Useful Rules of Thumb

When working with VaR models, there are two straightforward rules of thumb that may be quite useful to keep in mind. The first helps to estimate the number of days that a mark-to-market loss could exceed VaR. This can be approximated by the following formula:

[100 percent minus confidence level] × 250 = expected number of days that the daily mark-to-market loss will exceed VaR

The 250 used in the formula represent the number of trading days in a year. For example, if the confidence level used in the VaR model is 95 percent, then the expected number of days that losses could exceed VaR would be 12.4 [(100 percent – 95 percent) × 250].

The second rule of thumb helps convert a daily VaR estimate to another time period by simply multiplying the daily VaR by the square root of the new time frame. The square root function is widely accepted as a quick approximation of how volatility increases relative to increases in the observation period. For example, if the 1-day VaR is $5 mm, then to calculate the 10-day VaR, multiply $5 mm by $\sqrt{10}$: $5 mm × 3.2 = $16 mm. The same concept applies to calculating economic capital for market risk. In this case, the time period would be 250 (the number of trading days in a year): $5 × $\sqrt{250}$ = $79 mm.

MARKET RISK MANAGEMENT

Although risk management cannot *eliminate* losses, it is nonetheless crucial, as it can ensure a company's awareness of, and comfort with, the level of risk that it is undertaking. This chapter is devoted only to market risk, but it is important to keep in mind that market risk management should be considered together with strategic and business risk, credit risk, and operational risk in an enterprise-wide risk management framework.

Market risk management, like credit risk management (which we discussed in the previous chapter), requires participation on the part of five main groups of the company: the board and senior management, front office, back office, middle office/risk management group, and audit. While the different groups play different roles in the risk management process, each group's effort is essential for the proper control environment. The elements

of market risk management include policies, limits, reporting, economic capital management, and portfolio strategies. We will discuss each briefly.

Policies

Like credit risk, an organization should have documented policies on market risk to ensure that all market risks are identified, measured, monitored, controlled, and regularly reported to senior management and/or board of directors. These documents reflect the firm's perspective on the prudent management of market risks, and should be approved by the board of directors. Such policies should take into account the nature and complexity of the firm's activities, business objectives, competitiveness, , the regulatory environment, and its staff and technological capabilities.

The human side—or the soft side of risk management—is important to consider. Neither VaR, nor any other more or less sophisticated risk measurement technique, will safeguard against incompetent or rogue traders. Many of the most significant trading losses of recent times can be more accurately considered as fraud or other forms of operational risk. A risk measurement system cannot replace strong governance and audit processes; market risk policies should be therefore monitored to ensure compliance on a regular basis. The policies should also be reviewed periodically to take into account internal and external changes (e.g., new financial products, new markets, and changes in regulatory environment).

There is no single set of market risk policies that is applicable to all companies. Rather, policies should be tailored to the investment, funding, and trading activities of the company. There are two important benefits to establishing any risk management policies. First, the process of developing a risk policy facilitates management discussion of, and consensus for, important issues. Second, the end product is a document that clearly lays out how risk management will be performed within the company. In general, market risk policies should cover the following areas:

- *Roles and responsibilities:* This section should define who is responsible for each aspect of market risk management within the company, as well as the organizational and reporting lines. For example, the board reviews and approves risk policies and limits, the treasury and trading units develop the strategies, and the risk management unit monitors and reports on overall portfolio risks. Review and approval processes should be developed for new businesses and products, as well as new trading strategies and new models. In addition to the responsibilities of individual functions and units, the structure and charters of various market risk committees should be established.

- *Delegation of authority and limits:* This section should specify who is permitted to execute market risk positions for the company, including specific authorities with respect to individuals, types of products and strategies, transaction limits, and approval processes. Most companies have centralized the authority to execute capital markets and derivative transactions within a few organizational units. Explicit risk limits should be defined for each type of market risk exposure faced by the company. Another key control procedure is to segregate the functions that initiate the trades, and the functions that execute and record the trades.
- *Risk measurement and reporting:* The metrics, methodologies, and assumptions for various market risk measures should be defined to ensure that there is a consistent measurement of portfolio risks against policy limits. Reporting and escalation procedures should also be established in terms of periodic reporting of key measures to specific executives and committees, as well as immediate escalation of critical issues (e.g., limit violations, unauthorized trading activities, etc.). This section is critical to the board and senior management, who rely on other people and functions to inform them of critical risk exposures and trends.
- *Valuation and back-testing:* Accurate and timely financial statements and risk reports are prerequisites for effective market risk management. As such, this section should define how positions are marked to market when actual market prices are obtainable, and how they are marked to model when they are not. For example, some companies require at least three bids to establish a new valuation. A company should also define what prices are used (i.e., bid, offer, or mid) for various positions. Back-testing procedures and criteria should be developed for model-generated prices to ensure that they truly reflect the underlying value of the instruments.
- *Hedging policy:* A hedging policy defines the type of risks that are to be hedged, the target risk levels, and the products and strategies that can be used. A definition and measurement of hedge effectiveness should be established so that management can be assured that the hedging programs are accomplishing their objectives. If hedging strategies are not performing as expected, then that should trigger a review and resolution process. Many companies encounter hedging losses because they didn't have a hedging policy in place that required them to understand the products, as well as the objectives and risks of the underlying hedging strategies.
- *Liquidity policy:* The management of the company's liquidity is one of the most important aspects of a market risk policy. This section should define what measures are used to monitor the liquidity position of the company. Measuring liquidity is not straightforward. Alternatives range

from balance sheet measures (e.g., liquid assets minus short-term liabilities), cash flow measures (sources and uses of cash), and scenario-based measures (in the event of a downgrade in the company's debt rating). In addition to liquidity measurement, this section should establish target liquidity positions as well as the contingency plans that can be executed during financial distress.

- *Exception management:* A market risk policy should also establish how exceptions are handled and reported. For example, what happens when a market risk limit is exceeded due to large market movements (versus new trading activities)? One management response would be to reduce the risk position immediately, while another would be to reduce the risk position over a pre-determined period of time. Some exceptions are intentional, such as those to accommodate a legitimate customer request. Regardless, this section should provide specific guidelines on the monitoring and reporting of exceptions, as well as the processes for approval and resolution.

BEST PRACTICES IN MARKET RISK MANAGEMENT

Of the three risk management disciplines—credit, market, and operational—market risk management is perhaps the most mature with respect to industry standards and best practices. As we did with credit risk in the previous chapter, we will discuss the range of market risk management applications in three categories: basic practice, standard practice, and best practice.

Basic Practice

At the most basic level, a company evaluates the earnings impact of various market risk factors, such as interest rate and foreign exchange changes. Gap analysis is performed between re-pricing assets versus liabilities, or projected revenues versus expenses denominated in a foreign currency, which is then used to estimate how a change in a market variable will likely impact the company's earnings. To manage the company's market risk exposures within policy limits, asset/liability management and hedging strategies are developed and executed. This level of market risk analysis is generally what is required for regulatory and public reporting purposes. The use of market risk models is limited to spreadsheet models or basic vendor models.

The market risk management function is mainly a policy, analysis, and reporting function. It establishes the market risk policies and limits, analyzes the company's risk exposures against these limits, and provides risk measurement and hedging reports to senior management. The line and treasury

units usually perform the execution of balance sheet and hedging strategies. As a monitoring and reporting function, the performance of the market risk function is dependent on its policy development, reporting effectiveness, and analytical skills with respect to earnings volatility estimation.

Standard Practice

Standard-practice companies have developed more robust modelling capabilities, including VaR, earnings and equity-value sensitivity analysis, and simulation capabilities. These companies also have implemented internal transfer pricing mechanisms so that all interest rate risks and foreign-exchange (FX) risks are consolidated and centrally managed. This way, internal hedges are considered before external hedges are executed, thereby saving on hedging costs. Financial engineering capabilities are also developed to evaluate the risk/return trade-offs of different market risk strategies. Beyond risk limits, market risk policies establish targets and ranges (e.g., target duration of equity of five years, with a range of three to seven years) so that the investment and/or market risk functions can take advantage of market opportunities.

The market risk function at standard-practice companies manages the balance sheet much more actively. It implements balance sheet strategies—including investment, funding, and hedging transactions—that optimize financial return given market risk constraints. Earnings derived from the assumption of interest rate risk and FX risk exposures, as well as all hedging costs, are recorded in a central market risk book. As such, the market risk function has a P&L but its corporate mandate is not to maximize profits. The performance of the market risk function is therefore determined primarily by compliance with policy risk limits and secondarily by the earnings derived from the market risk book.

Best Practice

At best-practice companies, market risk management is both a corporate control function and a full-fledged profit center. As a corporate control function, market risk management ensures that changes in market prices and rates do not result in excessive losses. As a profit center, the market risk function(s) that reside in trading, investment, and treasury units also seek to maximize their profits within the risk limits established by the corporate control function. These companies have developed very sophisticated real-time trading and risk management tools that allow them to take advantage of mispriced securities in the global capital markets. They also seek a competitive edge by developing better research, more advanced analytical

models, and more timely market intelligence based on access to deal flow information.

For these best-practice companies, sophisticated market risk management represents a core competency. Any slight advantage, such as the early discovery of an arbitrage opportunity, or the development of a more accurate mortgage prepayment model—can mean millions of extra profits. Examples of these advanced risk management tools include:

- *Hot spot analysis* refers to the process of desegregating the total portfolio risk (measured by portfolio VaR or portfolio volatility) into contributory components. The breakdown of the risk can be done along one or more of the following dimensions: risk factors, asset class, geography, trading desk, instrument class, and positions.
- *Best hedge analysis* refers to the calculation of the amount of purchase or sale of each asset that is required to reach the risk-minimizing position in the portfolio. This tool can support optimal hedging of the portfolio given changes in the balance sheet and hedging costs.
- *Best replicating portfolio* is a simplified representation of the overall trading portfolio of a company in the form of a small combination of assets that replicate the primary risks of the portfolio. By summarizing the risks in just a few assets, the report demonstrates the market views expressed in the portfolio.
- *Implied view* (or implied bet) analysis takes the current portfolio as input, and reverse engineers a set of implied views on asset returns. This way, management can clearly see which market trends would most benefit (or hurt) the current portfolio.

Unlike credit risk and operational risk, which are skewed with a significant downside and limited upside, the risk/return profile of market risk is more symmetrical. As such, the role of the market risk function—as a corporate control function, a profit center, or both—is a fundamental question that is critical for the board and senior management. For companies that take on significant market risks, the culture of the market risk function is also critical. In contrast to the many stories of large market losses due to unauthorized trading, or aggressive traders who double down on their losing bets, my favorite and factual story is about a trading desk manager. One day, a senior trader at a major investment bank produced a daily profit that was twice his daily trading limit. When the trader could not produce a good answer as to why he exceeded his limit the manager fired the trader on the spot. A lesser manager would have simply looked the other way. I would take this trading desk manager with less sophisticated tools over a manager with less integrity and the most advanced tools.

CASE STUDY: MARKET RISK MANAGEMENT AT CHASE

Chase Manhattan (subsequent to the writing of this case, Chase acquired JP Morgan to form JP Morgan Chase), one of America's largest banks, has a venerable history. It can trace its antecedents all the way back to a water-supply company founded in 1799, but the current institution is, by and large, the product of two mergers, each the largest in US banking history at the time. The first was the 1991 merger of Manufacturers Hanover and Chemical Bank; the second, the 1996 merger of Chase Manhattan (founded in 1877) and Chemical Bank (founded in 1823). This Chase Manhattan is a holding company operating three main lines of business:

1. The Global Bank, which offers commercial and investment banking services,
2. Global Services, which offers processing and settlement; and
3. National Consumer Services, which serves retail customers through a wide variety of financial products and services.

During the 1999 fiscal year, Chase boasted more than $400 billion in assets, operating revenue of $23 billion (up 17 percent from $20 billion in 1998), operating earnings of $5.4 billion (up from $4.0 billion in 1998), and return on average common shareholders' equity of 24 percent.

Chase attributes this performance to a number of factors. Prominent among these is a highly successful risk management system that emphasizes the creation of shareholder value and links it to employee compensation. It claims to view risk as a central aspect of its business and risk management as an area of competitive advantage. This assertion is supported by the fact that it devoted 19 of the 94 pages of its 1999 annual report to risk management. As the Chairman's letter states:

> *Let me begin by stating the obvious: We are in the "risk" business, and managing risk smartly and proactively with sophisticated risk management systems can create significant strategic advantages.*

This may be stating the obvious, but it certainly helps to set the tone for the organization. Risk management at Chase focuses on the following principles and activities:

- Formal definition of risk management governance
- Risk oversight independent of business units
- Continual evaluation of risk appetite, communicated through risk limits
- Diversification

- Disciplined risk assessment and measurement, including Value-at-Risk analysis and portfolio stress testing
- Allocation of economic capital to business units and measuring performance on the basis of shareholder value-added (SVA)

Three committees carry out the above activities: one dedicated to credit risk, one to market risk, and one to capital. Their responsibilities are summarized in Figure 13.5, and each has decision-making authority within these areas. The Executive Committee, however, takes responsibility for major policy decisions, determines the company's risk appetite, and formulates the company's risks; it in turn reports to the Risk Policy Committee of the Board of Directors.

Chase's Market Risk Management Group employed some 70 professionals around the world prior to its merger with JP Morgan. The group's mandate is to develop appropriate risk measures, set and monitor limits, and keep the company's risk profile within the boundaries of the risk appetite mandated by the Board. Part of the reason behind the team's success

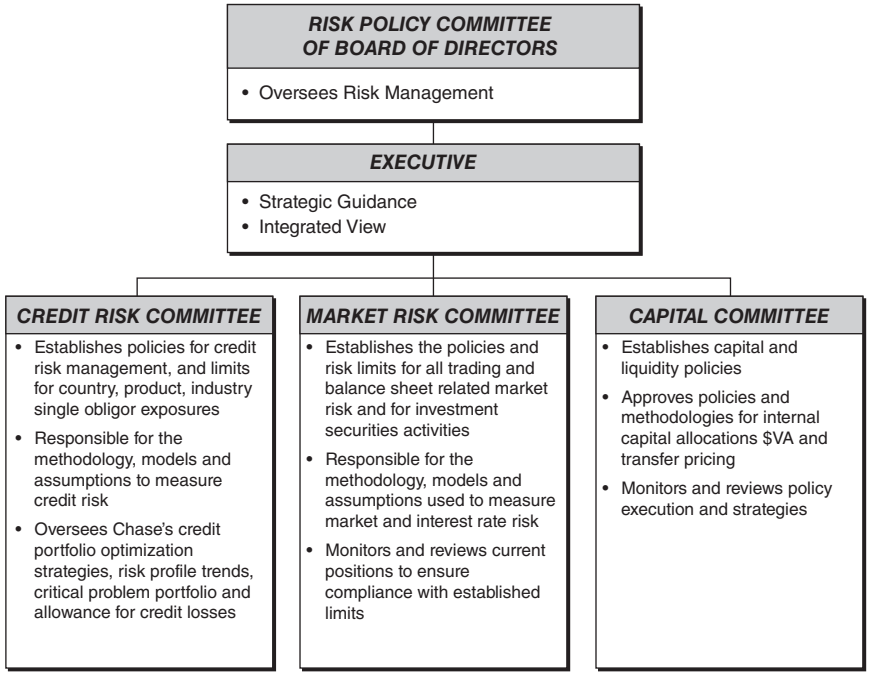


FIGURE 13.5 Chase Manhattan's Risk Management Structure

is that it was born out of the global markets business, not from a traditional watchdog like audit, credit, or compliance. The market risk management approach also strives to balance business and risk management needs, and was developed by Don Layton and Lesley Daniels-Webster, both from the business side.

Development of the market risk group accelerated sharply with the 1996 Chase/Chemical merger. Daniels-Webster, now executive vice president and head of market risk management, said that the merger came at a fortuitous time—technology had just reached the point where it was possible to take the huge book of business created by the merger and evaluate it from the bottom up, position by position. Neither company's legacy systems were up to the job, however, and it was the bank's willingness to spend heavily on new technology that proved critical.

The market risk group continues to enjoy the backing of Layton, now vice-chairman of global markets, and Marc Shapiro, vice-chairman of finance and risk. "Having these two senior people behind us gives us a lot of credibility, changing our role from one that's there for the sake of the regulators to one that is there for adding value to the business units," says John Duddy, a managing director of market risk management. The group manages the market risks generated on a number of different fronts:

- Market risk in its trading portfolios due to changes in market prices and rates (i.e., interest rate risk, foreign exchange risk, equity risk, and commodity risk)
- Asset/liability mismatch in its investment and commercial banking activities
- Basis risk in trading, investment, and asset/liability activities

The bank recognizes that market risk measurement and management should extend across all three of these activities. It learned that lesson fairly cheaply back in 1994, according to Daniels-Webster. During that year, the Fed raised interest rates repeatedly and somewhat unexpectedly, with one result being considerable disruption in the market for mortgage-backed securities.

"What we found was that we were fine on the trading business side, but one of our small S&Ls [savings and loans] that was state chartered had invested its primary capital in MBSs [mortgage-backed securities]," says Daniels-Webster. "The financial impact was very small, but what turned out to be much bigger was that we learned that you can't just look at a firm like Chase just in terms of trading activities." That helped redefine market risk management in terms of the total economic return of an activity, not just its mark-to-market accounting valuation—a definition that ties into Chase's goal of pursuing and managing shareholder value.

Risk Measurement and Management

Chase does not believe there is a single statistic that captures all aspects of risk and therefore employs a number of complementary metrics. These include value-at-risk (VaR), stress-testing, and non-statistical measures such as net open positions, basis point values, option sensitivities, position concentrations, and position turnover. These non-statistical measures provide extra information about the size and direction of risk exposures that can be particularly useful when the statistical measures break down (in anomalous market conditions, for example).

Chase views stress testing and value-at-risk as equally important in managing revenue volatility. Recognizing that value-at-risk numbers change relatively little once their calculation is well established, and say relatively little about the potential extremes of loss, Chase is more actively interested in stress tests. "Stress testing is the backbone of our risk management, not VaR," says Duddy. "The beauty of VaR is that once you agree upon the statistical process, there's nothing to argue about. With stress testing, it's something that's really evolving. It's a very key part of our risk management tools to the extent that we allocate capital based on it."

Stress tests are built around both actual events (e.g., the 1994 bond market sell-off, the 1994 Mexican peso crisis, and the 1998 liquidity crisis) and hypothetical economic scenarios. As of December 31, 1999, Chase was using six historical and five hypothetical scenarios to perform stress tests about once per month. The tests assume that no actions are taken during the event that change the company's risk profile, a premise which simulates the decreased liquidity that is often seen during market crises. Each stress scenario is extremely detailed, specifying more than 11,000 individual shocks to market rates and prices and involving data on more than 60 countries. Stress tests are performed on all material trading, investment, and asset/liability (A/L) portfolios. Chase believes that one key to successful stress testing is the continuous review and updating of scenarios to ensure that they remain relevant and are as detailed as possible.

Chase's VaR methodology is based on historical simulation, reflecting a belief that historical changes in market indices are the best predictor of possible future changes. VaR calculations are performed daily on end-of-day positions, using the most recent one-year historical changes in market prices. The historical simulation is performed on individual positions as well as on aggregated positions by business, geography, currency, and type of risk. Because it realizes that historical VaR is dependent on the quality of the data available, Chase performs back tests for its VaR estimates against actual financial results and uses confidence intervals to examine the reasonableness of its VaR calculations.

The bank manages the market risks that it has measured through the use of various types of limits, approved by the Board of Directors as falling in line with the risk appetite desired by the bank. The limit structure is specified at both the aggregate and business unit levels, going down as far as desk-level activities; it addresses authorized instruments, maximum tenors, statistical and non-statistical limits and loss advisories, and is based on relevant market analysis, market liquidity, prior track record, business strategy, and management experience and depth.

Risk limits are updated at least twice a year in order to reflect changes in trading strategies and market conditions. Chase uses stop-loss advisories to inform line management of losses that are being sustained. A review of the portfolio is automatically triggered if a Board-approved limit is breached. Chase believes that these procedures for tracking limits significantly reduce the likelihood that the daily VaR limit will be exceeded under normal market conditions.

Obstacles and Successes

One of the barriers to implementing the market risk program is the tension that arises naturally between risk managers and traders. This tension is usually a healthy one, ensuring that the bank balances business and risk objectives, but care must be taken to ensure that it does not turn into conflict or disregard for the rules. The problem tends to be at the desk level or below; senior business managers tend to understand and trust the risk managers more than those whose dominant concern is hitting their performance targets.

One way to deflate this problem is to make sure that risk management helps good, if complex, trades to get done, and does not just stop potentially troublesome ones. "We're like cops. If someone tries to rob you and we're there, you love us," says Duddy. "But if you're speeding and we catch you, you hate us." If the risk managers can persuade the traders that they want them to make money—but safely—they gain credibility.

A good example is unusually large transactions. "One-off trades undertaken for reasons of market opportunity or client demand usually involve hedging, structuring, and pricing issues such that we can either wring the risk out of it or price it smartly," says Daniels-Webster. Balancing the academic smarts of the risk managers with the market experience of the business managers can reap great rewards in this respect.

The most obvious evidence of Chase's success in implementing market risk management is the strength with which the company weathered the market turmoil of 1998. For that year, Chase reported earnings of $4.02 billion, up some 4.4 percent from the prior year. Chase had recorded

larger rises in other recent years, but the circumstances of 1998 made it remarkable that it posted any increase at all; many of its peers and competitors suffered significant losses.

Chase's success in weathering the collapse of the Russian economy in 1998 can be attributed to two of the guiding principles of its risk management program: the value of learning from the past and the importance of stress testing. Until 1997, Chase had aimed to lose no more than $500 million in the event of market turbulence. That year, however, it lost around $100 million in Latin American trading. That alerted it to the possibility that losses might exceed $500 million fairly quickly under extreme market conditions, and that its risk exposure was therefore greater than it had believed. The company reset its target loss limit to $250 million. The second lesson that Chase gleaned from this incident was that financial blowups could be global in nature, contrary to the previous assumption that economic problems in one part of the world would be unlikely to affect the performance of financial positions in another part of the world.

This realization was, in turn, a factor in Chase's decision to begin stress testing its entire trading and loan portfolio in late 1997, using scenarios that included global incidents. Stress testing using hypothetical scenarios enabled Chase to counterbalance the historical dependence implicit in its use of historical simulation in its VaR methodology. "We started doing these stress tests and got a number of about $500 million, which was a shock," remembers Daniels-Webster. "We didn't know what to do with such a large number except be skeptical of it."

The tests were soon borne out, however, as the economies of South-East Asia started to nose-dive in fall 1997. Chase's losses looked very similar, if smaller, than those predicted by the stress tests. The post-mortem proved a turning point in the risk management group's interaction with the business units. "This was the cultural watershed where people who didn't want to lose their jobs, who wanted discipline in their business, turned around and said they really needed these stress tests to understand the vulnerabilities in their businesses and hedge them."

Chase had no more inkling than any other bank that the 1997 Asian crises would rumble on into 1998, lead to a global drought of liquidity, and briefly threaten the stability of the global financial markets. However, it had prepared for a general scenario that coincided remarkably well with what actually happened—a sudden, pronounced flight to quality as investors swarmed out of stocks and into bonds and liquidity all but vanished in many markets. Because Chase had already used stress testing to examine the impact this event would have on its portfolio and had taken steps to mitigate its risks accordingly, its losses were less than they otherwise would have been.

While the company did take a $200 million charge related to the liquidity crisis, the changes the company had made to hedge against such a crisis put the bank in a strong position to take advantage of the financial opportunities that followed the panic. Its diversity and business mix (for example, the lack of a large equity business), coupled with sound risk management, put it in a strong position to carry on with its business. This allowed it to capitalize on market opportunities that others were too paralyzed to take advantage of, such as the plentiful opportunities for lucrative foreign exchange trading in October 1998. While competing banks stopped extending credit to clients during the market crisis, Chase continued to lend, a move that the company believes increased its prestige, won new clients, and increased business from existing customers.

A Look to the Future

The Russian crisis did leave its mark even on Chase, however. "A business that runs the same notional risk today as it did in 1997 will generate much more stress risk now, since we now include that scenario in our stress-testing," says Duddy. A simple business goal—growing back to the volume of business done before Russia—is therefore not easy to achieve. One of the market risk group's new challenges is finding ways for that to happen.

Another new frontier for the market risk group is in addressing the increasingly liquid loan market. "It is extremely important to look at credit risk from the perspective of loss upon default. The market is evolving very rapidly into a much more transaction-based and market-based approach," says Daniels-Webster. For Chase, a market leader in loan syndication, it is extremely important to stay abreast of this evolution. The concept of risk as variation in economic value is key here; not only in recognizing the differences between loans, but also in the differences between loans and other credit instruments such as bonds. The next challenge will be to meaningfully integrate the market and credit risk management of the loan book.

CHAPTER 14

Operational Risk Management

In many respects, operational risk is nothing new. Businesses have had to deal with human fallibility, defective processes, and unreliable technologies since time immemorial. However, the advent of enterprise-wide risk management, the introduction of new regulatory capital requirements, and the increasing emphasis on sophisticated quantitative models for other types of risk (such as market and credit risks) has jump-started interest in more active management of operational risk.

Operational risk has been the subject of increasing management attention over the past few years. A 2011 report by Deloitte found that about 66 percent of the surveyed financial institutions calculated economic capital for operational risk as well as credit and market risks, while 69 percent would prioritize improvements in operational risk management systems in the subsequent year (ranked third most important in a list of 12 different priorities).[1] An earlier study shows that 45 percent of the companies surveyed named the CEO (in addition to high-level management) as the spearheading force behind operational risk management initiatives.[2] These figures signify how business executives have come to see operational risk as just as important as other forms of risk. With corporate scandals (e.g., Enron, Worldcom, J.P. Morgan), the interest level in operational risk management has continued to grow, in conjunction with related discussions regarding corporate governance and compliance.

Is this interest justified? Operational risk has traditionally been managed informally, as part of the everyday work of a manager who might never have even considered that part of his or her job as an exercise in risk management. Beyond day-to-day management, operational risk issues are generally addressed through traditional audit and compliance functions. However, the episodic approach used by audit and compliance functions often results in operational risks being identified at a later stage.

There are three major reasons why a more focused and proactive approach is desirable. First, investigations of the major financial disasters

over the past two decades (e.g., Barings, Kidder, Daiwa, UBS, Société Générale) have identified operational risk issues as the main culprits in the majority of these cases. As such, senior management recognizes that operational risks must be addressed as part of any enterprise risk management program. Second, operational risks are often interrelated with credit and market risks, and an operational risk failure during stressed market conditions can potentially be very costly. For example, in the Barings case it was the confluence of events—ineffective management oversight of its Singapore trading operations and a steep drop in the Nikkei after an earthquake—that bankrupted the 233-year-old bank with a billion dollar loss. And third, if operational risk is not managed as a distinct discipline of risk, it tends to be managed differently in different areas of the company. This lack of consistent treatment can lead to the neglect of key risk issues and to a bias in various performance measures that may ultimately lead to management decisions based on inaccurate information.

Operational risk is an inherent part of any business. In many businesses, a significant portion of revenue is systematically lost due to run-of-the-mill processing errors and human mistakes. In addition to these everyday losses, businesses also face operational risk incidents of greater magnitude. Some of these events are unintentional, the result of accidents and failures, while others are intentional, such as in the case of fraudulent or other criminal activity. For instance, in 1994 and 1995, Citibank sustained losses totaling $1 billion as an outcome of three separate events—a wire transfer error, a failure of loan approval controls, and a computer hacking incident. Other potent examples of what can happen when controls over operational risk are lacking include the widely publicized collapse of Barings Bank in 1995 because of one rogue trader, and the alleged fraud that caused the demise of Kidder, Peabody in 1996. Bankers Trust and Enron, two remarkably similar corporate disasters that spanned two volatile industries, failed due to operational risks. Ironically, both companies were once considered leaders in financial risk management (i.e., market and credit risks).

Although these notable operational risk events have a low probability of occurrence, their consequences were tremendous. Failures to learn from past mistakes will only increase the likelihood of reoccurrence. For a more recent example of operational risk, consider the 2011 UBS rogue trader scandal. Kweku Abodoli, a UBS trader, slipped under the radar of management as he committed a series of unauthorized trades that ultimately cost the company approximately $2 billion in losses and damaged the company's reputation. This level of oversight was in blatant disregard of the standards prescribed in UBS's supervision policy, while the continuous failure to respond to policy violations encouraged increasingly outrageous non-compliance practices.

At that time, UBS's operational risk framework relied heavily on self-assessment by the front office—furthermore, the Operational Risk department did not conduct internal tests to validate these self-assessment results. The findings of a Transparency Report published by the UBS in 2010 argued that the blame should not be placed on "rampant" leadership that encouraged excessive risk taking—in fact, "top management was too complacent, wrongly believing that everything was under control."[3] Critics harshly condemn the bank for not setting in place a risk management system that would prevent single actors from wielding so much power: as Michael Schrage, a writer for the *Harvard Business Review,* says in disbelief, "We can decry the greed, the selfishness and poor character of dishonest individuals all we want, but even minimally competent systems successfully dissuade or detect single bad actors."[4]

Unfortunately, UBS is not the only company to lose huge sums of money because of one rogue trader. As the reader might recall from a case study in Chapter 1, in 2008 Société Générale was embroiled in one of the largest trading scandals to date when trader Jérôme Kerviel engaged in a series of reckless trades that cost the bank 4.9 billion Euros.

Quite apart from the impact on the bottom line, operational risk can make a company seem as though it is ill-equipped to prevent or deal with fraud, errors, or lack of controls. This in turn can result in enormous damage to a company's reputation. It is exceedingly difficult to quantify reputational loss, but such a blow is likely to impact customer relationships as well as current and future partnerships. Furthermore, damage to a company's reputation is also likely to negatively affect its dealings with the capital markets. For instance, debt may become more expensive to obtain, and the stock market may lower its valuation of a company's stock if it is not able to effectively manage its operational risk.

If operational risk management is not treated as a discrete area of risk, it tends to be implemented differently in various areas of the same company. This means risk assessments and quantification may be performed differently by each business unit, resulting in inconsistent treatment of similar risks. For example, some business units might report operational losses on a gross basis, while others might report net losses, and still others might subtract losses from revenues and not report them separately at all. This in turn may bias measurements of those units' performances, ultimately resulting in sub-optimal management decisions. The same is true in situations where responsibility for operational risk is not clear. For instance, one business unit might be held responsible for risk events that should have been addressed by another unit. As a result, the return on equity of the first business unit might be artificially pushed below hurdle rate, leading senior managers to decide not to expand that business. In this instance, inaccurate performance

measures would have obscured the business' true value, resulting in the loss of a growth opportunity.

Effective operational risk management has the potential to deliver three clear benefits:

1. Rigorous operational risk management should both minimize day-to-day losses and reduce the potential for occurrences of more costly incidents.
2. Effective operational risk management improves a company's ability to achieve its business objectives. As such, management can focus its efforts on revenue-generating activities, as opposed to managing one crisis after another.
3. Finally, accounting for operational risk strengthens the overall enterprise risk management system. A company with a good understanding of its operational risks will have a more complete picture of the risks and potential rewards run by its various businesses. This paves the way for sophisticated enterprise risk models that incorporate the correlations between the various components of risk: credit, market, and operational.

Although operational risk management may be new relative to other risk management disciplines, one can safely make three comments about its development thus far. First, it has already been widely accepted that all companies face operational risks and should develop systematic programs to measure and manage them. Second, given the complexity of operational risks, a comprehensive approach should be used. As we will see later in this chapter, such an approach will ideally incorporate both process-oriented methods such as total quality management and statistical methods such as economic capital and extreme value theory. Lastly, the focus of operational risk programs should be on management, not measurement, which includes the integration of operational risk with market and credit risks.

A company cannot claim that it has an enterprise risk management program without fully addressing the issue of operational risk. Throughout the rest of this chapter we will discuss the definition and scope for operational risk, tools that can help measure and manage it, an operational risk management framework, and the range of industry practices.

OPERATIONAL RISK—DEFINITION AND SCOPE

A common business adage is that you cannot manage what you cannot measure. In the case of operational risk, there is another step: you cannot measure what you cannot define. Unlike market and credit risks, the definition of operational risk represents a challenge for most companies.

In the early stages, operational risk was defined in negative terms, as the collection of risks that are *not* credit or market risks. Over time, industry sources converged to a more common definition:

"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events."[5]

While this definition presents a common ground, there is still considerable debate as to how it should be applied. For example, many organizations differ on whether business risk (e.g., margins, competition) and reputational risk (e.g., tarnished brand, loss of market confidence) should be included in the definition of operational risk. While both of these risks were explicitly excluded in Basel II, both risks are important risk management issues and key drivers of expected loss—the Basel III framework focuses on these areas by "enhancing the infrastructure for reporting key information," and "[improving] risk data aggregation," among other new efforts.[6]

Individual companies should establish an overall definition of operational risk, as well as its subcomponents. In this chapter, we will apply the above definition that includes process risk, people risk, system risk, and event risk. Additionally, we will add business risk. We'll define each of these in turn.

Process Risk

Operational risk occurs through ineffective and/or inefficient processes. Ineffective processes can be defined as those that fail to achieve their objectives, while inefficient processes are those that achieve their objectives but consume excessive costs. At times, there is a natural conflict between the two. For example, reengineering and cost-saving efforts focused on improving efficiency may inadvertently end up reducing the effectiveness of control processes because certain checks and balances (which tend to be redundancies) are eliminated. A balance must therefore be achieved between effective and efficient processes.

A common process risk for any business relates to the processing of transactions. This includes the potential for errors in any stage of a business transaction, including sales, pricing, documentation, confirmation, and fulfillment. In any stage of transaction processing, a company is faced with risks that can cause a financial, customer, and reputational loss. For example, a pricing error can result in lower profitability, while a fulfillment problem can cause a customer to stop doing business with the company. Furthermore, companies need to make sure that operations remain within the limits of legal and regulatory provisions. With the adoption of new regulations (e.g., Dodd-Frank Act, Sarbanes-Oxley Act, U.S.A. Patriot Act), the consequences of violations increase for corporate executives from both professional and financial perspectives. Compliance is also an important issue

with respect to a company's internal policies and procedures. For example, in managing a fund, an investment company must be in compliance with both its internal investment policies and any agreed-upon client provisions.

Another significant element of operational risk can result from documentation processes. Improper or insufficient documentation may result in miscommunications between the parties to a contract, creating additional, unnecessary risks if there is a dispute. Consider the example of master agreements for financial products transactions. Nowadays, master agreements play a major role in trading: they provide a uniform way of minimizing credit and legal risks across different financial products between two or more counterparties. They also provide the benefit of netting, which reduces the total credit exposures between frequent counterparties.

Many global derivatives dealers, however, struggle with master agreements. In 1998, the U.S. Federal Reserve reported 20 to 30 percent of banks had incomplete International Swaps and Derivatives Association (ISDA) master confirmations documentation regarding settlement procedures and counterparty risk management.[7] Larger dealers can be managing hundreds of active master agreement negotiations at any given time, and some have thousands of master agreements in place, many of which also undergo amendments over time to accommodate new products, industry developments, or mergers. They often experience delay, disorganization, and miscommunication in the course of executing these essential contracts, putting significant revenues in jeopardy.

One potential answer, favored by some regulators, is to automate the process. Charles Fishkin, a risk consultant, has brought this idea one step forward, saying that all master agreement activities should be managed in *one* system—from initial discussion, to execution, to amendments for both new and existing customers.[8] With each of these phases executed and recorded in a controlled electronic environment, all of the participants (traders, marketers, credit officers, lawyers, and documentation professionals or operations staff) can check their status at any time significantly more easily than before. Comprehensive reports can also be easily produced and sorted by categories (business unit, product type, geography, etc.). Information flow has become more consistent and transparent, which has helped to minimize issues like incomplete documentation realized at the time of need, or transactions booked under the wrong master agreements. As a result, decisions can be made faster and operating risk (and credit risk in this case) can be reduced.

Knight Capital On August 1, 2012, Knight Capital implemented new software that, within mere minutes of its debut, flooded the New York Stock Exchange with huge amounts of false trades in the form of unintended buy orders. The small glitch that had gone undetected during algorithm testing

led to an immediate, enormous pre-tax loss of $440 million, along with a subsequent drop in shares from $10.30 to $2.50 in the following days. The losses suffered by Knight Capital have refocused attention on the risks involved in automated trading.

Critics are scratching their heads, baffled at the nature of Knight Capital's unbelievable failure: Ian Green, of Credit Suisse, wonders how the program could have run uninterrupted for 30 minutes without being detected by a person or another computer program. "It is possible to create a risk firewall around algorithms that monitors their known behavior and risk parameters. If they operate outside these parameters, possibly due to a logic error, an infinite loop or a 'fat finger', then their trades can be blocked from going to the market," says John Bates, chief technology officer at Progress Software.[9]

The reactions of other banks to this incident have been mixed. Most are taking a defensive stance, and are fighting against efforts to tighten algorithm security measures, because they do not think that the mistakes of one firm should translate to further restrictions across the industry. This seems to be the common sentiment regarding the proposed introduction of further circuit breakers, which are "automated switches that halt trading if prices move by more than set percentages in a specified period."[10] This demonstrates that while firms within the financial sector are aware of the importance of heavy technological defenses for risk management, many are still unwilling to sacrifice the potential profits that could be lost as a result of restricting human or automated trader movement.

People Risk

People risks typically result from staff constraints, incompetence, dishonesty, or a corporate culture that does not cultivate risk awareness. Staff constraints occur when companies cannot fill critical open positions because of labor shortages, or because compensation and other incentives are not attractive to new candidates. Incompetence becomes an issue when employees lack the necessary level of skills and knowledge to do their jobs correctly. Lack of professional training and development would further compound human errors. Dishonesty within a company can lead to fraudulent activities such as employee thefts; interestingly, a National Retail Federation study showed that retail inventory managers attribute 25.8 percent of inventory losses to shoplifters and 44.2 percent to employee theft.[11] Corporate cultures that do not actively incorporate risk awareness, or encourage profit without regard to the methods used to make them, can also result in adverse employee behavior.

Every employee in an organization must be considered a risk, which is why background checks are essential in mitigating this risk. An alleged scandal at Disney World, whose business stands or falls on its reputation

for safe, innocent fun, graphically demonstrated the danger of overlooking employee-related risks. In July 1998, a 17-year-old cook at Disney World was accused of raping a 16-year-old tourist in the bathroom of a hotel. Were this not appalling enough, it was compounded further by the revelation that the cook had been hired despite having an extensive juvenile arrest record, including charges of aggravated assault, burglary, theft, and grand theft auto. At the time of his employment at Disney, he was on probation for a break-in in which he had been accused of putting a gun to a victim's head.

How could such an individual have come to be hired in the first place? Simply because Disney did not carry out background checks on all of its employees at that time. Such checks were only seen as necessary for certain jobs, such as security guards, child-care workers, and jobs that would require handling cash transactions. Nor was Disney's response a model of clarity: it initially said that it would not change its policy on background checks, but later recanted, saying it would perform such checks on new employees only. Furthermore, the company said it had no written guidelines, but would assess hiring on a case-by-case basis. By contrast, Universal Studios Escape, one of Disney's major competitors, was already running criminal background checks on all new employees.

System Risk

As technology has become increasingly necessary in more and more areas of business, operational risk events due to systems failures have correspondingly become increasingly significant. Companies today often use systems that are both integrated across the firm and specifically tailored to their particular business needs. If the development of a company's technological infrastructure does not keep pace with the development of its business, however, there is the potential for new risks. System risks include systems availability, data integrity, systems capacity, unauthorized access and use, and business recovery from various contingencies.

Another example of system risk is the risk of loss from faulty financial models. The institution may use inappropriate methodologies, assumptions, or parameters in evaluating a business or investment opportunity, and thus underestimate the risks it is taking on. Exposures to model risk can range from strategic decisions based on economic value added (EVA)-based models that understate the costs of risk, to investment decisions based on inadequate assumptions of how a complex derivative should be priced. The financial press is filled with stories of corporate losses due to inaccurate financial models.

In addition, the risks associated with programming errors and lack of planning can be significant. A small error in one algorithm can easily propagate through several models and across networks, causing great damage before the

error is detected. The immense expense associated with remedies for the Y2K bug is a good example of how costly small oversights can quickly become. Finally, systems failures constitute a large risk for businesses, as a breakdown of the system may force revenue-generating activities to stop.

Security is rapidly emerging as another key technology risk, particularly given the rise of e-commerce. In early 2000, a Web hacker successfully obtained a collection of more than 300,000 customer credit card files from the Internet music retailer CD Universe. This was possible because CD Universe had stored unencrypted credit card data on the web-server itself, a fundamental design flaw that allowed the hacker to download the personal information using weaknesses in the card-processing software.

Events such as this can and do occur with alarming frequency, which serves as a stark reminder that all organizations that conduct business in today's highly networked environment should specify data security as a primary goal in designing business processes and systems. Although sufficiently motivated and resourceful hackers will probably be able to compromise almost any computer software, there are several basic guidelines that can be taken to avoid becoming easy prey.

Event Risk

Event risk is the risk of loss due to single events that are unlikely, but may have serious consequences if they do occur—for example, internal or external fraud, system failures, market dislocations, and natural or manmade disasters. Incidents of event risk are often random and therefore difficult to predict, though they can be controlled through effective planning and management. While such events are unlikely, a business must expect the unexpected. It is also important to note that major events often result in implications for all types of risk—market, credit, liquidity, and operational. Moreover, unlikely events occur in much greater frequency than one might expect; Leslie Rahl noted that there has been at least one major market move exceeding 10 standard deviations every year for the past 10 years.[12] These market moves included the Brazil Crisis (1999), the Russian Crisis (1998), and the Asian Crisis (1997). The corporate frauds associated with the likes of Enron, Worldcom, Adelphia, and others will only add to a growing list of unthinkable operational risk events.

One of the most unthinkable recent events is the September 11, 2001, terrorist attack, during which thousands of lives were lost and insurable losses exceeded $40 billion (based on estimates from the Insurance Information Institute). Other notable loss events include Bank of Credit and Commerce ($17 billion), Long Term Capital Management ($4 billion), Texaco ($3 billion), and Sumitomo Corporation ($2.9 billion). Julian Fry, UBS's head of operational

control, notes that "the 1980s had seen only three loss events over $1 billion; 104 had occurred in the 2000s, and 54 already this decade."[13]

Business Risk

Business risk is the risk of loss that corresponds to unexpected changes in the competitive environment, or to trends that damage the franchise and/or operating economics of a business. It includes front-office issues such as strategy, client management, product development, pricing, and sales, and is essentially the risk that revenues will not cover costs within a given period of time. Given the importance of a company's reputation and brand, reputational risk should be incorporated into business risk, or treated as a separate category. Business risk is heavily influenced by external factors, is primarily determined by environmental, competitive, and evolutionary factors, and can be mitigated through effective management.

The most classic business risk example discussed in nearly every business school is the failure of railroad companies to redefine their businesses from railroad to transportation, resulting in the collapse of most of these companies. On the other hand, a recent success story in managing business risk is the transformation of IBM from a hardware company to a service and solution company. One of the key lessons learned from the Internet bubble is that every business must be based on a sound business strategy that will produce long-term growth and profitability. Achieving this objective is, of course, basic business management. The contribution of business risk management is to address key questions such as:

- What are the key vulnerabilities in our business strategy and plan?
- Do we have sufficient business and product diversification?
- Do we have the appropriate operating leverage (fixed vs. variable costs)?
- What if our business assumptions are wrong?
- When should we fix or exit a business? Do we have an exit strategy?

THE OPERATIONAL RISK MANAGEMENT PROCESS

Given the scope and importance of operational risk, management should establish a systematic process with respect to risk identification, measurement, and management. The operational risk management process involves the following steps:

1. Risk policy and organization
2. Risk identification and assessment

3. Capital allocation and performance measurement
4. Risk mitigation and control
5. Risk transfer and finance

Let's discuss each of these steps in turn.

Risk Policy and Organization

As a first step, a company should establish an operational risk management policy that defines what it wants to accomplish, including how it is organized to achieve its stated objectives. An operational risk management policy should include the following:

- *Management principles for operational risk:* What are the company's philosophy and principles on operational risk? For example, as with credit risk and market risk, one common principle may be transparency. With respect to operational risk, it is critical that bad news travel up the organization so that emerging problems are addressed before they become full-blown crises.
- *Definition and taxonomy for operational risk:* As discussed above, how is operational risk defined in the company, what is included and excluded, and what are the sub-categories? A common language must be built around the discussion of operational risk within the company.
- *Objectives and goals:* Management should establish the over-arching objectives (e.g., improved effectiveness and efficiency of core business processes) and specific goals that the company wants to achieve (e.g., a 20 percent reduction in operational losses, a 30 percent improvement in timeliness with regards to resolving outstanding audit issues).
- *Operational risk processes and tools:* This part of the policy lays out the corporate-wide processes and tools that business units are expected to adopt, such as risk assessment, measurement, reporting, and management processes. In this manner, a consistent approach to operational risk is used based on common applications and standards for these processes and tools.
- *Organizational structure:* The policy should also document the organizational structure for operational risk management. What are the key committees, memberships, and charters? What are the reporting lines between the board, senior management, line management, and the risk management and oversight groups?
- *Roles and responsibilities:* Given the complexities of operational risk, it is critical to clearly define the specific roles and responsibilities for every key aspect of operational risk management. At the highest level, the board

is responsible for establishing policies and ensuring that the appropriate resources and controls are in place. At the lowest level, every employee is responsible for being knowledgeable about the operational risks that they are involved in and for escalating problems and issues. Additionally, the roles and responsibilities of various risk management and oversight functions should be established (as further discussed below).

At most companies, there are a number of risk management, control, and oversight groups that have some connection to operational risk management. It is critical that specific roles and responsibilities are defined for these functions:

- *Operational risk management* to ensure an overall framework is established to measure and manage operational risks
- *Strategic planning* to ensure that business risks are addressed in business plans and reviews, as well as in new acquisition strategies and product plans
- *Finance/accounting* to ensure timeliness, accuracy, and quality of books and records, as well as business projections and profitability models
- *Audit* to ensure business-unit compliance with corporate policies and procedures
- *Legal/compliance* to ensure business activities are in compliance with applicable laws and regulations
- *Information Technology (IT)* to ensure critical systems and databases are backed up, business recovery plans are established and tested, and information security safeguards are in place
- *Corporate security* to ensure that corporate assets are maintained and protected

There are other important operational risk management functions, such as insurance, legal and compliance, quality management (or six sigma), human resources, and so on. One of the key issues is whether a function is primarily established as a consultant or checker or both. For example, at many companies, the operational risk management group acts mainly as a consultant for senior management and the business units, while the audit group acts as a checker, and the legal group acts as both. Other companies struggle with trying to set up their audit groups as both a consultant and checker, because the former role can easily hinder the independence of the latter role.

Risk Identification and Assessment

Given the wide scope of operational risk, a company should employ a range of qualitative and quantitative tools to assess, measure, and manage

operational risks. Below is a summary of the main operational risk management tools that companies use today:

- *Loss-incident database:* A company should capture operational risk losses and incidents for two main reasons. First, losses are easily measurable and can be used to show trends and ratios (e.g., loss/revenue ratio), whereas incidents can capture other events that should be noted. Second, every loss and incident within a company represents a learning opportunity, without which past mistakes are more likely to be repeated. As such, the loss-incident database should be used to support root-cause analysis and risk mitigation strategies, as well as to facilitate the sharing of lessons learned within the company. Additionally, there are a handful of industry initiatives to develop more robust loss-event databases, though it is too early to tell which one(s) will become the industry standard(s). It is unlikely, however, that the management of operational risk will ever become a wholly data-driven process; given the nature of operational risk, it will always be more an issue of management rather than measurement.
- *Control self-assessment:* A control self-assessment (also known as risk assessment and risk control self-assessment) is mainly an internal analysis of key risks, controls, and management implications. It is important for each of the business units to assess their current situation with respect to these operational risk elements. By doing this, each business unit will develop a clearer picture of where to start and how to proceed in the operational risk management process. Each business unit will also have a greater sense of ownership through the self-assessment process. Tools that support self-assessments include questionnaires, issue-specific interviews, team meetings, and facilitated workshops. The output is an inventory of key risk exposures, key control initiatives, and sometimes even a Letterman-style Top 10 Risks.
- *Risk mapping:* Building on the work from control self assessments, the company's key risk exposures can be ranked with respect to their probability and severity so that management can have a comparative view in the form of a two-dimensional risk map. For operations that are more complex (e.g., cash management, special purpose vehicles), risk-based process maps can be produced to show how various risk exposures can arise. These maps will aid in the identification of the risks encountered in each business unit, indicating problem spots, such as single points of failures, or where errors often occur. These maps will also enable each business unit to develop and prioritize its risk management initiatives to address the most important risks.
- *Risk indicators and performance triggers:* Risk indicators are quantitative measures that represent operational risk performance for a specific

process. Examples include customer complaints for a sales or service unit, trading errors for a trading function, un-reconciled items for an accounting function, or system downtime for an IT function. These risk indicators are usually developed by the individual business units and closely tied to their business objectives. Early-warning indicators should also be developed to provide management with leading signals (e.g., employee absenteeism and turnover as an early warning indicator of future operational errors). To track the performance of processes against an expected range, trigger levels can be established in terms of goals (where you want to be) and levels of minimum acceptable performance (MAP). If a key risk indicator falls below the MAP, then that would trigger an escalation report to senior management, and also initiate a corrective action plan. On the other hand, if a risk indicator is above goal consistently, then management should consider raising both the goal and MAP to facilitate continuous improvement.

Other sources of valuable information for risk identification and assessment include internal audit reports, external assessments (external auditors, regulators), employee exit interviews, customer surveys, and complaints.

Capital Allocation and Performance Measurement

Beyond risk identification and assessment, it is important to link risk to performance measurement through the capital-allocation process. Unlike market risk and credit risk where risk measurement methodologies have been developed and tested for many years, there are not widely accepted models for operational risk. In selecting a methodology (or combination of methodologies), each company should first establish its objectives and resources and choose accordingly. Different methodologies imply different interpretations of operational risk, and require various inputs to be useful. Given that there is likely to be no single solution, a combination of methodologies will allow the disadvantages of one model to be balanced by the strengths of another, allowing a more robust overall measurement to be developed. Some of the most common methodologies, including their strengths and weaknesses, are discussed here:

- *Top-down models:* The top-down approach to operational risk modeling calculates the implied operational risk of a business by using data that is usually readily available, such as the overall financial performance of the company or that of the industry in which it operates. Top-down models use relatively simple calculations and analyses to arrive at a general picture of the operational risks encountered by a company.

These top-down models benefit from the sophisticated methodologies already developed for credit and market risk. Examples of top-down models on operational risk include the implied-capital model, the income-volatility model, the economic-pricing model, and the analog model:

- *Implied-capital model: This* methodology assumes that the domain of operational risk is that which lies outside of credit and market risk. Thus, the capital allocated to operational risk must be the result of subtracting the capital attributable to credit and market risk from the total allocation of capital. Although this model provides an easily calculated number for operational risk, its simplicity presents three major disadvantages. First, total risk capital must be estimated given the company's actual capital and the relationship between its actual debt rating and target debt rating. Second, it ignores the interrelationships between operational risk capital and market risk and credit risk capital. Finally, this model does not capture cause-and-effect scenarios for operational risk; it is accounted for only implicitly.
- *Income-volatility model:* This model is similar to the capital-allocation model, but it goes one step further by looking at the primary determinant of capital allocation—income volatility. The volatility attributable to operational risk is calculated in the same way as in the capital allocation model—by subtracting the credit and market risk components from the total income volatility. One of the advantages of this model is that of data availability: historical credit and market risk data are usually easily obtained, and total income volatility can be observed. However, this model also has several shortcomings, the most dramatic of which is that it ignores the rapid evolution of firms and industries. Structural changes, such as new technologies or new regulations, are not captured in this model. The income-volatility model also fails to capture softer measures such as opportunity costs or reputation damage. In addition, this model fails to capture the low-probability, high-consequence risks, as is true in all of the top-down approaches.
- *Economic pricing model:* The capital-asset pricing model (CAPM) is probably the most widely used economic model, and can be employed to determine a distribution of the pricing of operational risk relative to the other determinants of capital. The CAPM assumes that all market information is captured in the share price, thus allowing the effect of publicized operational losses to be determined by evaluating the market capitalization of a company. The advantage of this approach is that it incorporates both discrete risks and softer issues such as reputational damage and the effects of foregone opportunities. With this approach, a company's stock price volatility (due to operational risk)

is derived by taking the company's total stock price volatility and subtracting from it the stock price volatility (due to credit risk and market risk). However, the CAPM approach presents an incomplete and simplistic view of operational risk. It provides only an aggregate view of capital adequacy, without information about specific operational risks. Furthermore, the level of operational risk exposure is not affected by particular controls and business risk characteristics, so there is no motivation to improve operations, and while tail-end risks *are* incorporated in the model, they are not thoroughly accounted for. This is a significant omission. Such incidents can do more than just diminish the value of a business; they can lead to the end of the business completely. Finally, this model does not help in anticipating, and therefore avoiding, incidents of operational risk.

- *Analog model:* The analog model is based on the assumption that one can look at external institutions with similar business structures and operations to derive operational risk measures for one's own organization. This model can be extended to look for the causes and effects of operational losses at such institutions. This method offers one way to proceed when a company does not have a robust database of operational risk losses. However, it takes some level of credulity to assume that the high-level numbers of another institution can accurately measure one's own operational risk, and as such, many are suspicious of this approach. In the words of one analyst: ". . . [The] intangibles within an institution—its risk-taking appetite, the character of its senior executives, the bonus structure of its traders—put so many wild cards into the operational risk equation that similarities in business volume, transaction volume, documented risk policies and other qualities that can be scored are swamped."
- *Bottom-up (Loss Distribution) Model:* The bottom-up methodology applies loss and/or causal factors to derive predicted loss expectancies. This approach requires a company to clearly define the different categories of operational risk it faces, gather detailed data on each of these risk categories, and then quantify the risk of loss. A company often needs to augment its internal data with an external loss-event database. The final output of this bottom-up approach is a loss-distribution model that can estimate operational risk capital for a given confidence level (e.g., target debt rating). According to a November 1999 study conducted by the British Bankers Association, the International Swaps and Derivatives Association, and Robert Morris Associates, there is an increasing preference for risk-based bottom-up methodologies over the top-down approaches.

  The data needed for this methodology can also be used to derive a business' risk profile. For example, turnover or error rates can be

tracked *over time, and combined with changes* in business activities to construct a more robust picture of the business' operational risk profile. By tracking the risk factors over time, the company can assess its operational risk exposure on an ongoing basis and can upgrade controls in appropriate areas as needed. Furthermore, continuous tracking provides a company's management with better information about its operations and increases awareness of the causes of operational risk.

However, bottom-up models do present several difficulties. Mapping loss data from the company with loss data from other companies is complex, due to the differences in business mix, size, scope, and operating environment. Translating each cause of risk into a numerical value is often challenging, because losses are frequently reported as aggregates of multiple risk sources that are difficult to isolate. For example, an operational loss on a trading floor might result from personnel risk, lack of controls, expanding overseas business, lack of back- and front-office segregation, volatile markets, senior management confusion, and incompetence. In addition, robust internal historical data may not be available, and this model is inherently flawed with respect to low-probability, high-consequence events since it depends on a large database of values for its predictions. Bottom-up models are usually based on statistical analysis and scenario analysis.

Statistical Analysis Traditional parametric statistical and econometric models strive to produce a good fit in regions where most of the data fall, potentially at the expense of good fit in the tails where few observations fall. A model of operational risk, however, must account well for the outer tail of the loss distribution in order to capture low-frequency, high-severity losses. Extreme value theory (EVT), which focuses on the extreme event data, rather than all the data, may be more appropriate in this context. EVT offers hope that reliable estimates of extreme probabilities may be achievable. A generalized extreme value estimation, for example, uses the largest loss observed in each of the preceding 12 months to obtain the distribution parameters best fitted by these 12 values. The results can be updated daily, weekly, or monthly on a rolling 12-month basis.[14]

Statistical analysis requires an ample supply of operational loss data that is relevant to the business unit. The lack of appropriate internal data is therefore the greatest obstacle to the widespread application of this methodology; the use of external data as a proxy poses several problems, as mentioned earlier. However, the analytical power of this tool will hopefully become more widely applicable in the near future as increased awareness of operational risk leads to improvements in data collection.

Scenario Analyses Scenario analysis is perhaps more subjective than the other methodologies mentioned here, but it offers several benefits that are not addressed by the more quantitative models. A scenario analysis is used to capture diverse opinions, concerns, and experience/expertise of key managers and represents them in a business model. Scenario analysis is a useful tool in capturing both the qualitative and quantitative dimensions of operational risk. Risk maps allow the representation of a wide variety of loss situations, and also incorporate the details of the loss scenarios envisioned by the managers surveyed. Risk maps of each business unit identify where operational risk exposures exist, the severity of the associated risks, whether any controls are in place, and the type of control: damage, preventive, or detective. Cause-and-effect relationships can be captured with this methodology. The shortcoming of such a model, however, is in its subjectivity, which creates a potential for recording data inconsistently and/or for biasing conclusions if one is not careful.

According to Stamford Risk Analytics, the 2008 global financial crisis "revealed the need for a paradigm shift in risk management practices."[15] They point out that the majority of current quantitative models are incapable of accurately portraying risk, because they are blind to the risk contribution of *black swans*—defined as "hard-to-predict, high-impact events."[16] Furthermore, risk models tend to rely heavily on historical data, which do not incorporate live changes to a firm's risk profile.

Additionally, Stamford Risk Analytics believes that these models are inherently biased because they create "risk-reward arbitrage opportunities," which allow "unethical managers to deliberately engage in high-risk activities while appearing to operate within stakeholder risk tolerances."[17] This is particularly dangerous, because it may encourage similarly negligent behavior at other firms, which are eager to remain competitive.

Despite the shortcomings discussed for the above models, the application of several divergent models can in fact help management develop a more confident, convergent view of how much operational risk capital is needed. Once an operational risk capital estimate is established, it can be integrated into the overall risk-return analytics of the company (as discussed in Chapter 10).

Risk Mitigation and Control

Assessing and measuring operational risk is important, but pointless unless directed toward the improved management of operational risk by improving and controlling key risk factors. Simply stated, the goal of operational risk management is to help management achieve its business objectives. Once a measurement framework is in place, the next step is to implement a process

that identifies actions that will reduce operational losses. These actions include adding human resources, increasing training and development, improving and/or automating processes, changing organizational structure and incentives, adding internal controls (e.g., more frequent or more extensive monitoring), and upgrading systems capabilities. The key to effective operational risk mitigation is to establish a cross-functional rapid-response team that will address and resolve any emerging operational risk issues. At one business unit at Fidelity Investments, these teams were called turbo teams, and would respond when operational risk indicators fell below MAP—they would report back to management on their assessments and actions within a few days or weeks. Finally, a mechanism for evaluating and prioritizing potential improvements must be created. Cost/benefit analysis and readiness assessments are useful tools that should be included in the evaluation process.

Some of the operational risk measurement approaches discussed above should naturally lead to improved operational risk management at the business-unit level. A business unit can monitor and improve its operational risk levels by setting operational goals, exposure limits, and MAPs on the basis of data collection and analysis. For example, an operational goal might be a stretch target, which a business hopes to attain over some period of time through the use of new procedures. A MAP level might be the maximum error rate permissible in a business process; if exceeded, the process would have to be re-evaluated. The allocation of economic capital for operational risk, if it successfully captures both performance and behavior effects, should motivate business units to improve their operational risk management in order to reduce their capital charges. For example, a business may set up procedures through which employees may respond immediately to operational problems and implement the controls necessary to monitor and improve operational risk performance. A key requirement for risk mitigation is to understand the root causes of operational risks, such as lack of training or inadequate systems, and then focus corrective actions on these root causes.

Besides risk mitigation through operational processes and controls, there are other financial solutions that management may consider. Companies can establish reserves to cover their expected operational losses as a form of self-insurance. Expected losses should also be embedded in the pricing of a product. Market and credit risks are already incorporated into some transaction prices as a matter of practice—including an adjustment for operational risk makes for a more comprehensive picture and allows for more accurate risk-adjusted pricing. For example, if a business unit performs 10,000 transactions annually, with an expected loss of $80,000 a year, then a risk adjustment of $8 per transaction could cover such losses. Additionally, the cost of capital for operational risk (and other risks) should be incorporated into the pricing of

a transaction. Beyond the cost of risk, pricing can also be driven by the target levels of returns that the company expects a product to achieve.

Risk Transfer and Finance

For critical operational risk exposure, a company must decide if the best strategy is to implement internal controls and/or executive risk transfer strategies. The two are not mutually exclusive and are often complementary. For example, most companies implement workplace safety procedures and purchase worker's compensation insurance—in fact, the former can reduce the cost of the latter. Another example is product liability, since a company can strengthen product-development controls in addition to obtaining product-liability insurance. Some risk transfer strategies are meant to be backstops to internal controls (e.g., directors and officers liability insurance provides protection against wrongful acts). More recently, companies are evaluating insurance policies for "cyber security" in the event established risk controls fail. In the past, insurance managers would purchase such insurance policies based on the structure, cost, and provider rating and service level. In the context of enterprise risk management (ERM) and operational risk management, a company should:

- Identify their operational risk exposures and quantify their probabilities, severities, and economic capital requirements;
- Integrate their operational risk with their credit and market risks in order to assess their enterprise-wide risk/return profile;
- Establish operational risk limits (e.g., MAPs, economic capital concentration);
- Implement internal controls and develop risk transfer and financing strategies; and
- Evaluate alternative providers and structures based on cost-benefit economics (i.e., comparing the cost of risk retention versus risk transfer).

There is an important difference between risk transfer and risk finance. Risk transfer is when a third-party insurance provider assumes the loss between the deductible and cap, whereas in risk finance the insurance company provides funding but is reimbursed over time. The Economic Capital and RAROC framework discussed in Chapter 10 is also a useful tool for evaluating the impact of different risk transfer strategies. For example, in executing any risk transfer strategy, the economic benefits include the lower expected losses and reduced loss volatility, while the economic costs include insurance premium, as well as higher counterparty credit exposures. In a sense, the company is both ceding risk and ceding return, resulting in a

ceded RAROC. By comparing the ceded RAROCs of various risk transfer strategies, a company can compare different structures, prices, and counterparties on an apples-to-apples basis, and select the most optimal transaction(s). Moreover, a risk transfer strategy with a ceded RAROC below the firm's cost of equity would add to shareholder value, and vice versa.

BEST PRACTICE IN OPERATIONAL RISK MANAGEMENT

It is ironic that operational risk is often the least-developed component of ERM, despite the fact that it was the first and, arguably, the oldest risk that companies face. Today, operational risk is widely recognized as one of the most critical risks that companies must control, but also an area where significant opportunities exist. There is also a wide range of industry practices in operational risk management, as discussed below in terms of basic practice, standard practice, and best practice.

Basic Practice

At the basic-practice level, a company has recognized operational risk as a distinct risk management discipline. A definition of operational risk, and its sub-categories, is in place. An operational risk manager, who reports to the chief risk officer (CRO), is appointed to develop the overall operational risk management program. An operational risk committee is organized with representatives from the line and oversight units. This committee meets monthly to share and discuss operating risk information and coordinate risk assessment and management activities.

With respect to risk assessment and measurement, the company has initiated the tracking of operational risk losses and has also begun reporting on risk indicators. Moreover, control self-assessments by business and operational units are performed on an annual basis. An operational risk policy has been developed and approved by the board of directors. The operational risk management group acts as a consultant to senior management and business units, and also provides support on crisis-management situations. The audit and compliance groups act as checkers with respect to the operational risk policy.

Standard Practice

Building on the basic practices described above, the standard-practice companies have developed a full set of operational risk indicators by business unit. They have also established goals and MAPs for these indicators, and created monthly reporting and ongoing monitoring processes. These

reporting and monitoring processes allow the board and management to understand their key risk exposures and trends. Additionally, standard-practice companies have initiated the development of early-warning indicators for their key operational risk exposures. To better understand their operational risk, risk-based process maps are developed to identify key areas of exposure within their business operations. Standard-practice companies have developed several years of operational risk losses and incidents, and also have linked their internal database with an industry loss-event database.

With respect to risk mitigation and control, standard-practice companies have developed response plans and contingency plans to mitigate operational risks when they arise. A team of operational risk professionals supports the operational risk manager. Their roles and responsibilities are well defined relative to the other oversight and control functions. To minimize gaps and redundancies, as well as maximize their effectiveness, they are integrated as part of the same organization. However, while audit is an active participant in operational risk management, they maintain their independence from the operational risk unit. To ensure organizational learning, the operational risk unit provides training programs, on-line risk policies, and post-mortems of past losses and incidents.

Best Practice

While operational risk management is still evolving rapidly, it is useful here to describe the more advanced applications that some of the leading companies have adopted. Best-practice companies integrate qualitative and quantitative tools to support their assessment and measurement of operational risks. They have also developed a full set of early-warning indicators, which not only provide leading signals on internal operational processes, but also the external business environment that the company operates in. Examples of external indicators include measures that track public opinion, political uncertainties, regulatory changes, and technology trends. Best-practice companies allocate economic capital to underlying operational risks, along with credit risk and market risk, in order to enable risk-adjusted performance measurement, which in turn provides corporate incentives for business units to improve their operational risk management. Additionally, they have initiated the development of scenario- or simulation-based operational risk modeling to quantify potential loss as well as evaluate various risk mitigation strategies.

The insurance function is fully integrated with the operational risk function. Based on the economic capital framework, risk transfer strategies are executed if the cost of risk transfer is lower than the cost of risk retention, unless the company deems a risk as undesirable to hold. To better manage operational risk, best-practice companies integrate operational risk controls

into their business management. This includes risk analysis in business plans and reviews, as well as in new products and acquisitions strategies. As such, the operational risk management function has evolved from strictly a control function to one that supports better business decisions on pricing, growth, and profitability strategies.

EMERGING IT RISKS

In the past several years, ERM and operational risk professionals have been challenged with a new and complex set of IT-related risks. We will review three of these emerging risks: cyber security, cloud computing, and social media.

Cyber Security

In March of 2013, James Clapper, Director of National Intelligence, announced that the greatest threat to national security today is no longer extremist terrorism, but cyber crime. This indicates a powerful shift in national paradigm, as the United States moves from the arena of physical threats to cyber attacks. Within the energy industry alone, cyber crime has cost the U.S. economy between $119 billion and $188 billion a year, with the numbers increasing steadily as the attacks intensify.

The U.S. government has categorized cyber criminals into the following tiers, ordered by increasing threat:

- Tiers 1 and 2: at these lowest-level tiers, attackers target "known vulnerabilities"
- Tiers 3 and 4: with higher levels of funding, these attackers can pinpoint "new vulnerabilities" to exploit
- Tiers 5 and 6: funding for these attackers can reach as high as the billions, allowing for the actual "[creation of] vulnerabilities"[18]

For the private-sector institution, this rising wave of cyber criminals and the increasing sophistication of their assaults signify the appearance of a new battleground in the form of cyber space, making the issue of cyber security an increasingly integral part of the ERM framework. Former National Security Advisor Tom Donilon voiced his serious concerns about the "targeted theft of confidential business information and proprietary technologies" that has occurred in the private sector, which serves as a compelling indication of how consequential the concept of corporate data security should be for firms, regardless of their corporate focus.[19]

There are other types of cyber attacks that do not aim to steal information—but this does not mean that they are any less dangerous. For example, a denial-of-service (DoS) attempts to overwhelm a network by flooding its web sites. This paralyzes it, denying users access to the Internet and other services, which can seriously cripple a firm's ability to perform essential day-to-day activities. In April of 2013, Charles Schwab was hit by a DoS, and as a result, the company's web site and mobile app were down, then malfunctioning for two days straight. Schwab spokesman Greg Gable said that "the denial-of-service had no impact on client data or accounts," but other firms who suffer DoS attacks may not be so lucky.[20]

Just as with other types of risk management, the aim of cyber security is not to eliminate the threat of a cyber attack, since these are external strikes that are beyond the firm's control. Instead, firms should concentrate on mitigating the damage done by minimizing the amount of data lost. A white paper recently published by Sidley Austin, LLP outlines some key measures that business leaders can take to protect themselves against the theft of intellectual property and other cyber resources. Interestingly, the best method of combating cyber threats is not to completely close oneself off—cyber security becomes more efficient if firms cooperate with each other.

Of course, anti-trust and competition issues make cross-firm collaboration in this manner difficult, with the result that firms have isolated themselves. Understandably, it is hard for private-sector firms to willingly reveal breaches in the hulls of their cyber security frameworks, but note that deliberate concealment of these weaknesses can ultimately backfire. Recognizing the need for a cohesive, guided effort to fight cyber crime, the government has been spearheading efforts to dam up the flood of lost data. However, without the cooperation of private-sector firms through transparent communication, these efforts have been largely frustrated. Tom Ridge, the first U.S. Homeland Security secretary, believes that the biggest barrier to stronger cyber security across the nation is the tense relationship between the public and private sectors, because "the infrastructure that the government relies upon is generally owned by the private sector."[21]

The government now requires firms involved in "critical infrastructure industries" (namely, finance, transportation, utilities, etc.) to accept the integration of government committees called "information sharing and analysis centers" (ISACs) into their corporate structures. This will increase the availability of cyber-security knowledge, which offers benefits to both the government and private-sector firms. Through the ISACs, the government can support and steer a nationwide defense against cyber crime, while private-sector firms can take advantage of the cyber-security resources of the government.[22]

Adapted from the recommendations given by the Department of Defense (DoD) with regard to tightening its own cyber-security measures,

here is a list that private firms can use to begin fortifying their cyber shields:[23]

- Protect Nuclear Strike, Ensure Availability of Conventional Capabilities: For the private firm, this translates into a need to continuously test and monitor existing IT systems against cyber attacks. The DoD recommends that nuclear systems should be isolated during testing, and re-designed if necessary: private firms can follow this method of quarantine to improve their ability to contain cyber attacks. It would also be prudent for the firm to review its corporate and legal environments in order to determine the areas most likely to be subject to cyber attacks.
- Refocus Intelligence: Here, the DoD recommends a paradigm shift within the department to shift its focus to cyber security as of paramount importance. This applies for private firms as well; cyber security should become a top priority risk with respect to risk policy and risk appetite statements, early warning indicators, and risk monitoring and reporting processes.
- Enhance Cyber Defenses: The DoD urges the development of automated cyber defense, which would eliminate the cost of and time needed to manually pinpoint sites of cyber attack—this is also crucial for private firms. Since the government is offering its support, private firms should capitalize on the government's sophisticated cyber-security resources.
- Change DoD Cyber Culture: For private firms, this means implementing training programs that ratify the firm's cyber security strategy and teach employees not only how to recognize a cyber attack, but also how to react to one. These training programs may also help to protect the firm from internal cyber attacks in the form of insider leaks.
- Incorporation of Cyber Requirements into System Lifecycle: Private firms should consider tailoring their existing cyber security frameworks so that they can be applied to all aspects of the firm, thus ensuring that the company is protected at all times. These frameworks should also be adaptable, to adjust to different forms of cyber attack.

Above all, it is important to realize that the constantly occurring advances in technology make cyber crime a dynamic and fluid challenge that is perpetually evolving. For example, computer networks are no longer the only sites of vulnerability—cyber criminals are now switching their targets to software and hardware that have yet to be integrated into the technological framework of private-sector firms, which expands the threat to the manufacturing process as well. Hence, it is essential for a firm's risk management framework to be flexible and to be constantly adapted to meet the cyber crime threat.

Cloud Computing

Cloud computing, which derives its name from the popular use of a cloud to symbolize the complexity and comprehensiveness of a cloud system, allows firms to use external cyber resources (such as hardware, software, and data). Not only does cloud computing allow firms to significantly reduce overhead costs by reducing the capital needed to invest in physical and electronic storage, cloud computing can also help firms to update their own IT environment, and so improve the firm's overall flexibility and efficiency. A recent Rackspace study shows that cloud computing increased profits by an average of 22 percent and saved companies an average of $478,300 on IT expenditures.[24]

Firms can choose to implement cloud-computing services internally, access a cloud system through external service providers, or pursue any combination of the two:

- Vendor clouds are sold by external cloud service providers (CSPs) and allow the firm to access resources, shared with other customers, through the internet (or other form of network).
- Private clouds, which are modeled after vendor clouds, are managed exclusively by, and can only be accessed from within, the firm itself.
- Hybrid clouds combine vendor clouds and private clouds to provide a cloud structure that can be tailored to fit the firm's needs.
- Community clouds are used by firms—normally within the same industry—that share goals and interests and can be internally or externally managed.

Despite the many cost advantages of cloud computing, it does not eliminate the risks associated with these resources pre-cloud implementation, nor does it contribute significantly to a firm's efforts to tighten cyber security, as we previously discussed. In fact, cloud computing brings with it a new set of risks, stemming mainly from a dilution of management's control over the firm's data.

The use of vendor clouds makes firms particularly susceptible to increased risk, because they are now also exposed to the risks experienced by the CSP's other customers, as well as the CSP itself. Neither the CSP nor the other customers are likely to make efforts to align their own risk management frameworks with that of the firm or engage in transparent communication about internal processes. This causes complications in risk management because we must now consider potential divergences in interest. Ultimately, the firm virtually ties itself to these third parties, which can threaten the stability of the firm's IT environment.

Cloud computing can also make the firm a more attractive target for cyber criminals, because they only need to infiltrate one network in order to

gain access to all the cyber resources available on that particular cloud. As such, the risk of data leakage—whether externally through cyber criminals, or internally through an insider leak—increases significantly when a firm shifts considerable amounts of private data onto a cloud system.

However, applying risk management strategies to cloud computing can allow a firm to harness its true potential without sacrificing data control. These strategies are concepts that we have seen before: the definition of a risk appetite statement, a robust model for governance, strong, defined pathways of communication, and a thorough grasp of the firm's current IT environment.[25] Most importantly, the firm's risk management framework should be adjusted to also encompass the risk universes of the CSP and the CSP's other consumers in order to give the firm a more complete vision of its own new risk universe.[26]

Social Media

The rise of social media has changed the business world in profound ways by ushering in an unprecedented improvement in the ease of community building, communication, and knowledge transfer. However, social media can be a double-edged sword for firms that do not fully comprehend its far-reaching potential in influencing key stakeholders' perceptions of the firm, especially in crisis situations.

Within the institution, social media can significantly impact the relationship between employees and the corporate environment because it obscures the line between personal and corporate boundaries. Firms that allow the uncontrolled use of social media during the workday risk experiencing a decrease in employee productivity as employees become distracted and lose focus. A recent Mashable study reveals that some form of social media interrupts employees every 10.5 minutes—this translates into a loss from the entire U.S. economy of close to $650 billion.[27]

Social media can also compound employee loyalty problems and increase the chance of an insider leak, particularly as more employees become disenchanted with management. Even in cases where employee loyalty is unshakeable, the lack of restriction in social media channels can encourage unintentional information breaches. On that note, the introduction of social media into the workplace has also amplified the risk of cyber attacks, since social media platforms are thriving hotbeds of active viruses and malware, which can very easily be downloaded onto the internal network by an unsuspecting employee.

Social media also plays a key role in shaping the relationship between the firm and the public, and can make or break the firm's brand image. Platforms

like Facebook allow firms to directly interact with their customers—for better or for worse. For example, in March of 2010, Facebook users attacked Nestlé's Facebook page after Greenpeace harshly condemned the company for its use of palm oil in its candy products. Nestlé's attempts to contain the negative feedback by closing the page to comments only fanned the flames by drawing attention to the incident.[28]

The Nestlé case demonstrates the importance of social media in not just selling products, but also in building relationships with consumers. Nestlé could have taken advantage of its Facebook page by using it to provide an explanation or the rationale behind its use of palm oil to the public, which may have lightened the impact of Greenpeace's campaign against Nestlé. Utilized properly, social media platforms can actually be risk management tools because they provide early warning indicators of emerging stories and issues and the ability to communicate with stakeholders. As it was, Nestlé's misuse of Facebook only deepened the public's perception of the firm's culpability.

The first step to managing the risk associated with social media is to realize that social media affects the entire corporation, and is not simply limited to the IT department. As such, all efforts to broaden the existing risk management framework to include social media should be led by a team comprised of individuals from all sections of the firm and all levels of management. From this point on, we can then, for example, develop a social media policy that specifies the permitted and banned activities with respect to work time and company IT equipment. It would also be prudent to constantly monitor social media channels to identify emerging narratives and themes, as well as to intervene in any backsliding of the firm's public image.

CASE STUDY: HELLER FINANCIAL

Heller Financial is a commercial finance company with a market capitalization of more than $2 billion. At year-end 1998, Heller had over $14 billion in assets and net income reached a record $193 million. Heller's vision is to become the leading provider of specialized financing solutions to mid-sized and small businesses in the United States and select international markets.

On May 1, 1998, Heller Financial returned to the New York Stock Exchange and the ranks of public companies. Previously wholly owned by Fuji Bank, more than 42 percent of the company's stock was released in the initial public offering (IPO), generating more than $1 billion. The IPO raised the bar of competition; Heller must now not only compete for customers against its peers in the commercial finance industry, but also compete for

investors' money against the broad spectrum of public companies. Chief Financial Officer Lauralee Martin explains:

> *The stakes are higher. The benchmarks of performance are not just your own standards; the benchmarks are set against all others. Tougher competition naturally raises you to a higher level of performance.*

The market's mandate is clear: maximize shareholder value by achieving exceptional risk-adjusted returns on investors' capital.

Heller's financial goals after this IPO are to:

- Consistently increase return on equity (ROE) to at least 15 percent
- Raise its credit ratings to mid-to-high single A
- Grow earnings in excess of 15 percent each year by growing revenues, improving margins, increasing operating efficiency, and maintaining credit excellence
- Maintain a strong financial position based on solid credit discipline, prudent risk management, and a balanced and well-diversified funding strategy

Superior risk management is key to achieving each of these objectives. To increase return on equity to 15 percent requires efficient capital allocation. To raise credit ratings requires effective overall risk management. To increase operating efficiency while maintaining credit excellence requires solid understanding and management of operational risks.

Changes Within the Organization

Proactive focus on risk management is critical given the amount of change occurring within Heller's organization. During 1998, Heller consolidated its domestic operations around five core businesses: Corporate Finance, Commercial Services, Leasing Services, Real Estate Finance, and Small Business Finance. In addition, the Project BEST initiative restructured each of Heller's businesses to streamline processes, eliminating redundancies and reducing the workforce by 15 percent. Heller also acquired approximately $625 million in domestic and international assets associated with the technology-leasing business of Dana Commercial Credit Corporation. Through 1999, Heller continued to reorganize. Leasing Services has been broken out into Global Vendor Finance, Capital Finance, and Commercial Equipment Finance business groups. The Commercial Services business has been sold. The Healthcare Finance group has been acquired. Expansion into new international markets

and integration of the acquired Dana Commercial Credit Corporation into the Global Vendor Finance group continues, widening the range of vendor leasing products Heller offers to customers and prospects.

In July of 1999, the Chief Credit Officer, Mike Litwin, circulated a memorandum calling for Heller to change its risk management approach in response to this environment of increased risk. Litwin summarized:

> *The reality is that whenever an institution is in the process of change or is developing new activities, it runs into much higher operational risks than does a stable or existing business. A comprehensive and proactive focused enterprise risk management function must be in place to address the risks attributable to mergers, implementation of new systems and reengineering of processes, launch of new products or entry into new markets and the acquisition of new staff and client relationships. In addition, I believe the entire organization is under stress as a result of Project BEST initiatives as well as the pressures of being a public company.*

This memorandum served as the catalyst for adopting a new approach to risk. In September of 1999, Heller Financial embarked on an enterprise risk management (ERM) initiative to redefine its risk management vision, with a particular focus on management of operational risks.

ERM and Operational Risk Management

Senior management sponsors of the ERM initiative believed that managers and business leaders across the organization also saw the need for better risk/return management, but this belief had to be confirmed. Heller therefore conducted a thorough assessment of its current risk management practices as a first step in the ERM project. This process included:

- An internal survey of 38 members of the Leadership and Credit Councils regarding their overall attitudes toward risk/return issues
- More than 35 one-on-one interviews with senior managers to discuss the company's current state and future direction
- Internal studies and benchmarking analysis of the company's current risk management practices (risk management organizational structure, policies, analytics, and reporting)

The assessment confirmed two key things. First, that there is strong management support for the ERM initiative. Second, that the key gap in Heller's risk management included operational risk management and the integration of various risk management activities into an overall ERM framework.

Heller's Evolving Risk Profile

The changing nature of Heller's business calls for commensurate changes in Heller's approach to risk management. The structural change in the commercial finance industry from a buy-and-hold model to an originate-and-distribute model has shifted the risk profile of Heller's assets from traditional credit risks to integrated market-credit risk hybrids. The shift in Heller's businesses from transaction-oriented to more flow processes, such as small business lending and small-ticket leasing, also changes Heller's risk profile, creating the need for increased attention to operational risks.

Heller has always had a strong credit culture; the time has now come for Heller to integrate market risk and operational risk into its credit culture to develop a culture embodying the principles of enterprise risk management. While the current credit risk management process has produced superior asset selection, liquidity, concentration, and diversification, it cannot be used to manage losses due to human error or system failure. Chief Credit Officer Mike Litwin argues:

> *It is my view that at the present time we do not have significant credit risk issues in our company . . . the risks we should be focusing on and the ones that have potential to significantly impact our financial performance and market credibility are not limited to Credit and Market Risks, but must include . . . Operational Risks. Ultimately many of these non-credit risks could manifest themselves as write-offs, however, we're deluding ourselves if we think these are credit issues that can be appropriately addressed in the credit process. We will be attempting to address the "effect" rather than the "cause" of the problem.*

In order to become best in class in the commercial finance industry and achieve superior risk-adjusted returns on capital relative to the market, Heller needs to incorporate a more sophisticated understanding of risk-return tradeoffs in its decision-making and become the best manager of risk in its class. An ERM approach is needed to go beyond management of credit risk to full enterprise-wide risk-return optimization. ERM looks at the risks Heller faces holistically, rather than separately addressing market, credit, and operational risk. The risks that Heller faces do not always lend themselves to easy categorization. Market and credit risks are interrelated; operational risks often manifest as credit losses. ERM integrates management of market, credit, and operational risk to ensure that risks that overlap categories are fully understood, taking into account all interdependencies among market, credit, and operational risks, and to ensure that all risks are addressed.

Objectives of ERM

The objective for the ERM initiative is both to protect the company against downside risks and to improve business performance through an integrated view of risk and return. The ERM approach will help management identify and grow businesses with the highest risk-adjusted returns and thus maximize shareholder value. The goals of Heller's ERM initiative are to:

1. Create an enterprise-wide awareness of the importance of risk management for the company
2. Create comprehensive, enterprise-wide reporting of risk—credit, market, and operational
3. Reduce long-term writeoffs
4. Enhance credibility with external stakeholders and potentially reduce Heller's cost of funds
5. Increase Heller's market capitalization

Organizational Changes

A Chief Credit and Risk Officer (CRO) position was created (Mike Litwin became the CRO), with overall responsibility for management of all types of risk. The CRO will be responsible for strategically managing the credit, market, and operational risks of the organization and will centralize the reporting and management of all the risks Heller faces in one position. An Operational Risk Officer (ORO) position will also be created, with centralized responsibility for measurement, monitoring, and management of operational risks. This new position will enable Heller to implement a consistent operational risk management approach across all aspects of its business, provide an overall view of operational risk, and share operational risk management best practices and lessons learned across business groups.

Components of the ERM Project

The initial phase of the ERM initiative was completed in late 1999. There were substantial achievements during this first phase, which included the following:

- An *ERM assessment* was conducted to obtain a better understanding of Heller's risk management practices, as discussed in previous sections.
- A *benchmarking study* across all risk types for several dimensions of risk management practices was completed, and Heller's current state was benchmarked against other financial institutions' practices.

- An *ERM framework document* has been developed. It addresses the three main components for ERM—risk awareness, risk management, and risk measurement and puts risk terminology in a common language.
- *Heller's vision* for ERM has been defined and articulated with senior management.
- A detailed *implementation plan for achieving Heller's long-term ERM vision* has been developed. It also contains specific interim milestones to benchmark the company's progress.
- A *framework for operational risk management and a standard operational risk report template* have been developed that can be applied consistently across all business units and support services. The framework was piloted at two business units: Small Business Finance and Global Vendor Finance.
- An *enterprise risk report template* has been developed.
- An *economic capital proof-of-concept exercise* was conducted.

Implementation Phase

The implementation phase for Heller's ERM program addressed the following key challenges:

- *Organizational realignment*: the ERM and operational risk management objectives will be integrated into incentive compensation, roles and responsibilities, policies and procedures, and training programs.
- *Enterprise risk reporting*: the data environment needs to be improved to capture and aggregate information for the enterprise risk report and operational risk report.
- *Implementation of operational risk management methodology:* the new Operational Risk Officer will be working with the rest of the business groups and support services over the next year to apply the new operational risk management framework and begin producing the new standard operational risk report.

ERM is like a journey, which will require the organization's commitment to fully reach all of its goals. There are, however, some quick wins that require relatively fewer resources, which Heller should pursue in the near term. With the right up-front preparation and a clear road map for heading forward, Heller will realize substantial successes and benefits, as other organizations have experienced on their similar journeys.

Post Note

On July 30, 2001, GE Capital announced that it was acquiring Heller Financial for $5.3 billion in a cash transaction, or $53.75 per share (a 48 percent premium over the pre-announcement price of $35.90). In its press announcement, GE Capital noted Heller's risk management capabilities as one of the company's key assets.

CHAPTER 15

Business Applications

The application of risk management concepts was born thousands of years ago; in Chapter 8, we noted how references to insurance and derivatives could be found in texts that are thousands of years old. However, only since the 1970s has risk management really evolved as a business discipline, thanks to a combination of factors—economic liberalization, the rise of shareholder power, regulatory pressures, and the increase in computational power among them.

There are three major business applications of risk management. The first is loss reduction, the second is uncertainty management, and the third is performance optimization. The combination of all three is enterprise risk management. This order is both the order in which the applications were developed historically, and also the order in which a particular institution will typically develop its risk management capabilities. Let's consider these in turn.

STAGE I: MINIMIZING THE DOWNSIDE

The first stage in risk management, which emerged during the 1970s and 1980s, focuses on protection against downside risks. Risk management practices mainly involved establishing credit controls, investment and liquidity policies, audit procedures, and insurance coverage. The objective of these defensive risk management practices was to minimize losses:

- Credit risk management was designed to reduce the probability of default and to maximize recovery in the event of default, through credit approval at the front end, and debt recovery at the back;
- Market risk practices were designed to minimize potential portfolio losses and liquidity crises. Portfolio risk was minimized through conservative investment policies, favoring government bonds and high-quality corporate debt;

- Operational risk controls focused on reducing the probability and severity of operational events, with audit and compliance procedures to ensure that books, records, and operations were accurate and orderly. Insurance was the primary means of risk transfer.

As it turned out, however, a simple focus on the downside was not enough, illustrated most clearly by the failure of portfolio insurance. Invented in 1980 by Professors Hayne Leland and Mark Rubinstein of the University of California, Berkeley, portfolio insurance was intended to reduce equity investors' downside risk by automatically trading out of stock into cash when the market fell.

Some $60 billion in assets were insured in this way by October 1987—but when the stock market crashed that month, portfolio insurance managers struggled to carry out sell orders fast enough to keep pace with the requirements of the model. Insured investors did only marginally better than their uninsured brethren, most getting out at or below their designated floors. Nonetheless, portfolio insurance fell out of favor, even being blamed in some quarters for worsening the crash.

More broadly, loss reduction has always been, and continues to be, a central objective for risk management, but the early focus on downside risk management was too restrictive. It gave rise to the destructive offense versus defense mentality described in Chapter 6, where business units taking risks are frequently at loggerheads with risk functions minimizing risks.

One way of overcoming this tension was to demonstrate how risk management can be a positive force in supporting profitability and business growth. That led to the development of the second application of risk management: managing uncertainty.

STAGE II: MANAGING UNCERTAINTY

The second stage of risk management—originating from a string of insights during the 1990s—focuses on managing volatility around business and financial results.

Over the past few decades, many new sources of volatility have appeared and the effects of traditional sources of volatility have become magnified. The 1970s saw a move from fixed to floating exchange rates, along with wildly fluctuating oil prices; the 1980s, double-digit inflation, interest rate volatility, and lending crises. The trends continued into the 1990s with derivatives losses, volatile equity markets, and the rapid contagion of turbulence from market to market. Finally, the turn of the millennium brought about the Internet bubble and crash.

At the same time, investors have shown less and less tolerance for earnings volatility. As companies faced up to the challenges of increased volatility, risk management practices evolved to help management anticipate potential loss and reduce the range of potential outcomes—in other words, to manage that increased volatility.

- Credit scoring and migration models helped credit risk managers to develop more precise estimates of the probability of default when extending or reviewing credit transactions. This allowed more accurate annual provisioning for losses and thus reduced earnings volatility.
- Significant advances were made in the management of financial market risks. Sophisticated simulation models projected potential changes in earnings and market value, while industry-standard measures were established—notably value-at-risk and economic capital techniques.
- Recognition of the importance of operational risk management increased sharply during this period. Disasters such as Kidder Peabody, the Exxon Valdez oil spill, and the 1990 Perrier benzene-contamination scare brought crisis prevention and management to the fore. Moreover, numerous industry studies—the Treadway report (1991) in the United States, the Dey Report (1994) in Canada, and the Turnbull report (1999) in the UK—pointed out the need for effective corporate governance.

As risk managers focused their efforts to manage volatility, risk transfer products (including financial derivatives and sophisticated insurance) experienced a vast increase in popularity. However, derivatives can pose significant risks if used improperly; in particular, complex derivatives such as compound swaps and structured notes are often highly levered transactions that are extremely sensitive to market movements. Highly publicized debacles such as those involving Barings, Metallgesellschaft, and Bankers Trust convinced many people that derivatives, rather than reducing volatility were themselves a threat to financial stability. This is probably unfair; most of the fiascos were, at root, due to management or process failures.

Nonetheless, it became apparent in the late 1990s that conventional derivatives and insurance were by no means a complete solution to companies' risk transfer needs. The result was the emergence of new instruments covering previously uninsurable risks; alternative risk transfer (ART) manifested as a way of either transferring previously uninsurable risks or transferring traditional risks in a more efficient manner.

Another key development was the integration of various risk management silos. ART products enabled corporations to transfer packages of risk, rather than individual risks. This mirrored the development of integrated internal models and controls for risk—for example, the integration of market and credit risk when assessing counterparty default risk.

This more holistic view of risk allowed the risk/return profile of a business to be considered more explicitly than before. This, in turn, spurred the use of risk management as a lever for performance optimization.

STAGE III: PERFORMANCE OPTIMIZATION

In the third stage, risk management is characterized by a more integrated approach to all kinds of risk. The partial integration of similar risks in Stage II gives way to complete integration of silo risk management functions within the organization and the corresponding rationalization of risk control and transfer strategies.

However, a more important aspect of integration is that of risk and return. As we discussed in Chapter 4, ERM requires the integration of risk management into the business processes of a company. Rather than the defensive or control-oriented approaches used in Stages I and II, which are designed to manage downside risk and volatility, enterprise risk management optimizes business performance by supporting and influencing pricing, resource allocation, and other business decisions. It is during this stage that risk management becomes an offensive weapon for management:

- Companies have developed pricing models for credit products that fully incorporate the underlying default risk of the counterparty and are priced accordingly. Combined with active portfolio management based on concentration limits, diversification, and hedging strategies, this has led to disaggregation of the overall credit business into underwriting, origination, portfolio management, and distribution.
- In market risk management, companies are making asset-allocation decisions across all assets, liabilities, and off-balance sheet items held by the overall business, not just in their investment portfolios. In so doing, companies balance the expected profitability offered by the marketplace against financial and regulatory constraints.
- Operational risk management remains the biggest challenge in terms of knowledge and applications, but the level of awareness about operational risk has been raised significantly. The massive volumes of process maps produced by re-engineering projects are enhancing understanding of business and operational processes. Activity-based costing techniques add to this understanding by quantifying the cost drivers for various business and operational activities.

Finally, the application of risk management to performance optimization has been accelerated by the acceptance of risk/return management by

companies and regulators. The best example is the use of risk-adjusted return on capital (RAROC) as a performance metric used by business management not only to measure business profitability, but also to support key strategic decisions such as acquisitions and business unit strategies.

THE FURTHER EVOLUTION OF RISK MANAGEMENT

As we have already seen, good risk management is an integral part of business decision making, not something external to it. The other side of the coin is that changes in the business environment affect the practice of effective risk management. Some obvious mega-trends affecting all industries are:

- Globalization—the growing interdependence of economies and markets and the internationalization of business operations through networks;
- Technology—the new operational risks associated with technology-driven businesses;
- Changing market structures—the impacts of deregulation, privatization and new competition; and
- Restructuring—the effects of mergers and acquisitions, strategic alliances, outsourcing, and re-engineering.

Each of these trends gives rise to new risk management challenges. However, that doesn't mean that these trends should each be considered in isolation, which would be a return to silo-based thinking; most are intimately related to each other.

For example, improvements in communications technology have helped to bring down the barriers between markets that were historically distinct, and contributed significantly to the globalization process. That in turn has forced deregulation, allowed new competitors to enter hitherto protected markets, and forced incumbents to rethink their organizational structures and practices.

Ultimately, it is safe to say that we live in times of great change, and the risks that these changes bring up require an integrated, enterprise-wide response. In this chapter, we discussed risk management applications from the perspective of any business. In the remainder of this section, we will examine risk management applications from the perspective of different industries and the specific challenges they face.

CHAPTER 16

Financial Institutions

The financial-services industry is in the throes of a transformation that is redefining both the competitive landscape in which financial institutions operate, and the dynamics of risk and return that shape their businesses. In the aftermath of the global financial crisis, banking regulators have dramatically increased their regulatory capital requirements and examination standards. If existing financial institutions are to survive and thrive in this new business and regulatory environment, they must adapt their business models and improve their risk management capabilities.

Financial institutions[1] are different from other companies in the sense that their ability to measure and manage risk is central to their competitiveness. Risk management has always been a core competence for financial institutions, and risk performance a key determinant of profitability. As Gary Wendt, the former CEO of GE Capital, put it: "If you don't get the risk management part of the equation right, then nothing else will matter." Put another way, the key to a financial institution's survival and prosperity is its ability to identify, quantify, price, and manage risk better than its competitors. As a manager of other people's money, the ability to gain and maintain the trust and confidence of clients is an absolute requirement for business success.

Moreover, the business of financial risk management involves some level of expected losses, which represent an important business cost component. Financial losses traditionally make up a significant portion of the cost of doing business in the financial services industry. Unsurprisingly, then, financial institutions are keen to point out how good they are at risk management. Their annual reports normally include a detailed discussion of the company's risk management capabilities, including risk committees and strategies for different types of risk.

As we'll see in this chapter, however, it is not enough for a financial institution to rest on its laurels. The financial services industry has been changing rapidly since the 1980s, with the result that the challenge of risk management is dynamic, not static. First, we'll examine the key industry trends that are changing the fundamental structure of the financial services industry.

We will then discuss the risk management requirements of financial institutions, with the aid of a case study of CIBC. Finally, we will briefly discuss the key challenges for the future management of financial institutions.

INDUSTRY TRENDS

To appreciate fully the risks facing financial institutions and the best approaches for managing them, we must first understand the fundamental business trends in the industry. There are four major, interrelated trends: consolidation, deregulation, competition, and convergence. Let's run through these in turn.

Consolidation

The financial services industry has been undergoing a massive wave of consolidation, beginning in the mid-1980s with American banks and subsequently spreading both to other types of financial institutions and around the world.

For example, the number of FDIC-insured banks in the United States shrank from 14,500 in 1984 to 6,096 in 2012, representing a 58 percent decline.[2] The number of banks acquired annually increased from 330 in 1985 to a peak of about 600 in the mid-1990s. While this number dropped steadily to below 400 in 2001, it surged again in 2007, which saw 1,048 deals.[3] After the financial crisis of 2008, only 198 deals were made in 2011, but the concentration of banking assets continues.[4] Research conducted by the New York Federal Reserve shows that these mergers have resulted in a doubling of the market share of industry assets owned by the 10 largest banks from 30 percent to 60 percent in the last 20 years.[5] Insurance companies and insurance brokers likewise consolidated; 19 of the top 31 brokers in 1988 no longer existed 10 years later.[6] As Sally Roberts notes in an article for *Business Insurance*, "of the 16 brokers that appeared in *Business Insurance*'s first broker profile issue in 1972," only Marsh & McLennon Cos. Inc. remained in 2007.[7]

Why this insatiable urge to merge? The first reason is simply that firms were now allowed to do so, thanks to deregulation (to which we will return below); changes in banking legislation first opened the floodgate to bank mergers and acquisitions. The 1927 McFadden Act and the 1956 Bank Holding Company Act had previously restricted interstate banking, but the 1994 Riegle-Neal Interstate Banking and Branching Efficiency Act overturned this, ushering in nationwide banking by October 1995. As mergers began, they were apparently self-perpetuating, as one-stop shopping and economies of scale became the buzzwords of the day. If a small bank did not merge, the belief was that it would be left behind by larger institutions that offered more products at more attractive prices.

For insurance companies, consolidation was facilitated by demutualization of their ownership structures. Insurers in the United States, the United Kingdom, Canada, Australia, South Africa, and other countries converted from their traditional mutual ownership structures to become shareholder-owned, often publicly offering their stocks at the same time. Demutualization funded a number of mergers, either by allowing the insurer to purchase other companies using stock instead of cash, or by raising cash for the transaction through a public offering.

Consolidation comes with its own risks. In particular, the considerable challenge of combining the different cultures and business systems of two financial institutions should not be underestimated. This may be part of the reason why the expected economic benefits of a merger rarely turn out to be as great as anticipated. In fact, separate studies done by KPMG and A.T. Kearney revealed that mergers do not enhance shareholder value. The KPMG study indicated that 83 percent of merger deals do not yield higher shareholder returns, while the A.T. Kearney study reported that "total returns on M&A were negative."[8] Another study found that bank acquirers in North America have underperformed in the past years, "with five consecutive negative quarters since Q3 2011."[9]

Deregulation

Deregulation in the financial services industry has been a double-edged sword. On the one hand, it removes unnatural regulatory barriers and allows greater competition; customers should reap the usual benefits in terms of lower price, better service, and greater choice. On the other, it exposes previously protected institutions to market forces and discipline. This can result in the demise of weaker players that may be ill-prepared to face the new risks of market volatility and intense competition.

An economist might argue that the weeding out of weaker players is a good thing over the long run, despite the short-term costs of bankruptcy, such as job loss and service interruptions—particularly because these short-term costs can be minimized if deregulation is planned and phrased in a thoughtful way. Sudden, poorly executed deregulation can give rise to undesirable behavior and to the potential for significant losses, often ultimately borne by the taxpayers.

A dramatic example is the case of the savings and loan (S&L) crisis of the late 1980s. During this dark episode in the history of U.S. finance, relaxed vigilance on the part of thrift regulators—combined with increased rate volatility and lax internal risk management—led to vast losses to the taxpayer.

A wave of deregulation between the late 1970s and early 1990s reduced the minimum capitalization required of S&Ls, abolished the ceiling on the interest rates they could offer customers, and allowed them to enter new

businesses, like stock brokerage. S&Ls quickly found they had to raise interest rates paid out if they were to retain customers in the competitive market for deposits. The problem was that there was no practical way to raise the rates they earned on lending—their main use of funding—to match the increased deposit rates.

The result was widespread losses through the industry in the 1980s, exacerbated by risky real estate deals made in doomed attempts to bridge the gap. The subsequent losses put renewed pressure on the institutions to not only raise deposit rates, but also extend their sources of funds from retail to wholesale customers, which led to a vicious circle in which rates continued to spiral and investments got increasingly riskier.

The rest is history. Huge swathes of the S&L industry went bankrupt, while the Federal Savings and Loan Insurance Corporation (FSLIC), which insured all S&Ls to the tune of up to $100,000 per depositor, was completely overwhelmed. Faced with bailouts costing $38.6 billion in 1988 alone, it was forced to keep more than 500 insolvent institutions open because it simply lacked the capital to shut them down and pay off their investors. The aftermath took years to clean up, at huge expense to the taxpayer.

Some good did come of the S&L disaster, albeit at far too high a price. Banks and thrifts created asset/liability risk management units that implemented gap, duration, and simulation techniques to analyze the interest-rate sensitivity of their balance sheets. They also designed mortgage products that were less sensitive to interest-rate changes. For example, adjustable-rate mortgages were invented that matched more closely with short-term liabilities such as deposits and CDs.

Banking regulators around the world revised capital requirements to more closely align capital with risk. In 1988, the BIS issued risk-based capital requirements that, for the first time, tied capital explicitly to the assets held by banking institutions. Another lesson the banking regulators learned was how to deal more effectively with the trade-off between closing an ailing institution and maintaining any remaining franchise value; isolating bad assets in a bad bank so they can be disposed of, while the good bank can be operated independently or be sold to a buyer. This was the approach adopted by Japanese regulators a decade later, as they worked through the massive credit problems in their country's banking system.

Competition

The wave of deregulation in the 1980s didn't just give established financial institutions enough rope to hang themselves; it also gave new competitors enough rope to trip them up. For example, mutual fund companies were

allowed to grant customers check-writing privileges. That allowed them to compete with checking accounts at banks while offering the more attractive returns of mutual funds.

Together with the advent of new information technology and the increased liquidity of the capital markets, deregulation meant that established financial services companies often found themselves vying with new (and sometimes more efficient) competitors for business—indeed, this was frequently the actual motivation for the deregulation. Change came swiftly, as exemplified by developments in the retail banking sector. By 1998, only 23 percent of households' liquid financial assets were held in conventional bank deposits, down from 49 percent in 1980.[10] Credit cards, mortgages, and commercial loans were also increasingly handled by non-bank institutions. As an example, the percentage of credit card outstandings held by community banks declined from 49 percent to 25 percent between 1984 and 2011, with much of that business going to non-bank institutions.[11]

Clearly, banks (in particular) needed both to cut costs and to find new ways to attract and retain customers in order to avoid further erosion of profitability and market share. The rise of e-commerce arguably allowed them to do just that, but it was non-banks who were quicker to grasp the possibilities. That meant new entrants, particularly those who had the advantage of specialization, were able to further encroach on businesses that had traditionally been the sole domain of banks.

One particularly dramatic development was the emergence of a new breed of online banks and brokerages. Because they lacked the costs of physical branches and customer service personnel, these institutions could offer extremely attractive rates, among other features, such as free electronic bill payment and low (often zero) minimum balances and fees. Online brokerages have likewise attracted investor dollars with the lures of efficiency and cost savings: online trading is cheaper and faster than trading by telephone or in person, and most online brokerages also offer conveniences like free real-time stock quotes, online portfolio tracking, and easy access to research.

But online brokerages face perils of their own. One key issue for the first wave of online brokerages, given the investment climate of the time, was the development and management of a strategy for rapid growth. Online brokerages needed to win potentially nervous users away from the incumbents, and so often adopted aggressive marketing strategies. Having attracted those users, they needed to deal with the swift development of technologies and processes to handle them.

Rises in competition also changed the face of the insurance industry during the 1990s. Rates for insurance decreased steadily from 1986 onward, largely as a result of increased competition within the industry. The soft

market was a boon for insurance buyers, who were able to take advantage of rock-bottom rates, but put an enormous strain on the providers. For example, in 1998 premiums rose by a mere 1.4 percent, while incurred losses rose 6.5 percent, and expenses rose 4.3 percent.[12] Many insurers' continued viability owed much more to the outperformance of their asset portfolios, which was driven by the runaway bull market, than to their prowess in underwriting. However, the recent bear market and post-September 11 claims have reversed these trends, as investment performance has declined but insurance premiums have increased dramatically.

Meanwhile, the nascent alternative risk transfer (ART) market threatened to further erode the insurance industry's market share and profitability (see Chapter 9 for more information on ART). While it would be in the insurers' best interests to see higher pricing in the market, the fact that ART providers are trumpeting savings as high as 20 to 30 percent over insurance premiums during a soft market does not make a hardening of the market seem feasible. ART products also provide greater flexibility and efficiency for the customer. Such products can be customized to meet particular customer needs and offer greater efficiency, since they often cover the buyer for a number of years and may reduce the number of insurers needed. Just as the mortgage-backed security market has reduced the cost of mortgage financing, the ART market should reduce the cost of risk transfer by increasing the availability of cheaper sources of risk capital.

Convergence

A third consequence of deregulation has been the elimination of barriers between different kinds of financial services. In the United States, for example, the Depression-era Glass-Steagall Act put a regulatory fence between securities business and commercial banking, as well as insurance. This meant that for nearly 50 years, the United States was home to entirely separate securities, banking, and insurance industries. This contrasts with the European situation, in which universal banks and bancassurers carried out various combinations of these activities.

During the 1980s, however, it became clear that regulation in the U.S. financial services industry began to relax; in response, commercial banks began underwriting securities on a limited basis. Banks were also allowed to sell mutual funds, bringing them even closer to achieving the status of financial clearinghouses. In turn, money market funds offered by mutual fund companies were allowed to offer check-writing privileges, which had previously been limited to banks. Insurance and banking also began to overlap as banks viewed insurance policies—along with annuities, retirement funds, and mutual funds—as opportunities to increase fee income.

By 1998, it was clear that the old legislative framework had crumbled, as evidenced by the debut of Citigroup, the financial titan formed by the merger of the Travelers Group (predominantly an insurer), Citibank (a commercial bank), and Salomon Smith Barney (a securities house that had just been acquired by Citibank). Citigroup's very raison d'être was to realize value by cross-selling banking, insurance, and securities services, and it apparently worked, as Citigroup's stock has outperformed those of other, less diverse banks. However, there is growing public and regulatory concern that convergence comes with a steep price when it comes to issues such as conflicts of interest (e.g., research versus investment banking), tying of financial products and services, and consumer rights.

The convergence of investment banks, commercial banks, and insurance companies has direct implications for enterprise risk management—both for better and for worse. The benefit is that such companies are more diversified, which smoothes their overall risk profile; they can also offer products that offer the advantage of such diversification to their customers. The cost is that the risk management of these multi-line financial businesses needs to be integrated if such benefits are to be realized, which is a challenging task.

RISK MANAGEMENT REQUIREMENTS

The confluence of the trends discussed above has increased the stakes for risk management for all players in the financial services industry. Deregulation has removed the barriers that once protected the industry from competition and from its own mistakes; consolidation and convergence has resulted in companies that are far larger and more complex than those that have gone before.

Risk management has become absolutely vital in ensuring both that established players do not lose the race and that new ones do not fall at the first hurdle. In the modern financial services environment, the consequences of a failure of risk management frequently go well beyond financial loss or strategic setback; in fact, they may ultimately include the demise of the afflicted institution as an independent company. The bar has been raised: what might have been considered best practice a few years ago is likely to be seen as a basic requirement today. To ensure ongoing success and survival, financial institutions must continuously upgrade their risk management capabilities.

Let's first consider the main types of financial institutions. We'll see that each type faces market, credit, and operational risks, but these take on different forms according to a particular institution's businesses. In the next section, we'll look at the challenges that cut across industry sectors and are common to a number of different types of institution.

Risks by Industry Sector

Depository institutions, such as commercial banks or thrifts, take credit risk by extending loans to borrowers. This credit risk must be managed through prudent credit analysis and effective portfolio management in order to prevent excessive credit losses.

One major source of profitability (and earnings volatility) is the interest rate spread between asset yields and liability costs. Interest rate risk arises from the difference in interest rate sensitivities between financial assets and liabilities. A depository institution's management must therefore establish appropriate asset/liability management and hedging programs in order to ensure a positive and stable interest rate spread throughout various interest rate cycles. As we saw in the discussion of the U.S. savings & loan crisis, the one-two punch that knocked out the industry was a round of higher interest rates followed by commercial real estate losses.

Another key source of profitability is fee income from services such as cash management and securities processing. The operational risks associated with these services must be managed to ensure accurate cash and securities movements and record keeping.

Securities houses such as brokerage firms or investment banks take on a variety of market risks. As securities underwriters, they earn a fee for assuming the risk that a new equity or debt offering will fail to win market acceptance at a favorable price. Failure can result in financial losses as well as tarnished reputation.

As market makers in certain securities, securities houses face the risk of market losses in a declining market. These losses may come from their existing inventories, as well as from new commitments that arise in the course of their market-making activities. These risks are still more significant if a firm is engaged in proprietary trades on its own account as well as trades made on behalf of customers; it may face huge financial losses if its market predictions are wrong.

In addition to market risk, securities firms very often take on default risk through margin lending to individuals and securities lending to institutions. They also face the counterparty risks associated with securities settlement processes and financial obligations such as swaps and other derivatives.

Insurance companies take on actuarial risk when they issue insurance policies that may result in larger-than-expected claims in the future. Their primary sources of income are the premiums paid on insurance policies and the investment income generated by investing the cash flows from these premiums. These income sources must between them cover expenses and claims. The ratio between the sum of premiums and investment income and the sum of expenses and claims is known as the *coverage ratio* and is a widely followed indicator of industry profitability.

Thus, insurance companies face two key risks. The first is a function of the relationship between premiums earned and claims paid; the second is the performance of the investment portfolio. In addition, insurance companies often cede a portion of their premiums to other insurance or reinsurance companies, which in turn take on a portion of their insurance liabilities. Since the ceding insurer may have to call upon the reinsurer if an insurable event occurs, it is exposed to the risk that the reinsurer may fail to pay up—a credit risk.

Insurance companies are also exposed to operational risks, often related to the complex distribution system for their products. Historically, insurers have often relied heavily on sales agents to distribute their products. The loyalty and discipline of these agents is variable, since they may be employees or free agents, and their compensation is linked heavily to commissions from one or more insurers. It is relatively easy for the incentive structure to become inappropriate, with potentially damaging results—as seen in both the United States and UK—in regard to various lawsuits on unfair sales practices on insurance policies and pension plans.

Cross-sector Risks

In addition to the sector-specific risks discussed above, financial institutions as a group are faced with a number of financial risks that are more fundamental to their business activities than they are to the business of non-financial institutions. While these present particular challenges for financial institutions, they represent important issues for any corporation with significant financial operations and capital markets activities.

Monitoring default and counterparty risks As discussed above, financial institutions are exposed to a variety of default and counterparty risks. These credit risks arise mainly from lending activities, trading and settlement processes, insurance/reinsurance contracts, and derivatives transactions. The two key questions to ask are:

- What is my aggregate exposure to a single counterparty or a group of similar counterparties?
- What is the likelihood of default and loss?

These questions can only be answered if there is an adequate credit-exposure measurement process and an accurate credit rating system.

Managing market risks on and off the balance sheet One unique characteristic of financial institutions is that most of their assets and liabilities are sensitive to

movements in one or more markets: interest rate, equity, foreign exchange, commodity, and/or real estate. Market risk exposures can originate both from on-balance sheet activities and from off-balance sheet transactions such as derivative contracts and forward commitments.

In order to manage market risks effectively, a market risk manager must first measure the sensitivity of the portfolio to external price changes. This analysis can be based on a combination of value-at-risk (VaR), scenario testing, and simulation modeling. Given an accurate and timely assessment of market risks, management can then decide on risk management strategies including product design and risk transfer.

Incorporating leverage and liquidity Financial institutions are generally much more highly leveraged than their non-financial counterparts, as a result of the need to maximize asset risks given thin profit margins and pressure from shareholders for healthy returns on equity. However, just as leverage increases the absolute returns on assets, it also magnifies the effect that a decline in asset values would have on the equity value of the institution.

Another important consideration is the liquidity profile of an institution's assets and liabilities. For example, an institution can easily liquidate a large position in U.S. Treasury securities, but may find it difficult to reduce its holdings in debt issued in an emerging market. Financial institutions must therefore be fully aware of how their market and credit risk exposures will be affected by leverage and liquidity. It is not enough to measure the 10-day VaR of an asset alone. The risk manager must establish a reasonable liquidation period over which price volatility should be measured, and also quantify the potential impact on equity value given the leverage of the firm.

Attributing economic capital and managing portfolio risks Economic capital represents the amount of capital required to support a consistent level of potential loss across all risk exposures. In essence, economic capital represents a common unit for the measurement and management of risk, and is an important concept for financial institutions to understand and apply. It is valuable because its attribution to risk exposures enables management to measure risk-adjusted profitability across different business activities.

For example, economic capital allows the profits from trading to be compared directly with profits from dissimilar businesses, such as retail lending or securities processing. Economic capital can also be used to support portfolio management decisions, such as the allocation of financial and human resources, to business activities that generate higher risk-adjusted returns. By explicitly incorporating the benefits of diversification, economic capital provides the appropriate signals and incentives for diversification and limit setting. Finally, risk transfer decisions, including hedging and insurance,

can be rationalized by comparing the cost of risk retention (i.e., the cost of economic capital for the underlying risk) with the cost of risk transfer.

SYSTEMIC RISK

Interdependency is part of the quintessential nature of financial institutions, with linkages created through business activities such as securities trading, foreign exchange, derivatives trading, reinsurance, syndicated underwriting, and stock lending. These relationships are the root cause of concerns about *systemic risk*, or the possibility that problems at a single large financial institution could create a chain reaction that could result in large losses or defaults at other institutions.

Systemic risk is the primary concern of many regulators, whose attention has shifted from the stability of individual organizations to the stability of the industry or system. An individual firm's management also has cause to be concerned, however: even if the system survives, the company may nonetheless suffer collateral damage along the way. The challenge for management is therefore to understand fully these interdependencies with other financial institutions and to put in place appropriate contingency plans and exit strategies in the event of a significant disruption in the financial system. It is also important for management to establish early warning indicators, such as higher market volatility or lower liquidity.

The events that lead to systemic risk tend to be rare and idiosyncratic, but there are two points to bear in mind. First, financial institutions face risks that are highly intertwined. For example, a sudden market drop can cause the default of a major financial player, leading to a loss of confidence and a liquidity crisis, which may in turn exacerbate the market drop. Secondly, the interdependencies in the financial system are not only associated with discrete transactional risks, but also with the linkages between institutions, markets, and countries. These global economic linkages only reinforce the criticality of the risk management requirements discussed above.

Consider the global financial crisis of 2008. The collapse of the U.S. housing bubble led to repercussions that echoed throughout financial institutions and markets around the world. An array of explanations have come forth which speculate about the cause of the housing bubble—they point fingers at factors ranging from misguided monetary policy to irrational consumer expectations. The fundamental cause of the crisis lies in both the huge increase in risky mortgages and the unrealistic expectations of both mortgage lenders and homeowners that housing prices would continue to rise, as they did from 1990 to 2006, while interest rates would remain low.

Traditional mortgages required substantial down payments of 20 percent of the house price, used primarily as collateral to reduce default risk. However, as house prices increased, and the demand for funds to purchase houses rose, mortgage lenders began to allow subprime loans for people who normally would not qualify. The roots of this movement can be traced all the way back to the Community Reinvestment Act of 1977, which encouraged banks to make loans to low-income borrowers, in pursuit of the ever-glorious American dream of universal home ownership.[13] These subprime lenders no longer required stringent down payments or income documentation; when default rates were low, moderate subprime lending was profitable. The rationale was that the borrower could always take out a second mortgage or sell his house at a higher price to pay back his debt. By 2007, home ownership was at a record high of 68.6 percent, which at the time, made the subprime mortgage system seem like a resounding success.

However, there was more to this system that initially met the eye. After accumulating these loans, the lenders would securitize entire pools of mortgages for sale to financial institutions, including commercial banks, investment banks, hedge funds, pension funds, insurance companies, and mutual funds. The issuers of the securities kept the residual risk, allowing mortgage-backed security issuers to raise capital from risk-seeking investors. These mortgage-backed securities were rated as triple-A assets by ratings agencies such as S&P, Moody's, and Fitch—time would prove them shockingly wrong.[14]

The two largest issuers of mortgage-backed securities were Freddie Mae and Fannie Mac, who initially purchased prime mortgages from borrowers who had good credit scores. However, in 2005, some investment banks also started issuing mortgage-backed securities—except these securities were from subprime mortgage-borrowers with weak credit histories. Although securitization allowed for some diversification of risk, it provided more funds for subprime loans, which allowed the perception of lower risk to snowball, while real, systemic risk was actually growing exponentially. This is epitomized by Alan Greenspan's remark in a speech at the 2005 annual convention of America's Community Bankers: "Overall, while local economies may experience significant speculative price imbalances, a national severe price distortion (i.e., a housing bubble) seems most unlikely in the United States, given its size and diversity."[15] The threat of a sharp decline in housing prices seemed minimal, but the drastic build up of risk was beginning to seethe ominously.

When house prices started to drop in 2006, homeowners that had bought their houses through subprime loans suddenly realized that they were left with mortgage payments they could not pay, which led to a wave of defaults. This shock caused investors to scramble to sell off their mortgage-backed securities, now revealed as ticking time bombs, leading to a further, more

drastic decline in their prices. As a result, investment banks, among other investors, experienced huge losses. In 2007, New Century and Ameriquest declared bankruptcy, while other financial institutions were estimated to suffer losses of more than $150 billion. Despite the expansionary policies pursued by the Fed, the entire economy contracted at an alarming rate.

Once these effects started to ripple out to England, Northern Rock Bank ran short of liquid assets. The Bank of England approved an emergency loan, which caused depositor confidence to plummet; as a result, depositors rushed to withdraw funds in England's first bank run in over a century.

As losses on subprime mortgages continued to rise, banks began to reduce credit availability, which further restricted economic growth. Banks like Bear Stearns and Lehman Brothers, which relied heavily on subprime mortgage-backed securities, found themselves cut off when other financial institutions, which viewed these securities as liabilities, stopped lending to them. In 2008, Bear Stearns had to be bailed out by the Fed to the dismal tune of a $30 billion loan, while Fannie Mae and Freddie Mac were bailed out for $200 billion. The arrangement for Lehman Brothers to be taken over by Barclay's fell through at the last minute. The bank had been a pillar of the financial system since 1850, and, furthermore, it was also the largest U.S. firm in any industry to declare bankruptcy—its fall led to massive, widespread financial panic.

Many of the credit default swaps (CDSs) issued in the 2000s were tied to these mortgage backed securities (MBSs). The sellers of CDSs on MBSs promised to reimburse their buyers if the market prices of the MBSs fell under a certain level. American International Group (AIG), which issued large amounts of these CDSs, reported in 2006 that the likelihood of losses on CDSs was "remote, even in severe recessionary market scenarios."[16] However, on September 16, 2008, when things began to quickly unravel, the Fed had to make an emergency loan of $85 billion to AIG in order to prevent a collapse on the scale of Lehman Brothers. AIG was deemed a classic bank that was too big to fail. Fed Chairman Ben Bernanke justified the Fed's actions by asserting that AIG's collapse "could have resulted in a 1930s-style global financial and economic meltdown, with catastrophic implications for production, income, and jobs."[17]

A LOOK TO THE FUTURE

Financial institutions have only recently started to manage risk in an integrated fashion. Traditionally, different types of institutions specialized in different types of risk: investment banks in market risk, commercial banks in credit risk, and insurers/reinsurers in insurance risk. However, the

industry is slowly moving toward specialization by function rather than by risk type.

In this framework, origination and customer service will be handled by risk brokers, separate conduits will handle underwriting and balance sheet management of all types, integrated investment banks will execute capital markets risk transfer, and portfolio managers will handle both financial and insurance securities. Similarly, risks that have traditionally been handled in silos are finally starting to be treated holistically by risk management teams reporting directly to the board.

Given the squeeze on profitability that all types of financial institutions have been experiencing, coupled with the increasingly complex risks of a global financial world, financial institutions must continue to be sophisticated in their quantification and analysis of risks. They must also balance this with an increased emphasis on the soft side of risk management by realigning incentives to promote ethical, risk-aware behavior, setting a tone of openness from the top, and developing communication channels to discuss risk issues.

As we saw at the beginning of this chapter, prudent risk management is not just about mitigating potential downsides, but also about maximizing profit in a safe way. In today's business environment, just one mistake could easily push a company into bankruptcy. The collapse of Lehman Brothers during the 2008 financial crisis is a prime example of this, and it caused business leaders to pause and reassess their overall approach to risk management. Moreover, potential consumer losses arising from Lehman-backed structured products and the AIG enhanced funds also led to important changes in risk disclosure practices.

On July 21, 2010, President Barack Obama signed the Dodd-Frank Wall Street Reform and Consumer Protection Act into law. This piece of legislation set out to reshape the U.S. regulatory system in consumer protection, trading restrictions, credit ratings, regulation of financial products, corporate governance and disclosure, transparency, and so on, in order to prevent another financial crisis of the size and nature of that of 2008. Instead of contracting the entire financial sector by limiting the amount of risk that banks can take, the Dodd-Frank Act attempts to single out the biggest institutions for "higher capital requirements and more careful scrutiny."[18]

For example, in section 165 of the 2010 Dodd-Frank Act, legislators mandate that the "FRB must require each publicly traded bank holding company with $10 billion or more in total consolidated assets . . . to establish a risk committee [of the board] . . . [the] Risk committee must . . . include at least 1 risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms."[19]

Title VI of the Dodd-Frank Act implements the Volcker rule, which attempts to minimize conflicts of interest between banks and their clients.

For example, it prohibits investment banking, private equity, and the proprietary trading sections of financial institutions from simultaneously entering into an advisory and a creditor role with clients. It also prohibits "insured depository institutions" from having any kind of ownership in hedge funds or private equity.[20] Hopefully, this will help to reduce the problem of imperfect information, where clients, among other shareholders, only have a very murky idea of what their banks are actually doing.

The Dodd-Frank Act and new Security Exchange Commission (SEC) disclosure rules also established stricter requirements for board risk oversight and risk-compensation linkage. In particular, the SEC implemented new rules that increase mandated disclosure with regard to "compensation, corporate governance, and risk policies and practices," that went into effect on February 28, 2010.[21] These new rules require increased disclosure in the following areas, among others:

- Compensation policies and packages for employees involved in risk management processes and risk-taking activities
- The qualifications and previous experiences of directors and director candidates
- The director-candidate evaluation process
- The structure of the board in terms of leadership and the overseeing of risk management
- The company's relationship to external consultants.[22]

These new mandates were designed to improve transparency into the risk management practices of publicly traded companies.

Despite the best intentions of the Dodd-Frank Act, and similar efforts to change the corporate culture that caused the 2008 financial crash, there are many who remain skeptical of their ultimate effectiveness. Arthur E. Wilmarth, Jr., a professor of law at George Washington University, believes that the Dodd-Frank Act is fundamentally shaky because it "[depends] heavily on many of the same federal agencies that failed to stop excessive risk-taking by LCFIs in the past," where the term LCFIs refers to "large complex financial institutions."[23]

He grants that certain aspects of the Dodd-Frank Act are positive—for example, the Orderly Liquidity Authority mandate, which provides a "superior alternative to the "bailout or bankruptcy" choice that federal regulators confronted" in 2008."[24] However, he nonetheless remains unconvinced that the Dodd-Frank Act has closed the enormous loopholes that litter the financial landscape. He maintains that the Dodd-Frank Act has not eliminated the many dangerous avenues of alternative financing—which are what caused the too-big-to-fail problem in the first place.

Reactions from the banks themselves have also been rather lukewarm. In a 2010 study conducted by Ernst & Young, 53 percent of the surveyed bank executives believed that "in the long run, profits will be significantly lower as a result of increased regulation."[25] Even more disappointing, only 14 percent "agree that the current approach to financial regulation at the global level is sufficient to make another global financial crisis much less likely."[26]

CASE STUDY: CIBC

The Canadian Imperial Bank of Commerce (CIBC) is a full-service financial institution with $270 billion in total assets and 44,000 employees operating around the world. In 2000, the bank generated $12 billion in revenue, earned $2 billion in net income, and achieved a 20.5 percent return on equity (ROE).

The financial services industry in Canada, like that in the United States, had been characterized by consolidation. Many Canadian banks allied themselves with other financial institutions, often through outright mergers and acquisitions, either to benefit from economies of scale or in order to deliver the wide range of financial products that their customers were demanding. CIBC's critical move in this respect was its 1988 acquisition of majority interest in Wood Gundy—a well-regarded Canadian investment bank. The Wood Gundy purchase signaled CIBC's intention to broaden its financing capabilities for corporate customers. The decision to offer integrated, global financial services and offer an increasingly complex product portfolio (including exotic and structured derivatives) motivated a substantial re-think of risk management at CIBC.

At the same time, Canadian regulators were beginning to think more in terms of enterprise-wide risk management. This culminated in the December 1994 Dey Report, published by the Toronto Stock Exchange (TSE), which recommended that the Board of every firm listed on the TSE take direct responsibility for risk management efforts within their firm, and communicate those efforts in the annual report. For banks, in particular, the Canadian banking supervisors were among those who drafted the 1996 Amendment to the Basel Capital Accord, which similarly emphasized firm-wide risk reporting and control.

So CIBC had a two-fold reason to invest in enterprise risk management (ERM). It was becoming more active in the capital markets at much the same time that regulators were looking closely at risk management. Its reaction was to start building an ERM team; its first significant high profile hire was Dr. Robert Mark, who joined the bank in July 1994 to be the Corporate

Treasurer as well as look after firm-wide market risk, operational risk, and sections of credit risk which included responsibility for managing credit risk in the trading book. Dr. Mark was promoted to Senior Executive Vice President and became CIBC's Chief Risk Officer in February 2000 and joined the CIBC Management Committee.

Dr. Mark articulated his vision from the very beginning, outlining his plans to build a strong ERM team made up of experienced risk managers with substantial business experience, to work in partnership with, but independent of, the business lines. "I will need your commitment to support my vision," he explained to key senior management and the board during his selection. He pointed out that "[the] objective is to be among the top five financial institutions in the world in terms of managing risk." Dr. Mark emphasized how he was going "to come in and make changes. There's no doubt about that." The board was not put off, and when Dr. Mark joined CIBC, he did so with a mandate to deliver world-class risk management.

Changes and controversy duly followed. Of the team he inherited, none were to be found doing the same job a year later. New executives with significant risk management and trading experience were put in place to implement the new vision. There was also a compensation differential between risk staffers and their colleagues on the business side that had to be evened out in order to attract and retain the requisite talent. Dr. Mark pointed out that his business partners were highly encouraging and supportive of upgrading the quality of risk personnel. In short, the change was nothing less than dramatic.

Today, the firm collects risk data from across the globe and disseminates risk reports through a series of risk management and business committees, illustrated in Figure 16.1. Risk management committees at CIBC establish risk management policies, limits, and procedures, approve risk management strategies, and monitor portfolio performance and trends. The Risk Management Division works closely with both the lines of business and risk management committees to manage CIBC's exposure to market, credit, and operational risks. "One of the keys to success is getting business and risk people to work effectively together," says Dr. Mark, "If you have people from both camps sitting together, agreeing, disagreeing, asking questions, then we all have a clearer understanding of the problems we face, and a clearer path to the answers. Our business partners provided us with invaluable insight as we evolved our risk management function into a world-class team."

The kind of Socratic dialogue that Mark favors isn't always frictionless. There have been occasions when risk management has been obliged to restrict the amount of business that certain units can carry out. "The ability to generate revenues is clearly a function of the volume of business you do,"

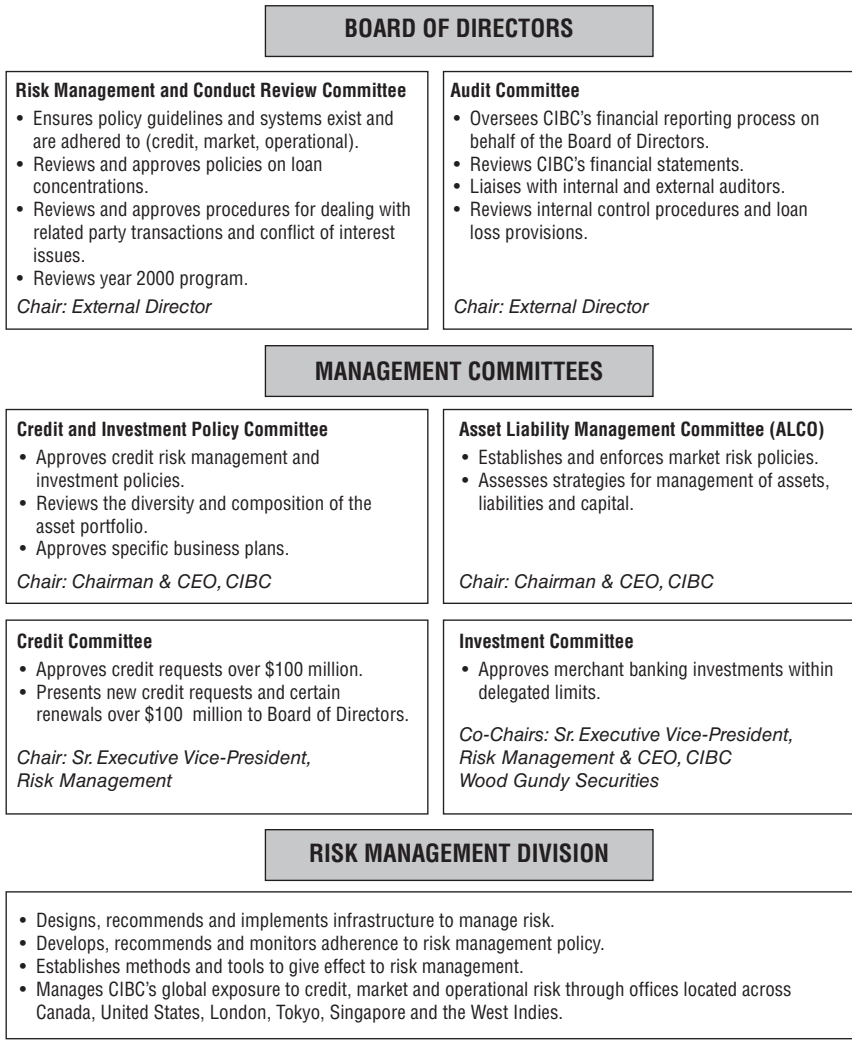


FIGURE 16.1 CIBC's Risk Management

notes Mark. By limiting business, risk management could be cutting into profitability, and individual bonuses—one reason why CIBC links compensation to risk-adjusted return performance.

CIBC has defined several objectives for its risk management program, which include reducing surprises, reducing losses consistent with risk/return objectives, reducing regulatory capital requirements, developing sophisticated risk metrics designed to capture various components of risk, and so

on. While risk information and analysis can be highly technical, they must be translated into a reporting structure that is meaningful and relevant for senior management. Mark suggests that the risk management program has succeeded in meeting those objectives.

Mark highlights the bank's reaction to the regulatory and market pressures of 1998. At the start of 1998, the Bank for International Settlements (BIS) implemented a new set of revisions to its Capital Accord—the regulatory standard used by regulators and central banks the world over. The revisions gave sophisticated banks the freedom, subject to regulatory approval, to use their own risk models as a basis for calculating the minimum required regulatory capital against market risk in the trading book (rather than a crude standardized multiplier system). It was a change that banks had long campaigned for.

When the new rules became effective at the start of 1998, CIBC was the only bank in Canada and one of the few banks in the world to receive approval for all aspects of the Accord in 1998. Mark explains: "As a bank, you'd almost have to be crazy not to take advantage of BIS 98. From the get-go, we saw that if we invested in risk management, we'd get capital relief, and the savings were huge."

Later the same year, CIBC's risk management team proved its worth in a very different way. The volatility that swept the globe during the third quarter was a test of fire for banks around the world, largely because almost every market was affected by the turmoil, but also because the early warning signs made little sense at the time. "During June and July we were seeing a lot of highly rare events that we didn't like," says Mark. "Liquidity was drying up in certain areas, correlations were diverging from their normal patterns, and credit spreads were widening." This uncertainty prompted Mark and his team of experienced risk managers, working in partnership with the business lines, to cut limits across the business by 33 percent in an attempt to mitigate exposure to volatility. Soon after the limits were cut, the markets broke. The losses sustained by CIBC were not easily digestible, but it could have been far worse. For Mark, it was a painful experience tinged with a certain amount of professional satisfaction. More than 98 percent of the losses suffered by CIBC during the 1998 market crisis were from positions which risk management had previously identified and placed on a hit-parade of the bank's top 10 risks. "We knew that if we were going to get hit that, it would be attributable to one of those exposures," says Mark.

CIBC has come up against a few challenges similar to many organizations that have faced the task of implementing integrated risk management practices. One issue is that of linking compensation to risk-adjusted performance. This is a key component of ensuring the effectiveness of each business and is a well-recognized practice at CIBC.

Another challenge to the risk management processes comes from one of CIBC's key competitive advantages—its culture. CIBC has long benefited from a culture that is decentralized, diversified, and entrepreneurial. This helps it to keep on its toes and respond quickly to the ever-changing demands of increasingly savvy customers. However, this type of culture can be difficult from an administrative perspective, and is sometimes a challenge to integrate into a system of risk reporting.

To support integrated financial risk management, CIBC has developed models for aggregating risk measures such as market VaR and credit VaR, in order to better capture the intersection between market and credit risk.

CIBC also wants to further develop an integrated and centralized method of collecting data for operational risk VaR. In addition, centralizing data collection within the next year, CIBC is also part of a global initiative to develop an operational loss database in conjunction with the Big Six Canadian banks, the British Bankers' Association (BBA), and the Risk Management Association (RMA).

CHAPTER 17

Energy Firms

The energy industry is one of the largest in the world. Energy sources are crucial to the functioning of modern economies, and global demand increased steadily during the twentieth century. The trend shows no sign of stopping: world energy consumption is forecast to grow by around 60 percent between 1997 and 2020, with most of that growth coming from the emerging markets.

Additionally, the United States, which imports about 20 percent of its energy needs at present, is projected to become close to self-sufficient by 2035 due to the rising domestic production of oil, shale gas, and bioenergy, as well as the improved efficiency of fuel transportation.[1] For example, oil production in the United States has so greatly accelerated that the United States is expected to overtake Saudi Arabia to become the largest global oil producer by the mid 2020s; U.S. production of natural gas is also set to increase substantially in this time period, which will help to contribute to self-sufficiency.[2] Simultaneously, the renewable energy market will continue to grow, increasing its market share for electricity generation from 20 percent in 2010 to 31 percent by 2035. This is an unprecedented growth track that is largely possible because of the many advancements in energy technology—for example, shale gas fracking—which we will discuss later in the chapter.

Such growth makes it even more important that energy companies manage their risks effectively, as we will see in the next section. The risks are, broadly speaking, the same as those for other corporations: strategic, business, credit, market, and operational. However, a number of factors have made energy companies more aggressive in establishing formal approaches for measuring and managing these risks, particularly market risks.

First and foremost among these is the trend toward deregulation in the natural gas and power businesses. Until the Natural Energy Act of 1978, which allowed energy prices to be determined by market forces, the energy industry was heavily regulated in most countries. This created an environment of relatively stable prices and allowed utility companies to pass any price volatility on to consumers. For example, a typical regulatory framework

would ensure that a utility selling natural gas to residential customers would realize an adequate return, regardless of how much it paid its own suppliers for the gas.

Deregulation has, however, made the industry more competitive and more subject to the vagaries of a free and open market in the relevant commodities. Consumers now have more choice when selecting an energy provider, which, in accordance with the logic of free markets, has exerted downward pressure on prices and made energy providers shoulder more of the burden when it comes to managing price volatility. Price volatility has itself increased dramatically; the early days of deregulation, in particular, were typically times of enormous volatility. While this leveled off as the market settled down, price volatility typically remains far higher than was ever the case in the tightly regulated market, and is likely to remain so. As James Rogers, CEO of Duke Energy, succinctly remarks, "Ben Franklin said there are two certainties in life: death and taxes. . . . To that, I would add the price volatility of natural gas."[3]

INDUSTRY TRENDS

The environment in which the energy industry operates suggests a dire need for enterprise risk management. In many ways, this environment is evolving in a very similar fashion to that of the financial services: deregulation has encouraged competition, leading to consolidation within industry sectors and convergence across sectors.

The 1990s saw a wave of deregulation in the energy industry, beginning in the United States, UK, and Scandinavia and moving into other countries as the decade went on. For example, the U.S. Federal Energy Regulatory Commission (FERC) has issued orders that have deregulated transmission in both the natural gas and electric power industries, with the aim of promoting price competition in these industries at both the wholesale and retail levels.

Such deregulation increases the onus on management to maximize shareholder value; if they do not, the company will not be able to attract capital sufficient to maintain or grow its operations. In the past, regulation made returns stable and predictable, and there were only minimal incentives to reduce cost. Shareholders in energy companies expected to earn stable returns while running minimal risks. As competition increased, however, earnings have become more volatile because energy companies have been forced to take on more risk—particularly price risk—instead of passing it directly to the customer. Shareholders have therefore begun to demand greater returns to compensate them for this greater risk.

This has had two major effects on the structure of the energy industry. The first is rapid consolidation, with companies merging both horizontally and vertically; the second is convergence, in that energy companies are no longer focusing on niches within the energy market, but rather have shifted to providing complete energy services for their customers. This convergence parallels the trend for one-stop shopping in financial services.

Consequently, the numerous niche players who previously populated the energy industry are giving way to a smaller number of firms that either own the entire chain in a given sector, from generation (or extraction) to delivery, or specialize in one part of the delivery chain but across a variety of sectors. An example of the first might be an oil company that owns exploration, refinery, and distribution businesses. An example of the second might be a company that delivers both gas and electricity to retail consumers. A number of energy firms have established significant trading operations, but they have retrenched since the collapse of Enron and other players in the energy trading markets. These trends pose new challenges for risk management. For instance, energy companies must now manage a wider set of risks, some of which were not typical of their former businesses. Moreover, merging two companies in different industry sub-segments often means risk management systems must be integrated; this integration must be done at an enterprise level, since the new entity is likely to have an entirely different risk profile from its separate parts. Also, there are likely to be many more ways to manage risk with respect to distribution and trading activities.

Fortunately, a larger company can make more resources available for risk management, and the evidence is that this is happening. Integration is most complete in the oil business, and most large integrated oil companies have invested substantial resources in developing their capabilities in this area. Electric and natural gas companies are likely to follow suit as these markets continue to deregulate.

As in other industries, senior management and boards of directors have become increasingly accountable for developing risk management policy and guidelines for risk tolerance levels. "The Boards of large-cap and super-cap diversified energy and utility holding companies are making risk management one of their top three priorities in 1999. This means active involvement in establishing and enforcing risk management policies. . . . For the best managed of such firms the attention is on enterprise rather than functional risk."[4] Senior management can no longer afford to delegate the risk responsibility to individual business units. In 2010, 47 percent of the respondents of a Deloitte study of the energy industry confirmed that the board led risk management efforts.[5]

However, this study also demonstrated that while 95 percent of respondents had a structured ERM framework set in place,[6] not very many

companies offer ERM training for employees outside the board room, which indicates how ERM remains in the hands of board members and senior executives.[7] As we have previously discussed, this may prove to be a barrier to full ERM integration.

The second effect of deregulation is the creation of full-fledged energy marketing and trading groups. These groups tend to be more active in the market, and thus more exposed to its risks and vagaries than their parent institutions. In many respects, they act like energy banks. A traditional bank or financial institution makes markets between buyers and sellers of financial products and risks; energy banks carry out similar functions, but with a focus on energy and related risks (such as the variability of the weather). In this regard, the value that these groups add is generated from the fact that they are making markets in energy-related exposures, managing a book of these risks, and hopefully making a spread which is, in turn, producing an adequate return based on the level of risk being taken.

Increased trading in volatile markets quickly led to an increased focus on risk management, just as it did in the financial markets. However, unlike financial services firms, where taking and managing risk was an essential part of the business' value proposition for many years, most energy companies were not nearly as comfortable with the idea of managing market risk. One answer was to adapt popular tools from the financial services industry: Value-at-Risk (VaR),[8] stress testing, and the use of limits to mitigate unwanted levels of risk.

Adapting VaR for energy companies is not a trivial task, however. The applicability of a VaR model to the energy industry is strongly affected by a number of factors unique to the energy industry; we'll examine these below. Furthermore, VaR models are not universally applicable to all of an energy company's market risk exposures, and are most useful to energy companies in the management of market making and trading activities.

VaR refers by definition to the potential loss in value of a position (or portfolio of positions) over a particular time frame (typically one day), based on a specific statistical confidence interval (usually 95 percent or 99 percent). This provides an effective measure of the potential short-term loss associated with an energy company's market-making activities.

However, energy companies, like other non-financial corporations, frequently hedge energy prices (as well as other types of market risk), to shield themselves from any impact on cash flow and earnings. VaR is of limited value when it comes to assessing these kinds of activities, and needs to be used in conjunction with other metrics, such as earnings at risk (EaR) and cash flow at risk (CFaR). For simplicity, in the rest of this chapter, we will use VaR to refer to the set of risk analytics used by an energy company.

Nor is a VaR model developed for the financial services industry of much use to an energy company in its unadapted form, even when it comes to market-making activities. A VaR model for an energy company must recognize a number of market risk issues specific to the industry; risk sharing, optionality, basis risk, and price transparency. Let's consider these in more detail.

RISK MANAGEMENT REQUIREMENTS

Thanks in part to deregulation, the volatility of energy prices can be significantly higher than the volatility of financial prices, such as those related to interest rates, foreign exchange rates, and equity prices. Figure 17.1 summarizes the findings of a 2013 CME Group study on financial, energy, and commodity price volatility from January 2010 to December 2012. The study clearly shows how price volatility is more turbulent in the energy markets than in the financial markets. Where U.S. Treasury bonds had a price volatility of 10 percent, and the S&P 500 had a price volatility of 15 percent, natural gas and crude oil had striking volatilities of 41 percent and 27 percent, respectively.[9]

These price fluctuations pose a risk to energy companies from both the buy side and the sell side. An oil refining company, for example, faces market risks from fluctuations in the price of the crude oil it buys, but also from

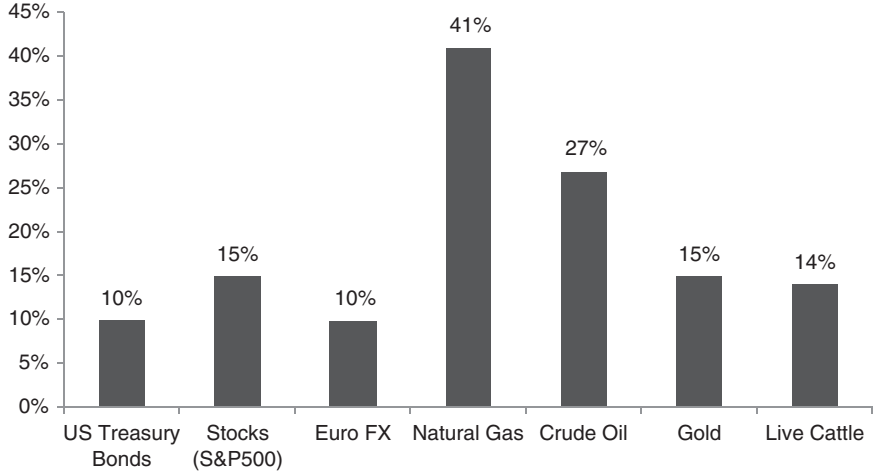


FIGURE 17.1 Annualized Price Volatility by Product/Instrument Type
Source: CME Group

fluctuations in the price of the refined products that it sells. Its profit margin is basically the difference between these two prices (the crack spread, in the jargon), and is thus doubly subject to market risk.

Some of this market risk can be hedged away; the company might hedge its crude oil needs using futures contracts. However, this leaves it exposed to the *basis risk* that the oil specified by the futures contracts will not exactly match its needs—it might be delivered to the wrong location, or at the wrong time, for example, or be of a different chemical composition. Not only does this mean that the oil may not meet the company's operational needs, it also means that the company's position is not actually neutral.

The risks do not end there. For instance, the company might also face currency risk if the crude oil is obtained from foreign sources or its products are sold in foreign markets. It also faces the risk that its suppliers or customers will default on their obligations. As is so often the case, this credit risk is intimately intertwined with market risk. As market prices increase, so does the value of a supply agreement, along with the credit risk associated with any default on that agreement.

Unsurprisingly, defaults typically occur when market conditions are least favorable and, as such, when there is most stress on the system; the result can be a succession of failures. For example, summer 1998 saw an enormous spike in electricity prices in the mid-Western United States, with prices reaching hundreds of times their normal levels. Among those who could not cope was a company called Federal Energy Sales, which defaulted on its obligations to supply power to a number of other companies. One of those, Power Company of America, was, in turn, forced to default on an estimated (and hotly disputed) $236 million of obligations to its own customers.

These price fluctuations can also be traced back to the structural inefficiencies in the energy market. For example, consider the structure of the US power grid. In the early 2000s, the United States was wracked by a series of power outages that left millions in the dark; critics blamed faulty transmission systems and the "chaotic combination of regulated and unregulated markets."[10] Since the power grids of different areas within the United States are not connected in one cohesive system, it is currently not possible to resolve a power outage by transferring energy in from elsewhere. This also affects energy prices, with the result that there can be stark divergences across the country. The increase in competition caused by deregulation may further complicate matters, as rival companies may refuse to cooperate with each other.

Today, retail energy prices are at an all-time high, with customers paying more than 43 percent more than they did in 2002. And yet, the power

grid seems to be less reliable than ever before: 349 power outages occurred between 2005 and 2009, which represents a 134 percent increase from the period between 2000 and 2004. The Electric Power Research Institute projects an estimated cost of $476 billion spread over 20 years for the development of a "nationwide smart grid"—though in the long run it would pay off and potentially save the economy trillions of dollars, we are unfortunately not likely to see the start of that industrious project anytime soon in light of today's still dismal economy.[11]

Price and Volume Risks

Business risks in energy companies take the form of pricing pressures and volume risks. Different sets of risk exposures exist at different points along the value chain, and so a given company's portfolio of risks will reflect both its sector (oil, gas, or electricity, for example) and its role in that sector (whether it is a generator, refiner, or distributor). For example, an upstream oil company involved in exploration and production will have materially different risks than a downstream oil company involved in refining and distribution. Both will be materially different than gas companies that convert oil inputs into wholesale and retail gas products.

As discussed above, energy prices are extremely volatile. Pricing pressures can occur when deregulation changes the competitive environment. Managers at natural gas companies and electric utilities have been faced with the prospect of declining prices as industry deregulation continues; they must now compete for customers and capital without the protection of the government. Moreover, energy companies have been forced to manage their volume risks, as market competition makes long-term contracts less prevalent.

To ensure the future viability of their operations in the changing competitive environment, energy companies must increasingly broaden the scope of enterprise-wide risk management to encompass all types of risks in their business and trading activities. Many industry analysts have predicted that the next two decades will be a time of unusual pressure for change, in terms of both environmental and economic reasons, in which companies will be driven to compete for survival and dominance in a new energy system.

Event and Weather Risks

Event risk losses for energy companies include extreme weather, litigation, equipment failures such as oil spills or well failures, or losses incurred by violations of company policies, that is, rogue speculative trading.

Lawsuits have become an increasing concern for energy companies over the last 20 years, particularly due to the rise in activism of environmental lobbies. For example, after the Exxon Valdez oil spill in 1989, Exxon agreed to pay approximately $1.15 billion to settle the civil and criminal cases against it, and to cover the cost of the lost oil and the ensuing cleanup. Similarly, the London-based BP oil company was fined $4.5 billion by the U.S. Department of Justice as a result of the Deepwater Horizon spill in 2010.[12]

One type of risk that is particularly relevant to energy companies is weather risk. Weather risk can impact a company by affecting credit, market, or operational risk exposures. For example, a severe heat wave can cause electric power shortages in certain markets. In this situation, it is possible that a counterparty might default on contracted electricity if the shortage is severe enough, as in the case of Power of America discussed earlier. That was an instance where a weather event directly caused a counterparty default.

Weather storms, such as Hurricanes Irene and Sandy (from the years 2011 and 2012, respectively), can severely mangle the energy industries by causing significant infrastructure damage. According to the U.S. Department of Commerce, 30 percent of the U.S. gross domestic product is directly or indirectly affected by the weather.[13] For example, Hurricane Sandy disrupted telecommunication in the Northeastern states, which caused many individuals to lose coverage and power. Hurricane Sandy also caused a steep dip in employment, with an estimated 20,000 jobs lost. As such, it is highly important for ERM programs to take into consideration the effects of weather disruption on the energy supply chain.

The year 2011 also brought an almost incomparable wave of other extreme weather conditions to the United States: the south was parched by droughts, while the north and the east drowned in torrential storms and floods. The U.S. economy was swamped by an overall loss of more than $148 billion as a result of the 2011 natural disasters.[14] While companies across the board were adversely affected by the harsh weather, those in the energy industries were dealt particularly hard blows. For example, Constellation Energy, a Texan electric power company, saw "reduced quarterly earnings of about $0.16 per share due to the record-setting 2011 heat wave" in its own home state.[15]

The electric power and oil and gas industries are particularly susceptible to damage by extreme weather. Not only can extreme weather damage infrastructure, and so hinder production, it also poses serious threats to employees. In 2005, because of two successive hurricanes (Katrina and Rita), electric power production company Entergy was forced to commit $1.5 billion to "coordinate and maintain more than 23,000 workers and relocate its New Orleans headquarters."[16]

In a study conducted in 2012, Calvert Investments recommended that electric companies consider the following factors—among others—when handling or planning for extreme weather conditions:

- Systems and processes: How does the assessment of weather conditions fit into the overall production or management framework of the company? What roles do management executives and board members play in this process?
- Extreme weather events: It would be prudent to consider the history of the company's reaction to extreme weather conditions; what was the effect on "generating capacity, production, transmission, and distribution?" How was the company impacted financially?
- Generating capacity: Putting extreme weather conditions like hurricanes and droughts aside, energy companies should also evaluate their performance under different variables such as temperature and humidity. What are their effects on the efficiency and performance of company equipment?
- Demand: Companies should take the time to analyze and understand patterns in the demand for their product. For instance, is it affected by temperature? Is it seasonal?
- Stakeholders and communities: In addition to measuring the direct impact of extreme weather conditions on the company, energy firms should also consider indirect impacts through stakeholders and communities. Note that stakeholders and communities can also be unexpected resources in times of need—which makes it even more important to maintain healthy relationships with them.[17]

Oil companies may be even more vulnerable to weather conditions, because they often operate in locations that are already off the beaten path—like in deep water or the Arctic Ocean.[18] Such areas experience extreme weather conditions often, which makes risk management of paramount importance for oil companies. For example, in 2011, the Mississippi River flooded its banks, forcing Rex Energy to "reduce its expected quarter two daily production by about 245 barrels per day for 60 days."[19] From a more long-term perspective, rising temperatures in Alaska have also hampered the oil and gas industries because the melting ice shortens exploration time and affects important infrastructure.

In addition to the factors that electric companies should address, oil and gas companies should also review the issue of what Calvert Investment deems "geopolitical risk."[20] While oil companies can be harmed by the natural world, the opposite is certainly true as well, and oil companies, among other energy industry participants, should be especially aware of their effect on the environment.

There are several ways that energy companies can benefit from using an enterprise risk management approach. Each energy company can set limits as to the amount of risk it can tolerate, measure its exposure to each risk type, and then hold sufficient capital to cover its risks at the appropriate level. Most energy companies face several if not all of the risks outlined above. An enterprise approach can comprehensively address all of the risks and their interdependencies in an energy company.

Risk Sharing

Settlement in the energy markets will often involve an exchange of both cash and the physical underlying commodity, something that is becoming increasingly uncommon in the financial markets. In some instances, these physical positions are very straightforward, which means that they are exclusively associated with the exchange of the physical commodity on some pre-arranged terms—for example, a contract to physically deliver the commodity at an agreed future date and price. In many instances, however, some of the portfolio of exposures may be embedded in an agreement between the energy producer or intermediary and their customers or suppliers. Such clauses must be quantified and factored into the overall VaR calculation.

Given that the energy industry is still at least partly regulated (and likely to remain so for some considerable time in many places), there are likely to be regulatory limits on the risks that companies can take in search of returns. There are also likely to be limits on the extent to which their customers can, in turn, be exposed to those risks. In some regulatory environments, a company may only be able to pass along a portion of any cost increase when acquiring energy supplies, and may need to pass along a portion of any savings resulting from their hedging strategy. These must also be quantified and incorporated into the VaR model.

Even if the industry does become fully deregulated, VaR models will still need to account for such limits—albeit imposed by industry practices in place of a regulator. For example, a company that passes on more risk to its customers (through price adjustments) than the industry average will likely lose customers. The first step in developing a VaR model that accurately reflects these structural elements is the assessment of the regulatory (or market) environment that affects a particular company's activities. These should then be built into the model in the form of assumptions, which accurately identify risk ownership, or the ability to pass the costs or profits of the commodity business with the ultimate consumers.

Optionality

Most energy suppliers implicitly offer some optionality in the amount of energy they provide to consumers (whether retail or commercial). They may also have complementary options to increase the supply of energy when market conditions are right. These two sets of optionality—of demand and supply, respectively—have value that must be included in the VaR calculation.

Individual consumers usually have the option to use more or less power over a given time period than the historical average. A number of factors will affect the exercise of this option, one of the most important being the weather. For example, an unusually warm summer may increase demand for air conditioning, and, as such, electricity, while an unusually warm winter may reduce the demand for gas for heating systems. The power consumption of large manufacturing companies, on the other hand, may be more reflective of the macroeconomic environment and demand for their goods.

This option has some value, which the supplier needs to consider in its pricing. In other words, the potential distribution of demand must be factored into the overall VaR framework to provide insight into an oft-ignored element of risk. The approach taken typically includes two steps:

1. Build a mathematical model for the demand as a function of various likely factors. The underlying relationship can be derived from historical data, though care must be taken in choosing a time period, geographical area, and customer breakdown that is a reasonable match for the current situation. This may require the company to build a number of models for different areas and customer segments.
2. The various forecasting models can then be used to create a distribution of potential usage. This distribution can be used in combination with the correlations of prices to determine potential shortfalls in generation capacity and/or pricing.

A company that possesses either power-generation capacity or some form of generation and/or storage capacity for the basic energy commodity (say, natural gas) is holding a physical position with inherent optionality. As with any option, this position has structural value, which can be assessed in terms of the factors generally considered in option pricing—strike price, volatility, time to maturity, and so on.

In the case of physical assets, the greatest difficulty arises in determining the strike price and time to maturity. Typically, the strike price is a function of the variable costs associated with producing power, and/or of obtaining the energy commodity from a production or storage facility.

For example, consider a company that owns both a power plant fueled by natural gas and a source of natural gas. The spread between the price of power and the price of natural gas would have to reach a certain level (the strike price) before the company would find it worthwhile to exercise its option to produce power from the natural gas, rather than simply selling the gas off in the spot market. The strike price will be determined by the cost of obtaining the natural gas, as well as the efficiency with which the plant turns it into power.

If the company owned several power plants or sources of natural gas, it might own a number of options corresponding to different combinations of plants and sources—each of these options would have to be priced individually. Furthermore, each generation asset would need to be modeled individually in order to accurately reflect potential risks. Operating characteristics that must be considered include the type of fuel, historical reliability (including both forced and scheduled outages), total operating costs, heat rates, and the marginal production and distribution costs discussed previously. These characteristics should be used to produce a distribution of the available capacity versus the total capacity for each period (e.g., hour, day, etc.), over a predefined forecast horizon. The results of this simulation will determine total capacity, as well as excess available for sale, for example, total capacity net of service load or obligated sales.

Basis Risk

In the financial markets, a security traded in one geographic market can easily be arbitraged with a similar security in another geographical market, thus eliminating pricing discrepancies. In contrast, commodities like natural gas and power cannot be arbitraged across locations so easily—for most practical purposes, a store of natural gas on the west coast of the United States is not the same thing as a store of natural gas on the east coast. Prices for the same commodity in different areas can diverge under the influence of local factors. Under these conditions, an organization that needs the commodity in one area is exposed to *basis risk* if it has to find it elsewhere.

Basis risk can be a function of several independent factors, all of which must be incorporated into VaR models. It tends to be a major consideration in markets where physical transportation of energy is not feasible; for example, in electric power, where electricity produced in the western United States cannot readily be transmitted into the eastern power grid, as we discussed earlier. Where physical transportation *is* possible, basis risk arises if an organization does not own the rights to use that transportation at a convenient time or fixed price.

Another important factor of basis risk is regional variation in weather, regulatory framework, or market environment. For example, many natural gas producers hedge their physical stocks of the gas (their natural long positions) by selling natural gas futures (acquiring short positions), in the hope that a loss in either position will be offset by gains in the other.

This strategy went badly awry in the first quarter of 1996, however. At that time, the only futures contracts available were listed at the New York Mercantile Exchange and stipulated that the gas was to be delivered at the Henry Hub, which serves the Northeast—this area was particularly affected by an exceptionally cold snap that resulted in extremely volatile prices for natural gas. Prices rose at the Henry Hub even as prices remained relatively flat in the remainder regional gas markets in the United States. The result was that natural gas producers suffered large losses on their futures positions that were not offset by corresponding gains on their national physical positions.

Many of the affected producers did have risk management policies and procedures in place, some of them quite well regarded. Still, their exposure to the weather-related basis risk between their long (physical) and short (futures) positions led them to suffer losses.

Price Transparency

One significant issue in many physical energy markets is the lack of reliable pricing information. In this case, a proxy needs to be found in the form of a similar market where pricing information is more readily available and whose long-term correlation to the target market is well known. VaR can then be approximated, though it becomes critical that stress-testing be carried out efficiently, since the correlations on which the model is based frequently break down during stressed market conditions.

Prices within commodity markets also tend to move differently than prices in capital markets, such as foreign exchange or interest rates. For example, a VaR model for energy commodities like power or natural gas should, in principle, account for the characteristics observed within the price movements of power and natural gas: price jumps, continuous price or diffusion, and mean reversion. These characteristics need to be modeled to determine the various paths of potential price movements and their range. In practice, these characteristics do not require a substantially different treatment from those in the financial markets.

A more significant difference involves the weighting of historical information. It is widely accepted that future volatility is best predicted on the basis of an exponentially weighted average of historical volatilities, since it gives more credence to recent observations than past ones, and thus

captures recent trends better than a simple average over the same period. It is therefore important that the weight and time period concerned reflect the characteristic trends of price movements, which tend to be shorter and more seasonal in the energy market than in the financial markets.

For example, analysis of recent price movements indicated that an optimal weighting factor for foreign exchange and interest rates would result in 99 percent of the volatility calculation being based on the past 151 days of historical observations, whereas it would be based on the past 42 days for natural gas markets and 23 days for power markets.

A LOOK TO THE FUTURE

In the longer-term, the most important issue facing energy companies may be the move toward new technologies and alternative energy sources, which are motivated by both environmental factors and the possibility of resource shortages. In 1997, petroleum was the most important of the various energy sources available, accounting for almost 40 percent of total energy production. Coal and natural gas followed, with 24.2 percent and 22.1 percent, respectively, while other sources (geothermal and nuclear power, for example) between them accounted for the remaining 14 percent or so.

This has changed significantly over the years. While coal remains important, the fastest growth is in the natural gas sector, driven by environmental considerations and technological advance. It looks increasingly likely that gasoline will gradually give way to natural gas and electrical power for smaller machines (most obviously, cars) while alternative energy sources such as biomass, wind, geothermal power, hydropower, solar, and nuclear will account for an increasingly large chunk of energy production. For instance, consider the fact that in 2012, coal accounted for about 37 percent of electricity production, compared to 49 percent in 2007. Conversely, our dependence on producing electricity with natural gas has risen swiftly, from 22 percent to 30 percent in the past five years.

Recent advances in technology have opened up a new energy frontier in the form of extracting shale gas through hydraulic fracturing—colloquially known as *fracking*. In the year 2000, shale gas only took up 1 percent of U.S. gas supplies, but by 2011, that number had grown to 25 percent.

So far, the rise of shale gas has worked wonders for energy prices, causing an oil and gas boom that has made—and continues to make—profound changes in the U.S. energy industry. For example, a decade ago, price levels were stagnating around $15 per million British thermal units, but today prices have been pushed all the way down to an all-time low of $4. If shale

gas production continues to expand as it has over the past decade, this pattern of extremely low gas prices is likely to persist, which is great news for consumers; this even translates to lower power prices, since shale gas produces electricity more efficiently than coal. In the late 2000s, fracking also helped to create more than 72,000 new jobs in the United States,[21] and has also brought carbon emissions to the lowest they have been since 1992.[22] Since renewable energy sources are still far from being capable of satisfying the enormous energy appetite of the United States, shale gas fracking seems to be an attractive solution.

Still, there some roadblocks to shale gas fracking that might turn what seems to be a miracle into a Pandora's box; there remains substantial ambiguity with regard to fracking's political stability. The ongoing debate about whether or not to regulate fracking is still heated, which may cause tensions within the shale gas markets that are similar to the market disturbances brought about by deregulation in the late 1990s.

While fracking gas is physically efficient and cheap, according to Jody Freeman, Harvard Law School professor and previous White House energy and climate change counselor, the environmental impact of fracking is far too great for states to monitor on their own. For example, fracking "produces significant amounts of air pollution and methane," and also "requires vast amounts of water, which can reduce regional supplies." She argues that because fracking affects the nation, the nation must set "federal minimum standards to guarantee that no state falls below a reasonable level of care."[23]

Professor Freeman also asserts that federal regulation would help to soothe public worries about shale gas. An ongoing poll conducted by the *Wall Street Journal* reveals that, as of June 3, 2013, almost a quarter of respondents do not support fracking at all—with or without government regulation.[24] Integrating what is currently an extremely haphazard and eclectic system of different agencies trying to work separately on regulation into an umbrella, national system would help to boost public confidence in the entire process of shale gas fracking. However, David Spence, a professor at the University of Texas, strongly disagrees, and instead maintains that since states are likely to be more familiar with the unique risks posed by fracking to themselves, they should be left to their own devices. He says, "States gain the most from added jobs and tax revenue; they face the truck traffic, noise, pollution risks, and rapid industrial growth."[25] He argues that the cross-state impact of the potential environmental risks of fracking are minimal, and that states are well-equipped to handle them. Government intervention would only be necessary in instances of emergencies. He points to the fact that "few, if any industries are overseen by a single federal agency," as a historical precedent that works against federal regulation.[26]

The low cost of gas today is also having an adverse effect on renewable energy efforts across the nation. Since renewable energy has never been quite as competitive as its less-clean rivals, the federal government has had to offer many incentives for private companies to continue to invest in developing renewable energy. The incomparable price advantages of shale gas have turned companies away from renewable energy, though, despite heavy government support. Internal Energy Agency (IEA) chief economist Faith Birol says that "renewable energy may be the victim of cheap gas prices if governments do not stick to their renewable support schemes."[27]

A study conducted by Massachusetts Institute of Technology demonstrates that the explosion of shale gas onto the energy scene will cause green house gas levels to rise by 13 percent by the year 2050, while simultaneously shifting resources away from renewable energy. MIT economist Henry Jacoby worries that while shale gas has many short-term benefits, "it is so attractive that it threatens other energy sources we ultimately will need."[28] The study reveals that the growth of shale gas production can potentially delay research on carbon capture and storage (CCS) which is a method of storing carbon gases underground, by around 20 years.

Jacoby also points out a fundamental weakness of shale gas production; because it is still a relatively new field of technology, there is a lot of inherent risk that we lack sufficient knowledge about. While it is true that shale gas has brought enormous benefits to the U.S. economy by slashing gas prices, it could be the case that we have yet to run into any major problems that would prove shale gas to be anything other than a much-needed miracle. Since there remains a lot of ambiguity as to the future of shale gas, there is also a lot of uncertainty as to how this period of enormous energy growth in the United States will ultimately play out in the long run.

Still, further improvements in oil-extraction techniques will likely continue to increase U.S. production of energy and independence from foreign oil sources in the future. The way companies handle this transition may result in a drastic shift in market share as some of the most successful companies are supplanted by up-and-comers who make the transition more smoothly. Given the importance of environmental issues in driving the transition process, reputational risk may prove a key issue.

Already, BP, one of the world's largest energy companies, has re-branded itself as "beyond petroleum." Energy companies that do not prove able to evolve fast enough may end up as extinct as the prehistoric life that makes up the fossil fuels they rely upon.

■ ■ ■

LESSONS LEARNED FROM ENRON

No chapter on energy risk management is complete without a few words about Enron. There are three lessons that are evident: keep your eye on the cash; manage *all*, not just some of your risks; and get auditors back to basics.

Keep Your Eye on the Cash

Prior to the restatements of its accounts, Enron reported $3.3 billion in net income over the five years ending 2000. Over the same period, it reported only $114 million of total cash generated—a mere 3 percent of reported income. A long time delay between reported earnings and actual cash flows should be a warning indicator for any company. This is especially true in financial markets and derivative businesses, where paper profits are prevalent and expected future cash flows are often counted as current revenue. If the gap cannot be closed, the company is liable to implode, as at Barings and Kidder, where reported profits were never reconciled with the cash positions of the firms. To quote one analyst: "Cash is king. Accounting is opinion." The lesson here is to focus on the cash.

Manage All of Your Risks

Ironically, Enron had a chief risk officer, who reportedly oversaw a 150-person staff, a $30 million annual budget, and a suite of market and credit risk controls that were widely believed to be state of the art. However, it was not a credit or market bet that bankrupted Enron. It was operational risk, in the form of basic failures in governance and accounting controls. There are uncanny parallels between Enron's rise and fall and those of Bankers Trust. Both companies were labeled masters of risk management in their respective industries; both ultimately met untimely ends due to soft operational risks associated with people and culture. (In the case of Bankers Trust, bad sales practices and mismanagement of client accounts broke the company's franchise as a sophisticated trading house.) Ironically, Enron's CRO, Rick Buy, was previously a Bankers Trust executive before joining Enron in 1994. The lesson here is that companies must manage all of their risks on an integrated basis, and not just the obvious ones.

Get Auditors Back to Basics

Auditors should, by no means, get the full blame for the Enron disaster. However, the profession has lost sight of one of its key roles, which is to ensure that books and records are accurate. I can't remember the last time

I met an auditor who told me that his or her main focus is to maintain the accuracy of books and records, though I meet hundreds of auditors each year who describe their roles as evaluating the effectiveness of controls and processes, helping business units perform self assessments, or providing operational risk consulting. Some of them also fail to recognize that the term internal audit outsourcing is an oxymoron. Who, when all is said and done, is minding the books? The lesson here is that the audit function should return to one of its basic and most valuable functions: to provide an independent assessment of the accuracy of a firm's books and records.

By the time the saga comes to its end, the financial losses and business repercussions of the Enron debacle could easily eclipse those of five other notorious corporate disasters—Barings, Kidder, Bankers Trust, Orange County, and Long-Term Capital Management, say. Those who wish to be wise, not foolish, in risk management should take this opportunity to learn for free what Enron and its stakeholders have learned at a very high cost indeed.

LESSONS LEARNED FROM THE BP OIL SPILL

On April 20, 2010, in what would become known as the Deepwater Horizon blowout, a pipe in an oilrig owned by energy giant BP exploded, killing 11 employees and spilling 1,000 barrels of gas daily into the surrounding Gulf of Mexico. Was this a freak accident, or had BP deliberately taken on risks that would cause and culminate in this tragic event? A series of *Wall Street Journal* studies demonstrates that BP could be held heavily accountable for the incident, in terms of both the decisions it made during the building process of the oil rig, and during the aftermath of containing the disaster.

As the *Wall Street Journal* asserts, "BP made choices over the course of the project that rendered this well more vulnerable to blowout."[29] Among the key factors that pushed the rig to collapse, the *Wall Street Journal* underlines bypassing testing procedures as among the most crucial. BP was extremely pressed for time, because it was behind schedule—and every additional day lost cost the company around $1 million. In an effort to catch up, BP skipped quality tests on the cement surrounding the pipe. Tests conducted after the spill revealed that there were serious problems in this area, which certainly contributed to the pipe's eventual bursting.

Furthermore, BP also decided to decrease the amount of time spent on applying the special drilling fluid—colloquially known as mud—to the pipe,

which would have helped to detect areas of potential breakage. While standard industry practice mandated a testing period of 6 to 12 hours, BP ran the test for just 30 minutes. There were also fundamental problems with the design of the rig itself. For example, instead of the industry standard of having two pipes—one inside the other—which would help prevent spillages, BP opted for a single pipe.

These poor building decisions may have occurred because of careless management. Robert Kaluza, the on-site manager who was overseeing these tests, was new to the job and did not have any experience with deep water drilling. While it is definitely prudent to train employees through on-the-job experience, it was less advisable of BP to leave a new manager to his own devices on such an important matter. More alarmingly, it appears that the theme of negligence had spread even further up the hierarchy, all the way to the U.S. Interior Department's Management Service, which apparently approved many of these shaky decisions because of its close ties to BP.

Without strong leadership, quality management slipped to the backs of the employees' minds, as the workforce began to think only of meeting looming deadlines. Indeed, in the wake of the spill, investigators found that a BP engineer had deleted 300 text messages evidencing that BP knew the oil flow rate was three times higher than they initially thought. As such, BP was aware of the likelihood of a spill, and yet still decided to skimp on safety measures.

This pattern of poor management was exemplified during the actual pipe explosion. Right after the initial explosion, there was chaos and confusion with respect to the chain of command: Kaluza, the commanding officer of the oil rig, was apparently "huddled on the bridge."[30] The situation was made even more difficult by the oil rig's overly complex safety procedures, which mandated that attempts to contain spillages had to be approved by two senior officers, both of whom were nowhere to be found when the explosions happened.

While BP's clumsy reaction to the explosion is certainly condemning, the overwhelming question remains: how did BP miss the early indicators of such a large failing in the rig? As a leader in the energy industry, BP uses state-of-the-art technology to perform its daily activities. However, as the *Wall Street Journal* notes, this technology "relies on the judgment and instinct of men," which introduces inherent, unavoidable weaknesses—or operational risks—into the system.[31]

It is also important to note that this is not the first time that BP has suffered the consequences of faulty workmanship. In 2006, there was an analogous incident in Alaska, but instead of learning from its mistakes there, BP continued to take on excessive risk by emphasizing cost cuts over quality.

In order to avoid future, similar disasters, BP should try to adopt a Bayesian perspective of risk management and integrate Decision Quality improvements into its ERM framework.[32] Under the Bayesian model, available data and expert judgment are combined to rigorously assess the risks involved in strategic and operational settings. A great contributor to the oil spill of 2010 was improper mitigation of operational risk; the Bayesian model will help to mitigate and monitor such risky behavior in the future.

CHAPTER 18

Non-Financial Corporations

As the twenty-first century begins, corporations from a range of industries and from around the world face unprecedented opportunities and risks. Globalization, technological advance, changing market structures, industry consolidation, intense competition, and outsourcing and re-engineering: combined with the stock market's increasing proclivity for earnings stability, these trends have placed new importance on the role of risk management.

Whereas financial institutions have long recognized risk management as a core competence in their business, non-financial corporations are beginning to realize that risk management tools can help them improve their financial performance beyond the traditional applications in hedging currency, interest rate exposures, or buying corporate insurance. Leading corporations are turning to enterprise risk management as a means of enhancing shareholder value, ensuring financial stability, and facilitating the achievement of strategic and corporate objectives.

In this chapter, we will examine the major changes affecting corporations from a wide range of sectors, such as consumer products, durable goods, high technology, pharmaceuticals, chemicals, and agriculture.

RISK MANAGEMENT REQUIREMENTS

A negative risk event incurs significant costs for a corporation. In addition to financial loss, it can damage a company's brand and customer relationships, as well as its reputation in the industry. It can also represent a strategic setback in terms of lost momentum for new businesses and products, since management time and attention is diverted to fixing the crisis.

However, while a company may die a quick death if it does not manage its critical risks, it will certainly die a slow death if it does not take enough risks. It will lose its customers if competitors introduce better service, or its competitive advantage will decline if it does not take sufficient research and development (R&D) risks and other corporations launch more innovative products.

Thus, as with financial institutions, the objective for enterprise risk management at non-financial corporations should be to optimize the company's risk profile by controlling undesirable risks and taking desirable risks. In this chapter, we'll examine the major risks faced by most corporations.

Credit Risks

Most corporations face some form of credit risk. The most common is the risk of customers defaulting on their obligations. Whether the business is a small tailor or a major car manufacturer, there is always some risk that customers will not pay in full or on time, unless payment in full is always received before services are rendered. This may be no more than a nuisance if the business rarely experiences significant credit losses, but it can jeopardize the success of the corporation if it gets out of hand.

Another credit risk that corporations face is counterparty risk—the failure of a counterparty to perform under the terms of a financial transaction, including trade finance and derivative transactions. A non-financial form of counterparty risk is the failure of a strategic partner or vendor to provide critical operations and services because of credit problems. For example, a company that uses vendors to provide critical services such as technology or order fulfillment is faced with the risk of disruptions and serious business problems if the vendors fail to perform because they are bankrupt.

Since the implications of credit losses for corporations can be wide-ranging, it is essential that executives have a clear sense of their overall credit risk, and what, if anything, should be done differently. Which accounts are questionable? How much do these questionable accounts amount to? Can corporate policy be changed to reduce credit risk without losing customers? Do we have an allowance for questionable accounts, and, if so, is it sufficient? Do we have a system in place to review accounts receivable regularly and assess their status? Are our business partners reliable? What is our back-up plan if they do not perform? Do our legal contracts protect us somewhat from credit loss? Regularly reflecting on questions such as these can help any corporation keep their credit risk exposure to an acceptable level, while not jeopardizing the growth and success of the company.

Market Risks and Hedging

Market risk involves any risk of loss due to market price fluctuations. Changes in market variables such as interest rates, foreign exchange rates, equity prices, commodity prices, and real estate prices can impact a corporation's financial positions in three ways.

First, the company has *transaction exposures* that represent the direct impact of changes in market variables on its revenues and expenses. Second, it is faced with *economic exposure* with regard to how such changes affect its competitive position, as well as buyer and supplier behavior. Finally, the company may have *translation exposures* when it converts the financial statements of foreign operations to its home currency.

These three types of exposure are frequently inter-connected, with a change in the level of one kind of exposure leading to a change in the level of some other kind. For example, a U.S.-based car company might make cars in the United States but sell them in Japan. The company would therefore face the following risks if the U.S. dollar strengthened relative to the Japanese Yen:

1. The revenues from sales in Japan will represent fewer U.S. dollars and thus the net profitability of Japanese sales will be reduced (transaction exposure);
2. The U.S. car company might be forced to raise prices in Japan, thus losing customers and market share to other car companies (economic exposure);
3. The financial statements of the company's Japan subsidiary will be translated into fewer U.S. dollars when the parent company consolidates its financial statements (translation exposure)

Stock Price Risk

One major market risk—and one that is not often considered as such—is that publicly listed companies can be very exposed to fluctuations in their *own* stock prices. When investors favor specific sectors, a company's stock price can soar, resulting in a higher market value for that company. This higher stock price acts as a stronger currency that the company can use in pursuing strategic initiatives such as business development and mergers and acquisitions.

By contrast, even a company with the strongest fundamentals can be at risk from significant devaluations in stock prices when investors are spooked. A reduction in stock price can limit a company's capital-raising opportunities as well as leaving it vulnerable to a hostile takeover. A clear and recent example of this type of stock price risk is the Internet crash of 2000, where the market meltdown for Internet stock prices and subsequent withdrawal of venture capital funding forced many dot-coms into bankruptcy and the rest to rethink their business plans.

Traditional brick-and-mortar companies are not exempt. In the current market environment, any negative surprises in corporate earnings can lead

to dramatic declines in stock price. For example, in March 2000, Procter & Gamble announced that it expected first quarter earnings to come in 11 percent lower than earnings for the same period a year earlier, sending its stock price tumbling 30 percent in one day. By the end of that week, the stock had lost 40 percent of its value and Procter & Gamble had lost $4.3 billion in market capitalization.

Investment Risks

More conventional market risks affect companies that hold investment portfolios. Most firms hold a significant portion of their available cash in fixed-income securities, a practice that exposes the firm to rising interest rates, particularly if the company has short-term liabilities and long-term assets. Furthermore, many firms take equity stakes in other companies, either in their investment portfolios or venture funds, and are therefore affected by the changes in stock prices. Finally, some firms with defined-benefit pension plans face market risk in the form of pension liability. If their pension funds are invested unwisely, a company may face a risk of being required to pay out more in pension liabilities than it holds in pension funds. This is becoming less and less of an issue as more and more firms turn to defined contribution plans, in large part to avoid this issue.

Hedging Risks

In addition to price fluctuations in the financial markets, companies are faced with uncertainties relative to their input and output prices. For example, as discussed in the previous chapter energy firms are faced with price volatility in the oil, gas, and electricity markets. Agricultural firms are affected by commodity prices. Technology firms are not only affected by the volatile prices of computer chips, but also by the costs of bandwidth for transporting data. Hedging is often used to offset some of a company's exposure to market risk, by allowing the hedger to benefit from adverse fluctuations in foreign exchange rates, for example.

Some hedging strategies, however, can be quite risky and can actually *increase* a company's exposure to market risk. For example, in April 1994, Gibson Greetings announced that it had lost $20 million on trading in derivatives for hedging purposes. Thinking that it understood the derivatives proposed to it by its banker, Bankers Trust, Gibson entered into derivatives contracts that bet on the movements of interest rates and financial indexes, but quickly found that it had bet the wrong way. Bankers Trust was ultimately found responsible for misleading Gibson Greetings and charged a $10 million fine. Gibson, meanwhile, had lost 40 percent of its share value

in less than four months—it was three and a half years before its stock regained its value of early April 1994.

In response to the high-profile derivatives losses and public outcry for improved transparency, the Financial Accounting Standards Board issued a standard, FAS 133, for accounting and reporting derivatives transactions. Many corporations claimed that this standard exposed them to significant earnings volatility by requiring them to reflect changes in the market value of derivative instruments in their income statements and balance sheets. Given these concerns, they requested that FASB amend the standard. While FASB partially met that request, and issued an amendment to FAS 133, the implementation of the new standard still poses a number of operational headaches for companies that they will have to contend with in the near future.[1]

Secondary Risks

In addition to these primary exposures to market prices, companies are also exposed to secondary price drivers. For example, temperatures can significantly affect a utility's revenues, while snowfall can affect the revenues for an airport. These secondary exposures are not strictly market risks, but share many similar characteristics, and market makers in the financial and insurance markets are fast developing new and innovative hedging products, as discussed in Chapter 9, to help companies cope with these price uncertainties. Beyond financial and commodity derivatives, these risk transfer products offer protection against price uncertainties with respect to bandwidth, temperature, and yes, even snowfall.

Operational and Insurable Risks

As outlined in an earlier chapter of this book, operational risk encompasses virtually any risk that is not a market or credit risk, and stems, broadly speaking, from potential loss due to a failure in people, processes, or technology. Operational risk is rapidly gaining acceptance as a critical risk because failures stemming from operational problems can be enormously damaging. As a result, operational risk management has been the subject of significant attention from risk managers, regulators, and the press as a critical challenge for all companies. Non-financial corporations face many forms of operational risk:

- Product liability resulting from defective products
- Failed mergers and acquisitions
- R&D underperformance risk

- Reliance on faulty financial models
- Changes in tax laws and regulations

Additionally, operational risk encompasses organizational and technology risks. Organizational risks include shortages in management talent and skilled labor, negative PR, or improper employee behavior due to poor hiring practices and/or adverse corporate culture and incentives. Technology risks include systems outages from older systems or untested applications, inadequate or faulty data, and information security breaches.

Catastrophic Failures

Examples of operational risk management failures, and their potentially catastrophic consequences, abound. One of the best-known examples is the 1984 chemical leak from a Union Carbide plant in Bhopal, India. In December 1984, a Union Carbide pesticide plant in Bhopal, India, was the site of what was then called the "world's worst industrial accident" in history.[2] A tank in the plant leaked five tons of poisonous methyl isocyanate gas into the air, killing more than 3,000 people and injuring tens of thousands. The Indian government successfully sued Union Carbide for $470 million in 1989, and criminal proceedings are still outstanding.

Another very high-profile example of an operational failure occurred when, in 1989, the cargo tanks of Exxon's oil tanker, the Exxon Valdez, ruptured when the ship ran aground off the coast of Alaska, spilling more than 10.8 million gallons of crude oil into the ocean. Exxon spent $3 billion to clean up and to settle government lawsuits, and, in 1994, was ordered to pay $5 billion in punitive damages to those harmed by the spill, an order that it contested publicly. The Valdez spill and Exxon's subsequent actions have damaged Exxon's reputation as a good corporate citizen. In fact, Exxon's corporate reputation reportedly led regulators to scrutinize Exxon's proposed 1999 merger with Mobil Oil more heavily than the similar merger between BP and Amoco, despite the fact that the latter posed more antitrust concerns. Exxon's opposition to the 1994 judgment in the Valdez spill caused it to be "known in the industry for never yielding an inch with legal opponents, including regulators."[3]

Business Risk

Adopting the wrong business strategy, or failing to execute the right strategy can also be considered a form of operational risk. Because a company's strategy is of paramount importance to its success, strategic uncertainties such as business plan assumptions, competitor responses, and technology

changes should be measured and managed along with any other risk management issue. In a rapidly changing business environment, even a company with a well-thought-out strategy must establish feedback mechanisms and contingency plans to ensure that the company's strategy is sound over time.

As history has shown with the railroads when automobiles were invented, or with large cars when gas prices escalated, companies with unbending strategies can face extinction. A more recent example would be Olivetti, which was one of the leading manufacturers of typewriters heading into the 1980s. Olivetti believed so firmly that the typewriter would always be commonly used that it did not follow other companies' lead and start to manufacture personal computers. Thus, it nearly lost everything by not recognizing the need to change strategy to focus on new technologies.

In another recent example, Boeing and Airbus have each bet the futures of their companies on their vision of the future of air travel. At issue is the question of whether the air travel industry requires a new super jumbo jet to fly passengers between major international hubs. Boeing believes that point-to-point service will be more important than travel through hubs in the future, necessitating smaller planes. Airbus, however, thinks that a super-jumbo jet with dramatically increased capacity will be greatly in demand, to satisfy the ever-increasing international appetite for air travel. Given the cost of developing new models of aircraft, these alternatives are, for most purposes, mutually exclusive—each company must pick the strategy it believes to be correct. Whichever turns out to be correct will stand to gain market share on the other's back and avoid potentially devastating losses from development costs. For the company that chooses incorrectly, the development costs and loss of businesses could be their undoing.[4]

Today, the battle between these two behemoths for control over the sky continues, in the arena of the "mini-jumbo"—"a twin-engine plane capable of going distances similar to that of a four-engine plane."[5] Both companies have their own prize products—Boeing touts the 777X series, while Airbus champions the A350–1000. While these planes are both categorized as mini-jumbos, the differences in their specifications imply the subtle disparities in the attitudes of the companies that make them. For example, Boeing's 777X planes will have a metal body and carbon fiber wings, while Airbus's A350–1000 is mostly made out of carbon fiber. Boeing believes that a "metal fuselage will increase performance but maintain reliability," while Airbus affirms that a lighter plane made out of carbon fiber will be cheaper to run, and as such, generate higher profits.[6]

It is still too early in the game to say which company will come out on top—though recently, British Airways, supposedly a loyal Boeing customer, ordered $6 billion worth of Airbus's 777X planes, which will no doubt prove to be a blow for Boeing. Still, Boeing has recently won a partnership

with General Electric, so by no means are they out of the race. Once again, only time will tell who the true winner is.

Cultural Risks

The wrong culture can also be a form of operational risk. IBM is a classic example of a company whose culture turned from a strength to a weakness, ultimately posing a significant risk to its success. During the 1980s, IBM fiercely maintained a culture that was described by others as "bureaucracy run amok"[7]—epitomized by the nickname Big Blue—while all around it the high technology sector developed a culture of golf-shirt-sporting executives leading organizations with flat hierarchies. IBM's "caution, obsessive training of employees, focus on following rather than anticipating customer needs, and a guarantee of lifetime employment to its workers" made it inflexible and were integral to its decision to focus on mainframes rather than personal computers in the late 1970s. That decision nearly cost the company its business. IBM went from earning a $6 billion profit in the early 1990s to a $5 billion loss just two years later; its stock price fell from $176 to the low $40s. Since that time, IBM has rebounded to a highly successful company that generates more than $16 billion in annual profit with a market value exceeding $200 billion. The turnaround is based on a dramatic shift in its corporate culture and business model from a computer hardware and software company to a global business services firm.

Pension Risks

Pension liability has increased greatly in the past decade. For instance, Milliman Inc. found that "the 100 largest defined-benefit corporate pension plans were underfunded by $453 billion at the end of September of 2012, a 30 percent increase from a year earlier."[8]

There are several important factors that have transformed pension funds into the capital-devouring black holes they are today, but the hardest-hitting blow has been the downward shift in the interest rate. The Federal Reserve has been keeping interest rates extremely low, and will continue to do so until 2015—and potentially beyond. For pension funds, this is bad news, because lower interest rates limit investment returns, and also reduce the discount rate that companies use to calculate the present value of future pension liabilities. Hence, lower interest rates translate into higher pension liability.[9]

Michael Moran, a pension strategist at Goldman Sachs, notes that in an effort to curb these growing liabilities, some pension plan sponsors have turned to lump sum options in order to minimize their pension liabilities.

Other sponsors have entered into annuity contracts with insurance providers in order to move liabilities off their books. He also observes that such actions have resulted in a general trend toward liability-driven investing across the board. He explains that pension plan liabilities are based on high-quality corporate bond interest rates, so investing in high-quality fixed-income securities in turn can help companies balance their assets with their liabilities.[10]

Outsourcing

With competition increasing in intensity every day, outsourcing—defined as the utilization of third parties to complete tasks that are normally performed internally—is quickly becoming an industry standard: 60 percent of survey respondents in a study conducted by Deloitte in 2012 stated that outsourcing was a standard practice at their respective companies.[11] There are many obvious advantages to outsourcing, which explains its popularity. For example, outsourcing gives a firm access to resources that would otherwise need to be acquired, or be unavailable, which greatly increases its business capacity. Furthermore, outsourcing can help to improve company focus by allowing the firm to concentrate on the tasks that can only be performed internally. It can also help firms diversify risk, reduce market entry times, and reduce operation costs, among numerous other benefits.

A study conducted by the Basel Committee on Banking Supervision in 2005 revealed that information technology (IT)-related services were the most popular kind of service to outsource. Of the "$340 billion spent on IT globally in 2003 . . . a third was entrusted to third parties."[12] Today, 76 percent of companies outsource IT services, while 81 percent predict future increases in IT outsourcing, acknowledging the fact that this movement increases efficiency and savings. Notably, cloud computing is on the rise, with 30 percent of companies using cloud services for essential company functions, such as emailing, web site hosting, telephony systems, and front-, middle-, and back-office systems.

While IT outsourcing demonstrates how outsourcing can increase a company's profitability, it also exemplifies how outsourcing can magnify the amount of risk a company takes on. When risk is transferred offshore—for example, through IT outsourcing—companies lose control over how these risks are monitored and regulated. ERM programs should be designed to take overseas risk management into consideration. For example, while Toyota, which uses U.S. suppliers, is flourishing in the auto industry, Boeing has run into a stream of problems with the foreign-made parts of its carrier, the 787 Dreamliner.[13] By moving production out of the United States, Boeing could not examine and streamline these processes, with the ultimate result of lower quality standards and shoddy craftsmanship.

To minimize the size of these kinds of risks, companies should always maintain strong, transparent, and mutually trusting relationships with their third-party partners. Steve Durbin, vice president of the Information Security Forum, says that "companies should do significant research on the outside company's security systems. . . . You really need to kick the tires" before embarking on an outsourcing venture.[14]

Reputational Risks

One of the most valuable assets a company can have is its reputation. One measure of a company's reputation is its brand or trademark value. In June 1999, Coca-Cola was considered the world's most valuable brand, with a trademark value estimated at $83.8 billion; nearly 60 percent of the company's market value.[15] However, that brand value and the company's reputation were seriously jeopardized when more than 100 people fell ill after drinking Coca-Cola products in June 1999. Coca-Cola products were subsequently banned by a number of European governments, including those of Belgium, France, Greece, Spain and Italy, forcing the largest product recall in the company's 113-year history.[16] Coca-Cola reported that the impact of the European recall cost shareholders two to three cents of second-quarter earnings because of a "loss of sales in several markets, a fall in equity income, and increased marketing expenses."[17] Coca-Cola Enterprises (one of Coke's bottlers) alone estimated that the recall would cost them $60 million (U.S.).[18] Furthermore, Coke's stock price lost nearly 13 percent of its value in one month, falling from $70 to $61 and eroding more than $22 billion in market capitalization.[19]

BEST PRACTICES IN CORPORATE RISK MANAGEMENT

As discussed above, corporations are faced with a wide range of strategic, business, credit, market, and operational risks. To mitigate these risks, management can develop governance structures, risk measurement and management processes, and risk transfer strategies. The overall risk management process for corporations include risk identification and assessment; quantification and reporting; and management and control. Let's look at each of these in turn.

Risk Identification and Assessment

One risk identification methodology made popular by corporations is the use of risk mapping. Today, risk mapping is increasingly used by both financial and non-financial companies to identify and monitor enterprise-wide risks.

Figure 18.1 shows an example of a risk map, which ranks risk exposures by severity on the horizontal axis and by probability on the vertical axis (see Chapter 3 for a discussion of these concepts). The process of developing and implementing a risk map is as follows:

1. Establish a top-down framework—an overall taxonomy for classifying all types of risk
2. Create a bottom-up list of specific risks by business and functional units, based on loss history and self assessments
3. Evaluate the probability and severity of each risk based on management judgment and/or risk models, and develop the risk map as shown in Figure 18.1
4. Identify existing controls to incorporate their impact and determine whether new controls are needed at the business and functional levels
5. Assign responsibilities for implementing new controls as well as for monitoring and reporting on specific risks
6. Aggregate individual risk maps into an enterprise-level risk map, and determine whether new controls are needed at the enterprise level
7. Go back to step 1 in order to update and refine the risk mapping process on an ongoing basis

Very few companies face many risks that are both highly severe and highly probable. One rare example is that of Internet companies that are projected to run out of cash within, say, 12 months. For these companies, the probability of depleting their cash positions is high, given their burn rate, and the consequence of such an event—bankruptcy—is the most severe

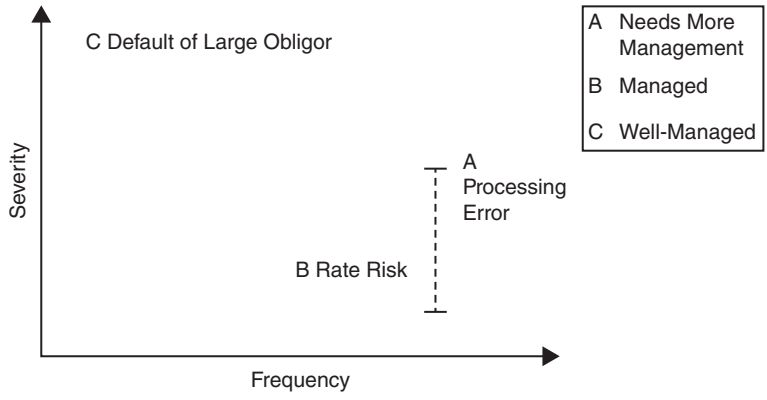


FIGURE 18.1 Risk Map

that can be faced by any company. Such exposures warrant significant management attention and the active deployment of risk mitigation plans. For the Internet companies, cash management is a critical activity and the ability to raise additional funds often means life or death for the company.

On the other hand, all companies face risks that are of both low severity and low probability. For example, it is unlikely that a company would experience a malfunction in its voice mail system. Such an occurrence should in any case have little impact on its business and financial performance (unless, of course, it is a company that makes voice mail systems). Risks that are considered low probability and low severity should simply be monitored to ensure that they remain in an acceptable range. Such risks are often only important if they recur: the cumulative impact of many, repeating small risk events may be much more significant than that of a single risk event. For example, many investment banks have a high error rate in the settlement of financial transactions. The focus of attention for these banks has not been to achieve a zero error rate, but to make sure that any such errors are within an acceptable range and that they are resolved in a timely manner.

Risk exposures that are of high severity but low probability are excellent candidates for contingency plans and/or insurance policies. Examples include events such as fire, earthquake, or other natural or business catastrophes. Finally, risks that are of low severity but high probability may include minor theft, machinery breakdown, and expected levels of receivables charge-offs. These exposures are generally self-insured by a company. Some exposures, such as interest rate risk, currency risk, credit risk, employee turnover, and product liability may range in probability and severity depending on the company's specific exposures and the actual volatility. For these exposures, management should establish effective monitoring and reporting systems, including early warning indicators that would signal problems ahead.

Risk mapping has become a widely used risk identification and assessment tool because of its flexibility to incorporate both financial and nonfinancial risks. Given its flexibility, the risk mapping process should exhibit the following qualities:

- Comprehensive: The risk map represents an overall framework for identifying and assessing all of the risks faced by the corporation.
- Consistency: A standard taxonomy establishes a common language to discuss risk exposures, and the standards for risk assessment provide a consistent methodology for evaluating their probability and severity.
- Accountability: Business and functional units are directly involved in the identification and assessment of risks, as well as in the risk monitoring and management processes.

If implemented appropriately, the risk map can be a highly effective tool for risk identification and assessment. However, the quality of a risk map is entirely dependent on the quality of the input and process that produced it. Without a sound methodology, risk mapping can become a bureaucratic exercise that yields little benefit other than a hodge podge of risk exposures that are not well thought out.

A misuse of the risk mapping process would be to gather a group of business and functional managers, brainstorm about risk exposures without a standard taxonomy, arbitrarily assign probability and severity without a methodology, and then create a risk map that will not be looked at until the following year. Such an approach might create risk awareness for certain issues, but is by no means a disciplined risk identification and assessment process. For a risk mapping process to be effective, it should follow the steps discussed above and be supported by risk quantification and reporting, as discussed in the next section.

Quantification and Reporting

Non-financial corporations should benefit from the risk quantification and reporting processes discussed in the rest of the book. In this section we will discuss how corporations can apply value-at-risk techniques to quantify and manage cash flow and earnings volatility, as well as make the appropriate risk adjustments in EVA and NPV models.

As described in Chapter 9, Value-at-Risk (VaR) is a summary statistic that quantifies the potential decline in asset or portfolio value given an adverse market price change over a specified period. For example, the VaR for a bond or bond portfolio can be calculated based on a 99 percent confidence level over a 10-day period. Such a number would indicate that, based on historical data, there is only a 1 percent probability that the company would suffer a value decline greater than the calculated VaR over any 10-day period.

VaR has become an industry standard for risk quantification and control for many companies, especially those involved in trading capital markets instruments such as financial institutions, energy firms, and non-financial corporations with significant capital markets activities. For these companies, VaR has been used to quantify risk exposures across financial risk positions as well as to establish trading limits. For financial institutions, which are increasingly managing their overall balance sheets on a mark-to-market basis, VaR represents an effective and concise tool for quantifying and reporting enterprise-wide risk exposures.

However, that is not the case for most non-financial corporations, because these companies use accrual accounting. Moreover, the financial and

risk management objectives of corporations are focused more on cash flow and earnings management, and not on the market value of its assets and liabilities. As such, corporations have applied VaR techniques to measure and manage cash-flow-at-risk (CFaR) and earnings-at-risk (EaR). The objectives of CFaR and EaR are to quantify and control the key variables that contribute to the volatility in the cash flows and earnings of the company, respectively. Corporations can use one or more of three general approaches to estimating CFaR and EaR:

1. Pro Forma Analysis

   This analytical approach is based on a pro forma analysis for each item on the cash flow and income statements. The starting point is the company's financial forecast, which provides a base case number for each item. A risk analyst then determines the key variables that might affect the outcome of each item and the potential range of these variables. For example, the risk analyst might determine that the dollar/yen exchange rate is a key variable for revenues; the use of contract labor might have significant influence on expenses; and receivables turnover is a key driver of cash inflows. Next, the risk analyst would establish a range for each of these variables and estimate the sensitivity of the cash flow and income items to these variables. An adverse change in the dollar/yen exchange rate might be 15 percent, translating into a 30 percent decline in earnings. Based on such an analysis, the full impact of specified changes in key risk variables to the company's overall cash and earnings positions would be quantified under various scenarios.
2. Regression Analysis

   The regression method quantifies the exposure of the company's cash flows and earnings to various risk factors on the basis of time series analysis of the company's prior performance and historical data. The purpose of the analysis is to use historical data on the company's cash flows and earnings, as well as key variables—such as interest rates, exchange rates, or worker's compensation—to determine the beta coefficients for each variable. These beta coefficients measure the company's sensitivity to each variable. For example, a 0.5 beta for interest rates would indicate that a 10 percent increase in interest rates would lead to a 5 percent decline in earnings. Other statistical tests can be used to measure the accuracy of the model and the significance of each variable.

   The regression model provides a linear estimate of the company's cash flows and earnings given a set of assumptions about the key variables. As such, management can quantify CFaR and EaR using a range of assumptions for the variables. The advantages of using the regression method are that it is a fact-based analysis using historical data, and

can be updated regularly given new data. The disadvantages include the inherent assumption that the future will be like the past, and that non-linear relationships between the variables and the company's cash flows and earnings will not be accurately captured.

3. Simulation Analysis

   The simulation approach quantifies potential changes to the company's cash flows and earnings on the basis of computer-simulated changes in key variables. The key advantage of simulation analysis is that it can incorporate dynamic changes in the external environment, as well as internal management decisions. This allows the simulation method to quantify risk exposures that are time and path dependent.

   For example, the company's interest expense sensitivity in the second year might be dependent on the first year's issuance of fixed versus floating debt, which in turn is dependent on the level of interest rates in the first year. A simulation model can be programmed to incorporate these relationships, given the potential changes and path of interest rates. An advanced form of simulation analysis is Monte Carlo simulation, in which the future distributions of interest rates and other variables are determined by random simulation of the values, volatilities, and correlations between these variables. The flexibility of the simulation approach allows management to evaluate the impact of competitive responses. For example, a pharmaceutical company facing the expiration of a key drug patent might want to evaluate the impact of various pricing strategies, including the likely responses from competitors with respect to their product and pricing strategies.

A corporation does not have to choose one of these three methods to the exclusion of the other two. It can select a specific method for specific business applications. For example, a corporation may use the simulation method for risk management, *pro forma* analysis for business and financial planning, and regression analysis for back testing. The key is to effectively quantify and report on the company's risk exposures in order to reinforce risk identification and assessment, as well as support risk management and control.

Beyond risk measurement, the quantification of a corporation's risk exposures should provide management with analysis of its capital adequacy. A corporation holds equity capital for two main reasons: to fund cash and investment requirements and to absorb unexpected losses. Greater quantification is useful in both these areas, and in particular the concept of economic capital—the capital held against risk (as explained in more detail in Chapter 9). If the economic capital is greater than the actual book capital of the company, the company is undercapitalized for the risks embedded in the business, and vice versa. Besides assessing the overall capital adequacy of

the company, economic capital can be allocated to individual business units, products, or investments in order to evaluate risk-adjusted profitability on a consistent basis.

Many corporations use net present value (NPV) and economic value added (EVA) tools to support investment decisions and business performance measurement. However, many of these applications allocate book capital or an average cost of capital to business activities, without fully adjusting for their risks. If the capital charge in these NPV and EVA applications does not fully reflect the underlying credit, market, and operational risks, then higher-risk investments and businesses would appear to be more profitable than the lower-risk ones. Over time, this would result in adverse selection—in other words, the business portfolio would have higher risk exposures but not the higher returns that would compensate for such risks. To ensure the appropriate risk/return linkage, corporations should either adopt the economic capital methodology or make specific risk adjustments in their NPV and EVA tools.

Management And Control

The risk management process does not end with risk identification and assessment, or risk quantification and reporting. The final step is risk management and control. In this section, we'll highlight some of the key risk management and control strategies that corporations can implement. Generally speaking, corporations are paid to take strategic and business risks, manage financial risks, and mitigate operational risks. Based on the risk assessment and quantification of these risks, management can then decide on the appropriate strategies, including internal control and external risk transfer.

A company's management should start by establishing clear criteria for business' acceptance of strategic and tactical risks and instituting ongoing processes for the monitoring of risks (see discussion of Policy 6.0 at GE Capital in Chapter 6). Beyond these, there are other strategic options that can provide the company with valuable flexibility. These include service-level agreements with vendors that specify performance standards with penalty and exit clauses, as well as provisions that allow the delay or extension of projects. The company can further optimize its business risk by diversifying business and product lines, staging R&D projects, and shortening time to market for new project launches. Management can also reduce profit margin volatility by reducing the operating leverage of the company (i.e., reduce fixed versus controllable expenses).

To reduce market and credit risk exposure concentrations, management can implement risk management policies and limits, as well as utilize internal and external hedging. Internal hedges for corporations include matching

foreign revenues and expenses by sourcing supplies and locating plants abroad, or matching the interest rate adjustments of financial assets and liabilities. External hedging would involve financial derivatives such as swaps, options, and futures contracts. The cost-benefit analysis between internal and external hedging should include hedging costs, administrative costs, and any residual basis risks associated with these alternatives.

Management should mitigate operational risks by developing quality-control procedures for high frequency but low-to-medium severity risk exposures, such as manufacturing defects. A corporation can also establish contingency plans and insurance strategies to mitigate event risks (low frequency but high severity) such as fire, earthquake, or a major systems outage. To mitigate risks associated with process or technology, single points of failures (also known as SPOFs) should be identified and redundant back-up processes and systems should be developed. For critical operations such as customer service and core systems, excess capacity may be appropriate.

Non-financial corporations face many of the same pressures to improve enterprise risk management as do their counterparts in the financial services and energy industries—namely a dynamic business environment, an unforgiving stock market, industry mandates on corporate governance, and changes in regulatory and accounting requirements (e.g., FAS 133). Many corporations, in particularly those with significant foreign operations and capital markets activities, have invested in the people, process, and technology for enterprise risk management. The case study below on Microsoft is a case in point.

CASE STUDY: MICROSOFT

Microsoft Corporation, the American software giant, began to implement its enterprise risk management program in 1994 and 1995. Scott Lange, the director of risk management at the time, started by developing a comprehensive list of the risks faced by the company and sorting them into a dozen broad categories: financial, reputational, technological, competitive, customer, people, operations, distribution, business partners, regulatory and legislative, political, and strategic.[20] "For the first time, management had a complete inventory of the organization's risk," said Lange. That helped them to recognize early on that their risk financing program, although "well-conceived and tremendously efficient," only covered about 30 percent of the risks the company faced.[21]

The recognition of the fact that much of Microsoft's risk exposure was not covered and the need to communicate that to senior management led Mr. Lange and his colleague, Jean-Francois Heitz, Microsoft's treasurer, to

develop an innovative communication tool: risk maps. The risk management map plots each risk's severity on the vertical axis and its frequency on the horizontal to show management easily what their risk picture looks like. The map then uses a color-coding system to indicate whether the risk is insured, partially insured, or uninsured, helping Microsoft to best decide where to allocate its risk management resources. Obviously, uninsured risks that are high in frequency and severity demand more attention than ones that occur infrequently or are of small impact. According to Mr. Lange, the maps revealed at least two things. "One, Microsoft had a lot of risks that needed to be actively managed. Two, there was little consistency as to why some risks were insured and others weren't."[22]

In order to help direct Microsoft management's efforts to address those risks that were not being actively managed, Mr. Lange and Mr. Heitz used a risk grid. The grid outlines in a readily understood format the risk management process for any given risk. It is a simple matrix with what Microsoft considers the five main elements of the risk management process (identification, assessment, mitigation, financing, and services) as the first column. The next three columns are labeled current, goal, and action required, and indicate, respectively, the current process for managing that risk, the ideal process, and what actions are required to move toward the goal. This tool is applicable to all risk types, and is easily used and understood by management throughout Microsoft, further enabling Microsoft to achieve its goal of enterprise risk management.

The process of going through this analysis helped Microsoft to realize that it had insurance policies with coverage or limits that were too small to be meaningful to their business, and the company was able to save premiums by discontinuing the policies or increasing the limits. Furthermore, risk analysis helped them to identify a risk of possible tort litigation for repetitive stress injuries that might arise from the release of a new keyboard. They determined the potential cost of repetitive stress injury suits and built that cost into the price of their keyboards, helping to mitigate the risk of future losses in that area.[23]

For the future, Microsoft wants to continue to manage its risks holistically, and may participate in the trend toward holistic risk transference. "Ultimately, we may package together our disparate risks and take it to market, if that makes the most sense for us," says Richard Sadler, Microsoft's current senior risk manager.[24]

Another of Microsoft's innovative approaches to enterprise risk management is its use of information technology as a risk management tool. Microsoft's risk managers recognized early on that they would have to make risk management an easy process for employees in order to maximize their compliance with risk management procedures, so as not to take their time

away from customer service. Thus, Mr. Lange realized that they "had to advance a strategy of mixing technology and outsourcing to free up the human horsepower [they] needed to get the job done."[25] So, they set up risk management information systems that track data on historical losses, both as a record and as the foundation for risk analysis in the future.

Next, they built an Intranet that all Microsoft employees can access to "communicate everything from A to Z that is happening in risk management."[26] The Intranet aims to integrate all Microsoft units' understanding of their risks and to give business units ready access to any information they might need concerning risks related to their businesses or business decisions.[27] Also, it helps to free up employee time by automating many repetitive tasks, such as loss claims. It enables employees to refine their needs so that risk management staff can provide focused and value-added information and services.

Microsoft's use of the Intranet for risk management has strong buy in from senior management, too. In the words of Mike Brown, Microsoft's CFO, "If you are a risk manager, the web is an incredible opportunity to take costs out of your model, to provide higher quality services, and to be much more informed about company issues. If I could pick one item in our risk program that really turns me on, it's the continual improvements in using on-line technology."[28]

CASE STUDY: FORD

While other firms were floundering and drowning during the financial crisis of 2008 and its aftermath, Ford remained steadfast, and flourishes today. Just recently, in 2011, the company issued bonuses to its employees of up to $5,000—the largest in a decade. What is the secret to its success?

It is true that Ford had mortgaged its assets in 2006, so that by the time the financial crisis hit and cash was quickly in short supply, it was already highly liquid. However, the special ingredient that cemented Ford's fortitude was actually William Clay Ford's decision to relinquish the CEO position to an external expert, Alan Mulally, former executive vice president of Boeing. Considered in terms of risk management, this was a spectacular move, because, as it turned out, "Mulally led . . . Ford back to profitability without the federal bailouts and bankruptcies" that plagued other automobile makers during the financial crisis.[29] Ford did not have to take any of the double-edged TARP money from the government in 2008, and nor did it need to declare bankruptcy (like top competitors General Motors and Chrysler had to).

With Mulally at the reins, Ford shed off "boutique brands like Jaguar and Volvo" in order to concentrate on perfecting its core products.[30]

Ford strengthened itself with new car models—the Focus and the Taurus—to boost sales revenues. Before it launched these two cars, Ford faced crippling sales losses: "Ford's traditional specialty of pick-up trucks and sports utility vehicles . . . left it particularly exposed" in a contracting economy where consumers were looking for fuel-efficient vehicles.[31] The Focus and the Taurus speedily closed the gap between Ford's products and current customer needs.

Today, Mulally is guiding Ford to a new market in China. Despite the fact that Ford entered China much later than GM and Volkswagen, it is making steady progress, beating Japanese rivals with a hefty 54 percent increase in sales over the last year.

Mulally's sharp decision-making exemplifies the spirit of meticulousness and hard work that permeates the entire company. Ford's engineers are paragons of ingenuity, and hold Ford in their minds even outside of the workplace. For example, engineer Todd Brown came up with the revolutionary idea of "curve control" (which automatically cuts vehicle speed in the case of reckless curve driving) while he was eating at a restaurant.[32]

Thinking in terms of risk management, this demonstrates how ERM was—and is—at the forefront of all decision-making at Ford. In a nutshell, Ford was able to withstand the trials of the 2008 financial crisis because it remained true to the spirit of the company, while others struggled with the turbulence of the markets.

CASE STUDY: AIRBUS AND BOEING

In recent years, both Airbus and Boeing—leaders of the airplane industry and fierce rivals—have struggled with maintaining their budgets and remaining on schedule when project after expensive project fell through. For example, in 2009, Airbus incurred a loss of $1.82 billion and also had to push back Malaysian Airline's order of the Airbus A380, which was due in 2010, by a full two years. Both companies have been using the profits from their smaller planes—which have been selling strongly—to fuel the sinkholes created by their new, larger ventures.

Desperate to keep frustrated customers happy, the two competing companies have redesigned their approaches to building jetliners. In the early 2000s, Airbus and Boeing relied so much on external contractors to build their aircrafts that they lost control of their projects; Boeing had more than 40 faulty Dreamliner planes rusting in its inventories as a result of the slew of manufacturing issues. Former Boeing Executive Vice President, Jim Albaugh, remembers how the company "didn't provide the kind of oversight necessary for some of the people that were doing work that they'd never done before."[33]

While neither company has cut back significantly on outsourcing, today, Airbus and Boeing do keep a tighter grasp on their outsourcing practices, working closely with external suppliers to ensure that everyone is operating on the same platform—using the same designs, the same technology, and visualizing the same overarching plan. Didier Evrard, leader of the Airbus A350 project, even re-organized the internal structure of the company by forcing plants in rival countries, such as Germany and Spain, to operate using the same standards and equipment. With increased awareness and control over both internal and external processes, Airbus and Boeing have streamlined their production processes. As Thierry Larroque, a senior executive member of Airbus, says, "We don't know everything, but know all about the risky ones."[34]

While these new operating processes have helped Airbus and Boeing cut back on their costs by reducing the chance of expensive mistakes, they do not address the fundamental risks of the airline business. For example, design and implementation in the plane production industry can be years in the making, which saddles companies in this industry with substantial, seemingly unavoidable risk. Once committed to a project, they have no choice but to ride it out for a decade or more—for better or for worse.

Airbus CFO, Hans Peter Ring, noted how "[Airbus] must now do a better job of putting a price tag on the risks inherent in their airplane programs."[35] His acknowledgement of this weakness indicates signs of healthy self assessment within the company. While this will not guarantee that Airbus will become more efficient at risk-based pricing, that they are aware of their failings bodes well for future development. The fact that Ring openly stated this at all also marks a significant recognition of the importance of fully incorporating the cost of risk into product pricing.

SECTION

Four

A Look to the Future

CHAPTER 19

Predictions

We began this book by discussing the concepts and processes for risk management and made the case for an integrated enterprise-wide approach. We discussed the general principles of this *enterprise risk management* (ERM) and then investigated the components of a well-founded ERM framework. Next, we reviewed the applications of ERM in the three key functional areas—credit, market, and operational—as well as specific industry sectors, including financial, energy, and non-financial corporations.

Throughout this book, from the title to the individual chapters, I have emphasized the importance of taking a balanced approach to enterprise risk management. One facet of this is balancing control over the downside (loss minimization) with support for the upside (shareholder value maximization). Another is the need to strike a balance between weighing internal controls over risk (policies, functions, and processes) with external risk transfer mechanisms (derivatives, insurance, and alternative risk transfer).

A final aspect of balance in risk management, and perhaps the one that will prove most critical in moving away from silo risk management toward ERM, is the need to always consider both the yang or hard side of risk management (systems, reports, limits) and the yin or soft side (culture, people, skills, and incentives). In the spirit of yin and yang, we'll take a summary look at the major drivers of change at the human and technological levels: the emergence of risk management as a professional discipline, and the way that technology supports many levels of convergence toward enterprise risk management. As we'll see, both starting positions ultimately lead to a point when the two overlap and intertwine—just like yin and yang.

I'll close this section by bravely making 10 predictions for risk management over the next decade. Those of you who want to take a (fictional) glimpse of what the future might look like are invited to read the following chapter, in which the travails of Pamela, a risk manager in the year 2010, are described.

THE PROFESSION OF RISK MANAGEMENT

As the practice of risk management has expanded from a silo approach to an ERM approach, so has the career path for risk professionals. In the past, risk professionals were defined by a specialization: actuary, auditor, credit analyst, asset/liability manager, market risk manager, and so on. These roles were largely independent of each other, with significant differences in their educational and training programs, professional qualifications and certifications, work practices and terminologies, and professional associations.

Given this specialization, there was only so far that a risk professional could rise within an organization. Expertise in buying insurance or pricing derivatives is not a board-level skill. At most, an ambitious risk manager might hope to become the head of a risk function, such as chief auditor or head of asset/liability management. However, even as the head of these risk functions, it was unlikely that a risk professional would be included in the executive committee of the company—even if they were, their compensation was usually a small fraction of what their counterparts made in line units.

Since the mid-1990s, however, risk management has become more recognized as a professional discipline—one in which there are numerous specializations, all of which share a common set of core competencies, just as in accounting or law. Why should this recognition have arrived only now? A quick answer is that it is because of the successful demonstration of value-added at individual companies against the background of a rapidly changing business and regulatory environment. Companies today are under more pressure to perform well—without acting irresponsibly—than ever before, while the environment in which they operate is arguably changing more quickly than at any time in the recent past.

The core competencies of risk management can help with both of these goals. On the one hand, risk managers have made more effort to project themselves as custodians of shareholder value. On the other, risk management has been successfully presented as a compulsory component of change management—a discipline much in demand as technology has fueled massive, sometimes disruptive, changes in the ways that many businesses work and compete.

Both of these contributions are much more in keeping with the mandate of executive management, and so the risk professional today can aspire to become a chief risk officer (CRO) with responsibilities for all risk functions within a company. A CRO is usually a member of the executive committee and commands compensation that has risen rapidly over the past decade.

A Career In Risk Management

The kinds of people attracted by the CRO role—particularly those who are likely succeed in achieving it—do not necessarily fit the profile of the

traditional risk manager. A career in risk management has always been an attractive option for professionals with a quantitative background in a subject such as finance, accounting, or math. In risk management, quantitative methods—securities valuation, probability estimation, and covariance analysis—can be directly applied to solve real-world business problems. Today, the trend toward ERM and the acceptance of the CRO role have helped the role of the risk professional evolve from that of a quantitative analyst, focused only on models and analysis, to that of a senior executive who is also concerned about corporate strategy, product and development, performance measurement, and incentive compensation.

In short, the risk manager has evolved from a number cruncher to a full business partner. Unsurprisingly, the prospect of someday becoming a CRO is very attractive to risk professionals. I led an Internet conference organized by ERisk in September of 2000, and polled the 175 professionals on whether or not they aspired to become a CRO. Nearly 70 percent of them said yes. The career path to CRO offers the risk professional the opportunity to think more broadly, learn new skills, and most importantly, add more value to the business.

As reflected in the rapidly rising compensation packages, companies have recognized the value that is added by risk professionals. Those with cross-functional skills are enjoying the lion's share of this increase, as highlighted by the rising compensation for CROs. Based on conversations with CROs and executive recruiters, the high-end compensation for CROs had increased from the mid-six figures in the early 1990s to more than seven figures by the end of the decade. Today, even those reporting to the CRO can command more than seven figures. In addition to higher compensation, the role of a CRO offers the risk professional the chance to have a much greater impact on an organization.

A CRO often reports directly to the CEO and sometimes even to the board of directors. For example, the CROs of Citigroup, CIBC, and Duke Energy report directly to their respective CEOs. In additional to being a C-level executive, CROs participate in the key business decisions of a company.

Today, a career in risk management is more exciting and challenging than ever before. But the widespread effort to improve risk management standards is not just about elevating risk managers. If an organization really wants to manage risk more effectively, it must disseminate understanding of risk throughout the business.

Today's employees are likely to know how the work of staff functions such as accounting or legal affects their business. Trading desk managers will know something about the tax and accounting of financial transactions; product developers will know something about liability issues. The greater the effects, the more they need to know and the more effort the company

should expend on making sure they understand the issues involved. The same is true for risk management.

Education and Evangelism

Education is an essential part of almost any job, but it is of paramount importance in a rapidly changing field like risk management. In fact, it would be fair to say that the success of a company's risk management program can be greatly enhanced by a well-developed risk education program. Even the most sophisticated risk management tool will be rendered ineffectual if employees do not know how to use it to its maximum possible advantage.

A good education program is essential for equipping a company's risk professionals (and general staff) to carry out their current functions more effectively and also lays the foundation for new responsibilities that may be assumed in the future. The steps involved in setting up a risk management education program include determining what topics need to be covered, finding appropriate materials to use in covering these topics, and determining the mode of delivery.

The topics to be covered in the program must be tailored to the specific needs of the organization and the group being educated. While many programs focus on traditional risk management areas such as market risk and credit risk, a comprehensive program would include other topics. For example, an ERM educational program might include:

- *Market risk management:* Market risk methodologies are generally well developed relative to other types of risk management. Standard coverage of this subject includes topics such as asset/liability Management, imposition of trading limits, and types of market risk.
- *Credit risk management:* Credit risk topics include credit ratings, exposure measurement, and limit management.
- *Operational risk management:* This is an area that is often vaguely defined and glossed over in risk management education programs. Topics to be covered include control self assessments and risk process mapping.
- *Enterprise risk management:* Coverage here should include establishment of risk frameworks, organizational structure, systems, and reporting, and risk culture. Risk analytics such as economic capital and VaR should also be included.
- *Risk transfer strategies:* Derivatives, insurance, and alternative risk transfer (ART) should be covered. This is an area of rapid change in risk management, so this portion of the curriculum will have to be updated on a regular basis.

Clearly, it is mandatory that industry practices, internal policies and procedures, and regulatory requirements are discussed for each of these topic areas. However, such rote learning tends not to grab the imagination of busy employees with other concerns, particularly when the subject, like risk management, is generally poorly understood and may be seen as a dull housekeeping function, rather than an active contributor to business performance.

As such, educators have to work doubly hard to ensure that their students find the material interesting. Fortunately, there is no shortage of illustrative—and interesting—stories about risk management. Specific examples and scenarios should be used throughout all phases of the curriculum to illustrate the principles being taught in a concrete and engaging manner. These case studies should include both best practices and debacles, followed by a discussion of lessons learned from these practices and situations. Using case studies will both demonstrate how the material being taught is relevant to real-life situations and maintain listeners' interest.

A comprehensive risk management education program will likely incorporate a variety of different modes of presentation. It is important to recognize that the educational effort should not only seek to inculcate new recruits in the company's approach to risk management, but should also provide for the continuing education of current employees. This continuing education takes three forms.

The first is the continuation of a formal training program (geared, say, toward various levels of certification). The second is providing employees with a way to remind themselves of what they have learned, or look up an unfamiliar topic. The third is to provide forums for discussion of specific risk problems, allowing expertise gained by one employee to be shared by another.

The Internet and company intranets are especially useful for these latter aspects of ongoing education and awareness. Materials covered during official education sessions, along with supplemental readings and reference materials, including complete information on the company's risk policies and procedures, should be made available to employees via an intranet application. A division of one asset management firm, for example, has a risk policies and procedures help function that is a part of every employee's computer desktop.

TECHNOLOGY AND THE CONVERGENCE OF RISK MANAGEMENT

Just as the profession of risk management has increased in importance, so too has the availability of tools that make the practice of risk management easier. Most notable among these has been the increasing emphasis on

quantitative tools and techniques, from pricing models to portfolio simulation and beyond. As we saw in Chapter 10, the effectiveness of these tools and techniques, and of the risk managers using them, is intimately linked with the technology built to support them.

More generally, the great strides made in risk management over the past few years have been supported by great strides in technology, first in the form of exponentially increasing processor power and subsequently in the form of networks, most obviously the Internet. One does not have to be a fan of dotcoms or a cheerleader for the New Economy to recognize that professions dominated by information and technology—risk management among them—are changing rapidly and will continue to change radically for the foreseeable future.

Risk professionals, including risk managers, technology providers, market makers, and consultants, must find new ways to leverage the power of this technology, and in particular the distributive power of the Internet and related technologies. One of the most obvious network-related trends in risk management today is *convergence*.

Within an institution, convergence has meant enterprise risk programs that integrate the management of market risk, credit risk, and operational risk, often under the leadership of a CRO who can take a holistic view of an enterprise's total risks. Within the financial markets, convergence has meant innovative risk transfer solutions such as catastrophe bonds and integrated insurance/derivative products, which provide more complete protection, including hitherto unmanageable risks. And across industry sectors—even across entire industries—convergence has meant a loosening of the traditional barriers between different institutions and organizations, as shared networks and protocols for the transfer of information allow companies to dynamically streamline and reshape themselves in the pursuit of business opportunities.

While convergence was an emerging trend even before "e" entered the business dialogue, the Internet and related technologies have added exponential speed to the process, and will continue to do so. This will happen in four ways: it will support the creation of a genuine risk management community; help establish common standards; enhance risk education; and improve analytics.

Develop a Community The Internet will help unite the various risk management groups into a common community. As we've already seen, different groups have historically been responsible for market risk, credit risk, operational risk, and insurance risk, each operating as an independent silo within an institution. These silos extended beyond their institutions. Different risk professionals joined different associations and purchased products and services from different providers.

As a highly efficient aggregator and distributor of content, the Internet will help develop a common community among risk professionals, allowing them to network with each other and share issues and ideas. The growth of the Global Association of Risk Professionals (GARP) is a good example of this effect. Founded in 1996, with no official headquarters or staff for many years, GARP was established on the Internet as a virtual meeting place for risk managers. Today, it is one of the world's largest risk management associations, with more than 15,000 members from more than 100 countries representing all risk disciplines.

Establish Common Standards In the past, risk professionals used different terminologies and methodologies when dealing with essentially similar risk concepts. Risk managers seemed to speak different languages when discussing the risks they faced. Consultants and regulators promulgated different standards designed for the risk of the month. Likewise, software providers developed applications designed for specific products.

Over time, risk practitioners have grown to recognize that risk is risk, and that common standards must be established for measuring and managing all aspects of risk within an institution. The Internet will provide an interactive medium that will help establish common risk standards and best practices for risk management. Regulators can put new supervisory proposals on their web sites and get feedback from a wider audience of risk professionals. Academics can do the same for peer reviews. Risk managers can benchmark their loss experience and risk practices against industry best practices. These interactive processes will speed the development of risk standards. A good example of this effect was JP Morgan's decision to post RiskMetrics, a Value-at-Risk methodology on the Web. RiskMetrics had an enormous take-up rate, quickly becoming a *de facto* benchmark for market risk.

Enhance Education One of the major barriers to effective risk management has been the lack of good educational resources for the various risk disciplines, particularly for operational risk and ERM. While professional associations such as GARP, the Risk Management Association (RMA), and the Risk and Insurance Management Society (RIMS) each play a constructive role, there remains a significant void in risk education. The Internet will help fill that void. It is without peer as the most powerful technology for developing, organizing, and distributing educational content; no less a figure than Cisco CEO John Chambers has suggested that the Internet's greatest value will be in education and e-learning. As long as bandwidth continues to increase at its current rate and search engines become more intelligent, the Internet will play an ever-more-effective role in providing risk

education. The Internet will provide interactive videos, on-line conferences, e-magazines, and faster and cheaper access to risk experts. It will also provide better access to general risk knowledge, as well as specific case studies for lessons learned and best practices.

Improve Analytics The Internet will improve risk analytics with respect to risk aggregation, risk monitoring, and risk technology. In terms of risk aggregation, the Internet will help corporate managers develop a consolidated view of risk, tracking losses, reporting incidents, and measuring aggregate exposures across the enterprise in real time. It will also provide the appropriate individuals with 24/7 access to critical risk information. In terms of risk monitoring, the Internet will do for risk professionals what My Yahoo has done for individuals. It will provide risk dashboards that integrate internal and external risk information. A risk manager will then be able to go to a single source and see the company's portfolio risk exposures, along with customized news, data, and early warning indicators.

The Internet will become the technological platform of choice, especially for small- to medium-sized institutions that cannot afford large Information Technology (IT) budgets. It will reduce prices for risk software and increase the number of users, resulting in significant cost economies with respect to software development, implementation, and maintenance. Today, leading providers of risk management software, whether in-house programmers or outside vendors, are quickly moving to web-enable their risk models. As risk models move from packaged software to an application service provider (ASP) environment, model risk should decrease because risk managers will have greater access to different models. They can then more easily test the sensitivity of their portfolios according to various risk models and assumptions.

TEN PREDICTIONS

The future for risk management is bright. Regulators and managers are recognizing the importance of risk management as a way to minimize losses and improve business performance. Risk professionals are moving up in the business world, both in terms of organizational level and compensation. Advances in risk methodologies and technologies are introducing a vast array of new tools for measuring and managing enterprise-wide risks, at a higher speed and lower cost than anyone could have imagined just a few years ago. While there are many remaining challenges, one cannot help but examine the progress and think that the best is yet to come for the risk management profession. Against this backdrop, I made 10 predictions in the first

edition of this book of how I thought risk management would change over the next decade. Let's revisit these predictions and compare them to today's reality to see how far the industry has come.

1. **ERM will become the industry standard for risk management**: ERM will continue to gain acceptance as the best way to ensure that a firm's internal and external resources work efficiently and effectively in optimizing its risk/return profile. New financial disasters will continue to highlight the pitfalls of the traditional silo approach to risk management. External stakeholders will continue to hold the board of directors and senior management responsible for risk oversight and demand an increasing level of risk transparency. More importantly, leaders in ERM will continue to produce more consistent business results over various economic cycles and weather market stresses better than their competitors. Their successes will gain attention and other companies will follow. These trends, coupled with a stock market that is increasingly unforgiving of negative earnings surprises, will compel businesses in all industries to adopt a much more integrated approach to measuring and managing enterprise-wide risks.
2. **A CRO will become prevalent in risk-intensive businesses:** The rise of the CRO goes hand-in-hand with the trend toward enterprise risk management. Risk management is a key driver of success for financial institutions, energy firms, asset management firms, and non-financial corporations with significant risk exposures. Many market leaders in these industries have already created the position of a CRO. Others will follow suit. Companies without a CRO are faced with three perplexing questions: First, are we comfortable with diffused risk responsibilities, and if not, who is the *de facto* CRO—the CEO or CFO? Second, are their necessarily part-time efforts sufficient to manage risk in an increasingly volatile business environment? Finally, will the company be able to attract and retain high caliber risk professionals if a CRO career track is not available to them? For an increasing number of companies, the logical resolution of these questions will be the appointment of a CRO and the dedication of resources to implement an ERM program.
3. **Audit committees will evolve into risk committees.** As boards of directors recognize that they have responsibilities to ensure that appropriate risk management resources are in place, they will replace or supplement their audit committees with risk committees. A number of leading institutions, Chase and Export Development Corporation of Canada among them, have already established risk committees of the board. As we discussed in Chapter 5, the board's responsibilities for risk management have been clearly established in regulatory and industry initiatives

worldwide. Key governance and risk reports include the Dey Report in Canada, the Turnbull Report in the UK, and the Treadway Commission Report in the United States. The result of these and other similar initiatives is that board directors have begun to realize that their responsibilities go beyond traditional audit activities, and that they need to ensure resources and controls are in place for all types of risk. Going forward, companies will establish risk committees of the board, and their audit committees will either become sub-committees or independent committees that have the traditional audit committee focus of ensuring accurate financial reporting and statements.

4. **Economic capital will be in; VaR will be out:** Managers and external stakeholders will demand a standardized unit of risk measurement, or common currency, for all types of risk. This way, they can spot trends in a company's risk profile, as well as compare the risk/return performance of one company against others. To date, VaR has gained wide acceptance as a standardized measure for market risk. However, VaR has three major flaws. First, it does not capture tail risks due to highly infrequent, but potentially devastating, events. Second, its inability to capture tail risks makes VaR a poor measure for credit and operational risks (or even market risk positions with significant optionality). Third, VaR measures the risk, not the return, of any risk position. Yet financial models that have passed the test of time, such as capital asset pricing model (CAPM) or the Black-Scholes option-pricing model, evaluate both risk and return. The concept of economic capital is intuitively appealing because one of the main reasons companies hold capital is to absorb potential losses from all types of risk. Risk-adjusted return on capital extends the concept and measures business profitability on a risk-adjusted basis. The Basel Committee has already adopted economic capital as the framework for international regulatory capital requirements in the banking industry. Other industries will follow and adopt it as a common currency for risk.
5. **Risk transfer will be executed at the enterprise level:** The integration of risk transfer activities has already happened as far as hedging and insurance strategies are concerned. For example, companies that hedge with derivatives realize they can save on hedging costs if they execute portfolio hedges rather than individual securities hedges. Companies that bundle their insurance coverage through multi-risk, multi-year policies are also realizing significant savings on insurance premiums. Alternative risk transfer (ART), reviewed in Chapter 8, goes one step further in combining capital markets and insurance techniques. The rise of ERM and ART products will mean that risk transfer strategies are increasingly formulated and executed at the enterprise level. In the

past, companies made risk transfer decisions to control specific risks within a defined range, without being particularly thoughtful about the cost of risk transfer unless it was prohibitively high. In the future, companies will make risk transfer decisions based on an explicit comparison between the cost of risk retention versus the cost of risk transfer and execute only those transactions that increase shareholder value.

6. **Advanced technology will have a profound impact on risk management:** As discussed in the previous section, the Internet will have a significant impact on risk management and how information, analytics, and risk transfer products are distributed. Beyond the Internet, the increase in computing speed and decline in data storage costs will provide much more powerful risk management systems. Mid-sized companies will have access to sophisticated risk models that were once the privilege of large organizations. Even individual investors will be able to apply advanced risk/return measurement tools in managing their investment portfolios. Just as market risk measurement at large trading organizations is being conducted increasingly frequently, the time interval for enterprise-wide risk measurement and reporting will move from monthly to weekly to daily, and perhaps ultimately to real time. Moreover, the development of wireless and handheld communication devises will enable the instantaneous escalation of critical risk events, and allow risk managers to respond immediately to emerging problems or new opportunities.
7. **A measurement standard will emerge for operational risk:** Today, there is considerable debate not only about the quantification of operational risk, but also how to best define it. Approaches to assessing operational risk range from qualitative assessment of probability and severity based on management judgment, to quantitative estimate of potential loss based on industry and company loss histories. The lack of consistent operational loss data, partially as a function of the infrequency of major operational risk events, has led to the development of analytical models such as extreme value theory to come up with loss estimates. Other models borrow from total quality management techniques or dynamic simulations to quantify operational risk. More recently, there has been some support, and some encouraging results, from early experimentation with neural networks to recognize patterns in operational risk. As the practice of operational risk management gains acceptance, and as data resources become more available as a result of company and industry initiatives, a measurement standard will emerge for operational risk. However, the greatest challenge for operational risk will remain one of management, not measurement.

8. **Mark-to-market accounting will be the basis of financial reporting:** Over time, the risk management profession has recognized the importance of mark-to-market accounting versus accrual accounting in reporting the financial condition of a company. While accrual accounting is adequate for reporting the value of physical assets, it can provide the wrong signals in reporting financial and other intangible assets. The use of marked-to-market accounting is widely accepted in the market risk field, and is gaining acceptance in credit risk management, where credit-based assets are mark-to-market given their probability of default (e.g., credit ratings or credit spreads). Given the cry for greater risk transparency from shareholders and regulators, it is likely that variability (i.e., risk sensitivity) will be much more integrated into financial reporting in future, including the full use of mark-to-market accounting for all financial assets.
9. **Risk education will be a part of corporate training and college finance programs:** As companies recognize the need to train and develop their risk management staff, corporate training programs will increasingly feature risk management. These training programs will likely be a combination of internal and external resources, and include internal workshops, external conferences, and Internet-based training tools. Given the rising corporate demand for skilled risk professionals, professional organizations and colleges will continue to integrate risk management into their course offerings. Professional certification and college degree programs will gain popularity and acceptance. Similar to the development of the CFA certification in finance and investments over the past decade, a widely accepted professional certification in risk management will emerge in the next decade. Colleges will expand their course offerings beyond derivative products and credit analysis to offer courses in ERM, risk management applications in various industries, and integrated risk transfer.
10. **The salary gap among risk professionals will continue to widen.** The trend toward ERM and the appointment of CROs has created an exciting career path, and attractive compensation opportunities, for risk professionals. However, this new career opportunity will only be available to risk professionals that continue to develop new skills and gain new experiences, while the others will be left behind. The salary gap that has developed over the past several years will continue to widen in the next 10 years. On one hand, the compensation for risk professionals with cross-functional skills will increase faster than other professions due to rising demand for their services. On the other hand, risk professionals with narrow skills or who serve in limited intermediary roles will not enjoy above average raises, and may in fact see their job

security decline as their jobs become less relevant in the new world of risk management.

2013 LOOKING BACK

Looking back from a decade after I first made these predictions, it may be fun to see how clear my crystal ball was at the time. Bill Scotti, of the Global Association of Risk Professionals (GARP), recently evaluated my predictions in a 2012 article—the findings of which are summarized below:

1. **Enterprise Risk Management (ERM) will become the industry standard for risk management:** While ERM has yet to become an industry standard, there is certainly a lot of movement in this direction, which makes this prediction a true one. For example, a Global Risk Management study conducted by Accenture in 2011, which spanned a number of different countries and industries, demonstrated that "more than 80 percent of the survey respondents overall have an ERM program in place or plan to have one in the next two years." However, companies are still having difficulty breaking away from the traditional silo approach to risk management, which has hindered the growth of ERM as an industry standard. Thus far, ERM is the most prevalent in the financial sector, with banks, hedge fund providers, and broker-dealers in the lead.
2. **A CRO will become prevalent in risk-intensive businesses:** Likewise, the 2011 Accenture study also proves this prediction true, because it shows that C-level management of risk management is becoming increasingly prevalent among risk-intensive businesses: 66 percent of survey respondents already have a CRO, while a further 20 percent have executives who perform CRO responsibilities (and simply do not have the title).
3. **Audit committees will evolve into risk committees:** This has also been proven true by time. In September of 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a paper called "ERM-Integrated Framework;" as suggested by its title, the paper outlined the essential framework of successful ERM. This has greatly influenced the transformation of the internal audit function. For example, the Institute of Internal Auditors (IIA) recommends that internal auditors should work with both the audit committee as well as management to implement ERM. IIA also draws some clear lines around the responsibilities of internal auditors: they should *not* undertake "setting the risk appetite, imposing risk management processes, management assurance on risks, making decisions on risk responses, implementing

risk responses on management's behalf, and accountability for risk management."

4. **Economic capital will be in; VaR will be out:** Bill Scotti says that "VaR is useful for market risk and control over a short period of time," but it does not consider "risk reward trade-off for all of the economic units of an institution," while economic capital *does*. In his eyes, this certainly makes it superior to VaR. Economic capital also addresses risks apart from the most visible and most easily quantified market risk—liquidity risk, operational risk, and strategic risk can all run rampant without supervision (as demonstrated by the market crash of 2007). Furthermore, economic capital also helps to streamline ERM—the advantages of economic capital have been recognized in corporate culture, where there has indeed been a shift in primary usage from VaR to economic capital.
5. **Risk transfer will be executed at the enterprise level:** This was actually already starting to occur when the first edition of this book was published in 2003, in terms of hedging and insurance strategies. This has continued through today, where the "management of risk transfers" now occurs through "assessments, systems, and other tools."
6. **Advanced technology will have a profound impact on risk management:** This is definitely true in 2013: during this last decade, we have seen "exponential growth in the speed of data processing," incredible booms in cloud and social media services, as well as a shift from "in-house software development to ASP models that provide comber-based services to customers over a network."—all of which has transformed risk management profoundly.
7. **A measurement standard will emerge for operational risk:** Unfortunately, this has not come true in 2013. While Basel II and Basel III provide strict regulations for banks, this "metric doesn't cut across industry" and most other kinds of firms are left to their own devices. For example, recovery costs and loss-event data are not properly utilized in product pricing, while the front office is still finding it difficult to implement operational risk management tools. Furthermore, because there is no industry standard, it is difficult for line managers to implement operational risk management, which makes the entire ERM implementation process less efficient.
8. **Mark-to-market accounting will be the basis of financial reporting:** While this might have happened organically if nothing out of the ordinary occurred, the financial crisis of 2008 caused the abrupt return of "fair value accounting under FASB 157." Currently, there is still conflict between FASB and IFRS with regard to mark-to-market accounting, making it unlikely for it to become the basis of financial reporting in the near future.

9. **Risk education will be a part of corporate training and college finance programs:** Happily, nowadays most major universities offer a graduate degree in risk management, so this is definitely true. Organizations like GARP and PRMIA also offer "risk training and certification programs."
10. **The salary gap among risk professionals will continue to widen:** This is also very true; Ben Scotti says that "generalists are compensated at a greater level than specialists because of their cross-function skills," which exactly matches the original prediction. The Risk Talent Associates' 2011 annual salary survey demonstrated that the salary gap between senior associates and CROs continues to widen.[1]

In summary, Scotti concluded that eight of my 10 predictions made 10 years ago have been fulfilled, while the jury is still out on the remaining two.

CHAPTER 20

Everlast Financial

It is the year 2020. Everlast Financial is a fictional financial services company with global investment bank, commercial banking, and insurance operations. Pamela was appointed CRO two years ago, after spending five years as a trader and three years as a market risk manager.

Pamela, the Chief Risk Officer of Everlast Financial, is enjoying breakfast at home when her cellular watch suddenly begins beeping furiously. She checks the digital display and notes the warning "Operational Risk Alert." She thinks to herself that, despite the many advances in risk management, an operational risk debacle is still every risk officer's worst nightmare. Using her laptop, she logs on to the global risk management system to find out what is happening. Before she can so much as check the interactive risk monitoring program, Garrett, Chief of Staff, appears on the screen using the PC videoconferencing application. "We've identified a rogue trader," Garrett says. "While we were examining the traders' records to prepare for their annual compensation review, we identified a discrepancy in Rick Gleeson's accounts. Further investigation of the transactions in question revealed that they were fake transactions designed to conceal about $200 million in trading losses in emerging markets bonds over the past nine months."

"We need to move quickly on this to avoid additional losses and bad press," Pamela replies, "Let's initiate a videoconference with the CEO, the heads of the audit committee, the trading unit, corporate communications, the legal department, and human resources. We need to clarify the details of what happened, why it happened, and what should we do to handle the situation."

"I'll get right on it," says Garrett.

The next day, Brandon, the CEO of Everlast Financial Corp., has called Austin, the head of trading, into his office. "Your trading operations have generated nearly half of the corporation's profits over the past three years, but this is a very serious problem. Our investigation has turned up evidence that Rick has indeed been involved in unauthorized trading and we have a

zero-tolerance policy for unethical behavior. Austin, how did this happen under your watch and what should we do about Rick?" Brandon asks.

"I assumed our risk management systems would have picked this up. Also, Rick is one of our most talented traders," Austin argues. "He just had the bad luck to be trading bonds in emerging markets at a time when the market was a bit rocky. While we shouldn't condone what he did, the performance pressure here can be immense, and, if his gambles had paid off, we would be rejoicing right now rather than talking about this crisis."

"So what do you think we should do?" Brandon asks.

"Well, he should forfeit all of his bonus for this year, based both on the fact that he generated losses for the firm and that he violated risk management policies which could cause us great embarrassment in the public eye."

"So you think that is the only punishment he should receive? You don't think he should be fired, which is the stated consequence for this kind of offense in our risk policies manual?" Brandon asks.

"I know that is what is recommended, but it would be such a shame to lose one of our best traders. I strongly encourage you to give him another chance," Garrett asserts.

"We have already determined in our company-wide risk policy that there will be no second chance for offenders of this magnitude. Your willingness to overlook such non-compliance in pursuit of higher profits poses a much bigger risk to the firm than the loss of a skillful rogue trader. We can easily replace him with another trader, but the damage he has done is irreversible. Since you have demonstrated a blindness to this basic risk management concept, you are both fired. I have plenty else to do to deal with this fiasco, so don't try to argue with me," Brandon states in his most assertive voice.

As Austin leaves, Brandon calls Jennifer, the head of HR, who comes into his office for a discussion. "I want you to personally take care of the dismissals of Austin and Rick. I also want to discuss what we can do from an HR standpoint to prevent these scenarios in the future," Brandon says. "Pamela informed me that one of the abnormalities that we discovered about Rick in retrospect was that he never took vacations longer than two days. Learning from this, I want HR to generate an annual report on employees' vacation time, flagging any employees who have not taken vacations of at least a week in length during the past year. Also, employees who consistently fail to use all of their allotted vacation days should be identified because they may either be hiding something or be candidates for burnout."

"That sounds like a good idea," Jennifer agrees, checking to see that the voice-interface on her smartphone has been recording all of these ideas. "I also think this situation and its consequences should be incorporated into one of our training videos offered through the risk intranet. It would be a valuable lesson learned for our new managers and employees."

"Absolutely. When we make that video, I want to speak in it to set the tone from the top and demonstrate how seriously we take breaches in our risk policy," says Brandon.

Meanwhile, Curtis, the COO, has been meeting with Peter, the company's head of risk transfer, to determine what coverage Everlast Financial Corp. has for this event. "Fortunately," says Peter, "the integrated risk policy that we have has specific provisions for operational risk failures such as rogue traders. After a $10 million deductible, we are covered for any losses up to $1 billion. For the future, though, I think we should consider looking into earnings per share insurance, since that way we would have much broader risk coverage and there will be no question as to whether or not our insurance policy covers specific losses."

"Yes, I know that EPS insurance has come down a lot in price since it has become more popular. Go ahead and get us some quotes," says Curtis. After his meeting with Curtis, Peter dials into risk.com, the Internet risk exchange, to get some quotes on EPS insurance. He submits a standardized term sheet for EPS insurance, attaches Everlast Financial's loss history and enterprise risk rating, and within 10 minutes, his inbox receives five quotes from pre-qualified insurance providers. Peter finds that two of the quotes represent a net cost of risk transfer that is below Everlast Financial's net cost of risk retention. His analysis on the on-line risk calculator shows that by executing an EPS insurance transaction, the company's market value should improve by 4 to 5 percent. After a brief conversation with Pamela, Peter executes the EPS transaction with a European insurance company.

Back in his office, Curtis calls Brandon to relay the good news that the trading losses will be covered by the firm's insurance policy. After speaking briefly with Curtis, Brandon calls Garrett again to exchange information with him and generate further ideas for using the situation as a learning experience. "I understand that besides not taking more than two consecutive vacation days, over the past year Rick's trading behavior was unusual in terms of trading volume and pattern. I've already spoken with Jennifer about identifying potential problem employees from an HR perspective, but I want you to consider creating other metrics to serve as early warning signals for possible rogue activities. Look at Rick's trading from as many different angles as possible to determine the ways in which it differed from other traders' activity. Maybe we can share data with trading units at other financial institutions to jointly identify patterns of trading that should serve as early warnings of irregular activity. I want you to start thinking about what we might want to include in a new operational risk report. That is the area where our risk reporting needs continuous improvement since operational risk can rear its ugly head in so many different ways. We need to work on that."

Brandon tells his secretary to set up an impromptu videoconference with the board members, as well as conference calls with the equity analysts who cover Everlast Financial Corp. Brainstorming the ideas that he wants to convey to these stakeholders, Brandon decides that key points should include ideas such as:

- State-of-the-art risk management can't ensure that bad events will never happen, but the investments that Everlast Financial has made over the past several years in ERM and risk technology have identified and corrected this problem at an early stage.
- The company has every intention of openly communicating the details and proceedings surrounding this situation as soon as they become available, since open communication and risk transparency is one of the tenets of Everlast Financial's risk management program.
- Based on the lessons learned from this fiasco, steps are being taken to reduce the likelihood of a similar event in the future, as much as this is possible. The soon-to-be-implemented vacation report from HR, the work in progress on better operational risk analysis and reporting, the incorporation of the situation into a case study for a training video, and the dismissal of both the rogue trader and the head of trading will all be discussed.
- The analysts in particular must be assured that the costs of the debacle will not substantially affect the company's earnings due to the insurance policy coverage. Additionally, the company has executed a broader EPS insurance coverage to protect itself from unforeseen events going forward.

As the day draws to a close, Brandon sits back and thinks about the risk management advances that have made this situation less explosive than it would have been 20 years ago—the real-time risk escalation that alerted him and Pamela of the situation that morning, coupled with technology-enabled instant response; and the insurance coverage for operational risk failures. Without this sophisticated risk monitoring, the rogue trading may have continued unnoticed for years, as was the case with a number of prominent rogue traders in the twentieth century. How did risk managers function in those days without the technology and risk transfer products that are now available? While the advances were substantial, there was still much to be done, thought Brandon as he shut off the lights to go home. With his highly competent risk management group and the technology that enabled him to stay abreast of business developments 24 hours a day, he could go home with the assurance that if any major new developments occurred, he would be among the first to know.

SECTION

Five

ERM Implementation

CHAPTER 21

ERM Implementation

Confucius said, "The essence of knowledge is, having it, to use it." With respect to ERM, it tells us that while careful planning and research is all very well, if we do not act upon this accumulated knowledge, it goes to waste. In this last section of the book, we will discuss implementation requirements that will help firms to translate the concepts that we have discussed in the previous sections into actions.

To share my first experience in implementing enterprise risk management (ERM), I would like to return to the story of my tenure as Chief Risk Officer at GE Capital, which demonstrated to me the veracity of this idiom very tangibly. As the reader might recall from Chapter 4, in 1993, I was hired to be the CRO of GE Capital Markets Services, which was, at the time, going through the start-up phase with aggressive growth and profitability targets. In order to quickly build up the organization, the company had hired a team of traders from a foreign bank, hoping to benefit from their industry contacts and years of experience. As part of GE Capital, with its pristine triple-A credit ratings, it was critical for the new business to establish a comprehensive ERM framework—and for this to happen quickly.

So I hit the ground running. I spent the first few months focusing on the hard side of risk management—setting up risk policies and limits, analytical models, and an integrated system and reporting infrastructure. However, I immediately came up against opposition, because the traders had never operated in such a controlled environment in their previous jobs. As such, they didn't take risk management seriously and were entering only 80 to 90 percent of their trades. Hence, each morning the risk reports were full of errors because they didn't represent the full portfolio of positions. When I went to discuss this issue with the head trader at the time, he blatantly rejected my authority and brushed me off. "We know the risk of our portfolio like the back of our hands," he told me dismissively, "We don't really need your system to tell us about our portfolio. Our team is busy building the business. We will enter the trades when we have free time."

FIGURE 21.1 The Hard and Soft Sides of Risk Management

Frustrated, I informed the group president that I couldn't do my job without the cooperation of the traders. I have to admit; I was impressed by what the president did when he heard about the situation. He made a critical decision that changed the culture of the group and helped me to appreciate the *soft* side of risk management for the rest of my career. Determined to set the tone from the top, the president shut all business operations down for two days and put all of the employees through a risk management boot camp at GE's corporate training center in Crotonville, New York. We reviewed all of the ERM policies, why they were set in place, and exactly who was accountable for each step of the process. At the end of the two days, the president conveyed a clear message that we will be running the business in a risk-controlled environment, and if the traders didn't change their behavior we would change the traders!

To me, that was a defining moment in the risk culture of the company. From that point on, the traders underwent a drastic change in attitude and we had 100 percent compliance with the ERM framework. In fact, the capital markets group was recognized as an example of best practice in risk management within GE Capital, and the company honored me with the Pinnacle award. We went on to capture 25 percent of market share with no policy violations. My experience at GE Capital has taught me just how important it is to balance both the hard and the soft side of ERM—the yang and yin, so to speak. Figure 21.1 outlines the key features of both.

BENEFITS OF CORPORATE GOVERNANCE AND ERM PRACTICES

To build the business case for ERM implementation, it is important to articulate the expected benefits and how it can create business value. For individual companies, the benefits of ERM will depend on their unique business

challenges, investments in staff and systems, and implementation success. However, it would be useful to examine industry surveys and empirical studies that indicate how better governance and ERM practices are associated with improved financial performance and shareholder returns. Below, we provide summaries of several key studies.

McKinsey & Company (2002)

In 2002, McKinsey & Company conducted a cross-industry, global survey of more than 200 institutional investors, which indicated that poor governance structure would turn 60 percent of investors away from a company. Nearly a third of the survey respondents also indicated that they would even avoid an entire country that had poor governance standards. In fact, investors are willing to pay a premium for well-governed companies. The McKinsey reported that the average premium in the United States was 12 to 14 percent, 20 to 25 percent in Asia and Latin America, and as high as 30 percent in Europe and Africa.[1] The attractiveness of a strong governance structure to investors is a good indicator of how much value it can potentially add to an organization.

Brown and Caylor (2004), Cheng and Wu (2005)

A Brown and Caylor study of 2,327 cross-industry firms published in 2004 reveals that companies with strong governance structures outperform those with weaker governance structures in terms of return on equity (ROE), profit margins, and dividend payouts. For instance, firms ranked in the tenth percentile of the Corporate Governance Quotient[2] produced five-year returns that are 3.95 percent lower than the averages of their respective industries. Conversely, those in the ninetieth percentile yielded returns that were 7.91 percent higher than industry averages.[3] A similar 2005 study by Cheng and Wu compounded these findings by establishing that this phenomenon is augmented by the size of the firm.[4] In other words, the larger the company, the bigger an effect governance structure will have on returns.

By performing regression analyses on 35 variables regarding "board composition, compensation, takeover, and audit," the Brown and Caylor report determined that "firms with weaker governance perform more poorly, are less profitable, more risky, and have lower dividends than firms with better governance."[5] Intriguingly, the study identifies board composition as the single most important factor behind the success of companies with firm governance structures over those without them, based on their significant, positive contribution to one-year returns.[6] We will discuss the importance of board structure further in the next chapter.

Hoyt and Liebenberg (2009)

Hoyt and Liebenberg conducted a study in 2009 investigating the relationship between ERM programs and firm value. They analyzed data from 117 publicly traded U.S. insurers between 1998 and 2005.[7] After performing regression analysis, they found that ERM programs are associated with a 16.5 percent, statistically and economically significant, equity premium. In addition to this finding, the study identifies insurance companies with an ERM program as having lower returns volatility. The results indicate that ERM is associated with improved shareholder wealth and financial stability.

Standard & Poor's (2010)

In 2010, Standard & Poor's evaluated the stock performance of 165 North American and Bermudan public multiline insurance companies.[8] S&P assigned each company an ERM score ranging from "excellent" to "weak" and then compared their score with their stock performance. The study found that between January and November of 2008, companies with an "excellent" ERM score fared better than their counterparts, experiencing a –30 percent change in stock performance compared to –60 percent for companies with "weak" ERM scores. In 2009, companies with "excellent" ERM ratings experienced a +10 percent change in stock performance, versus a –10 percent change for companies with "weak" ERM scores. Furthermore, S&P finds a strong correlation between having a high ERM score and experiencing low share price volatility in 2009. These findings are significant because they show that during periods of economic fluctuation, strong ERM programs can help individual companies to maintain stability and value.

ERM IMPLEMENTATION REQUIREMENTS

ERM implementation is more important than ever in today's turbulent economy. At the 2009 World Economic Forum in Davos, Switzerland, it was reported that the global financial crisis has destroyed 40 to 50 percent of world wealth. While there have been other severe recessions, this one stands out in an important way; its impact is felt not only by every country and industry, but also by every company and individual. The current economic downturn has thus served as the ultimate stress test—one that many companies have failed to pass.

The GE Capital story is one of ERM implementation, where the capital markets group moved itself from where it was to where it wanted to be.

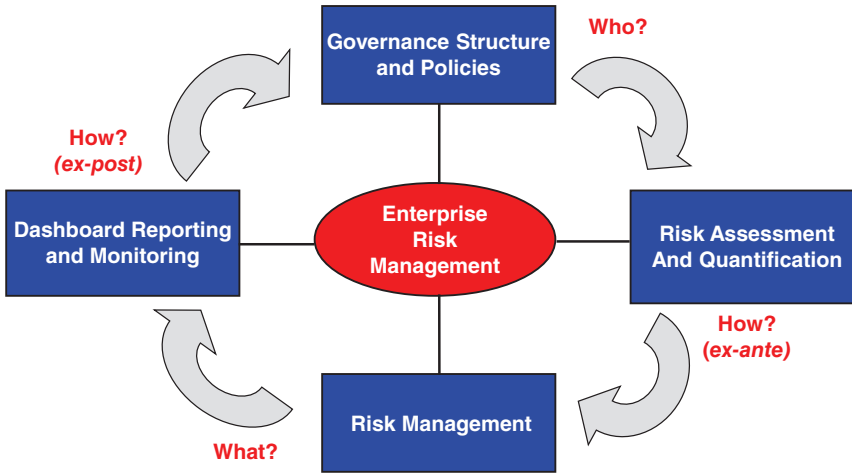


FIGURE 21.2 ERM Implementation Requirements

Other companies must go through their own growing pains as they implement ERM in a structured and balanced way. What are the key implementation requirements for ERM? Figure 21.2 provides an overview of four key building blocks, which are designed to address four fundamental questions:

1. *Governance structure and policies: Who* is responsible to provide risk oversight and make critical risk management decisions?
2. *Risk assessment and quantification: How* (ex-ante) will they make these risk management decisions in terms of analytical input?
3. *Risk Management: What* specific decisions will they make to optimize the risk/return profile of the company?
4. *Reporting and Monitoring: How* (ex-post) will the company monitor the performance of risk management decisions (i.e., a feedback loop)?

The above questions may sound simple but addressing them effectively can be very challenging for most firms. Let's look at the main characteristics of each requirement here. Chapters 22 to 25 will provide further details on implementation steps.

Definitions of Risk and ERM

Based on the ERM implementation building blocks in Figure 21.2 and the notion that any risk can be conceptualized (and ideally quantified) as a bell

curve, we can establish the following updated and more detailed definitions of risk and ERM:

- *Risk* is a variable that can cause deviation from an expected outcome, and as such, may affect the achievement of business objectives and the performance of the overall organization.
- *ERM* is an integrated management process for managing enterprise-wide risks—including strategic, financial, operational, compliance, and reputational risks—in order to maximize firm value. This process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting.

Governance Structure and Policies

Governance structure and policies address the question of *who* (i.e., individuals or committees) is responsible for making risk management decisions, and *what* are the policies that provide incentives, requirements, and constraints (e.g., risk tolerances) for the decision makers. Governance structure and policies should include the following:

- *Risk governance:* How should the board provide effective risk oversight? First, should the board consider establishing a separate risk committee, or assign risk oversight responsibility to the audit committee or the full board? Second, should the board consider adding a risk expert to assist in risk issues, similar to the additions of financial experts to oversee financial issues? Finally, should board members be more engaged in the risk management process? These questions regarding the board's governance structure, risk expertise, and its role in ERM should be addressed to enhance the board's effectiveness in providing risk oversight. As a recent example, UBS announced that it added one CRO and two CFOs to the board, and investors reacted favorably, sending the stock price up 7 percent in late trading. Finally, board members should be fully engaged in the risk management process. This includes debating risk tolerance levels, challenging management on critical business assumptions, and holding management accountable for the risk-return performance of past decisions. Beyond the board structure, the management structures at the corporate management and business segment levels should also be fully aligned.
- *ERM Policy:* An ERM policy should be established to support the risk management oversight activities of the board. Key components of an ERM policy may include board and management governance structure,

summary of risk committee charters, risk management roles and responsibilities, guiding risk principles, summary of risk policies and standards, analytical and reporting requirements, and exception management processes. Moreover, one of the most important components of an ERM policy is the delineation of specific risk tolerance levels for all critical risk exposures. These risk tolerance levels enable the board and corporate management to control the overall risk profile of the organization.

- *Risk-compensation linkage:* The design of incentive compensation systems is one of the most powerful levers for effective risk management (including risk culture), yet insufficient attention has been paid to how incentives influence risk/return decisions. For example, if incentive compensation is driven by earnings growth or stock price appreciation, then corporate and business executives would be motivated to increase risks in order to drive up short-term earnings and the stock price. Traditional executive compensation systems do not provide the appropriate framework for risk management because they can motivate excessive risk taking. To better align the interests of management and investors, incentive compensation systems must be driven by long-term, risk-adjusted financial performance. This can be achieved by incorporating risk management performance into the incentive compensation system; establishing long-term risk-adjusted profitability measurement; using vesting schedules consistent with the duration of risk exposures; and applying claw-back provisions to account for tail-risk losses.

Risk Assessment and Quantification

Risk assessment and quantification processes address the question of *how* analytical tools and processes support risk management decisions. Risk assessment and quantification tools for ERM include:

- *Risk assessments* that identify and evaluate the key risks facing the organization, including estimations of the probability, severity, and control effectiveness associated with each risk.
- *Loss-event database* that systematically captures an organization's actual losses and risk events so management can evaluate lessons learned and identify emerging risks and trends.
- *Key risk indicators (KRIs)* that provide measures of risk exposures over time. Ideally, the KRIs are tracked against risk tolerance levels and integrated with related key performance indicators (KPIs).
- *Risk analytical models* that provide risk-specific and/or enterprise-wide risk analyses, including value-at-risk (VaR), stress-testing, and scenario

analyses. One of the key objectives of these models is to provide loss estimations given an organization's risk portfolio.
- *Economic capital models* that allocate capital to underlying risks based on a defined solvency standard. These models often support risk-adjusted profitability and shareholder value analyses.

While the above tools can provide useful information, organizations should be aware of potential pitfalls. One of the key lessons from financial crises is that major risk events are usually the consequence of not one risk, but a confluence of interrelated risks. To avoid the silo approach to risk analysis, companies need to integrate their risk assessment and quantification processes, as well as focus on critical risk interdependencies. Currently, many companies use value-at-risk models to quantify market risk, credit default models to estimate credit risk, and risk assessments and KRIs to analyze operational risk. However, each of these tools might be used independently. Going forward, companies must integrate these analyses to gain a broader perspective.

Risk models are only as reliable as their underlying assumptions. Prior to the financial crisis of 2008, many of the credit models used were based on the assumption that years of rising home prices and benign default rates would continue in the future. Moreover, credit and market risk models often assume some level of diversification benefits based on historical default and price correlations.

However, the financial crisis has also provided strong evidence of the risk management adage that price correlations approach one during market stresses (i.e., global asset prices dropped in concert). In other words, the benefit of diversification may not be there when you need it most. Companies should stress-test the key assumptions of risk models to understand how sensitive model results are relative to these assumptions.

Risk Management

Risk management addresses the question of ***what*** specific decisions are made to optimize the risk/return profile of the company. Key decision points include:

- *Risk acceptance or avoidance:* The organization can decide to increase or decrease a specific risk exposure through its core business, mergers and acquisitions (M&A), and financial activities.
- *Risk mitigation:* This involves establishing risk control processes and strategies in order to manage a specific risk within a defined risk tolerance level.

- *Risk-based pricing:* All firms take risks in order to be in business, but there is only one point at which they can get compensated for the risks that they take. That is in the pricing of their products and/or services, which should fully incorporate the cost of risk.
- *Risk transfer:* If risk exposures are excessive and/or if the cost of risk transfer is lower than the cost of risk retention, an organization can decide to execute risk transfer strategies through the insurance or capital markets.
- *Resource allocation:* An organization can allocate human and financial resources to business activities that produce the highest risk-adjusted returns in order to maximize firm value.

At most organizations, the risk management function does not handle most of the above decisions. Rather, they are made by business units and other corporate functions. However, the risk function should support business and corporate decision makers with the risk/return analytical tools outlined in the previous section. Moreover, the risk function should provide an independent assessment of critical business/risk issues.

The role and independence of the risk management function is a critical issue that should be addressed by each organization. Should the risk function be a business partner and actively participate in strategic and business decisions, or take the role of a corporate overseer and provide independent oversight? Can the risk function balance these two potentially conflicting roles? A related issue is whether the chief risk officer (CRO) should report to the CEO or the board.

One organizational solution may be to establish a solid reporting line between the CRO and CEO, and a dotted reporting line between the CRO and the board. On a day-to-day basis, the risk function serves as a business partner advising the board and management on risk management issues. However, under extreme circumstances (e.g., CEO/CFO fraud, major reputational or regulatory issues, and excessive risk taking) the dotted line to the board becomes a solid line such that the CRO can go directly to the board without concern about his or her job security. Ultimately, to be effective the risk function must have an independent voice. A direct communication channel to the board is one way to ensure that this voice is heard.

Reporting and Monitoring

The risk reporting and monitoring process addresses the question of *how* critical risk information is reported to the board and senior management, and how risk management performance is evaluated. It has been wisely said that what gets measured gets managed.

However, there remains a general sense of dissatisfaction among board members and senior executives with respect to the timeliness, quality, and usefulness of risk reports. Currently, companies often analyze and report on individual risks separately. These reports tend to be either too qualitative (risk assessments) or quantitative (VaR metrics). Risk reports also focus too much on past trends. In order to establish more effective reporting, companies should develop forward-looking role-based dashboard reports. These reports should be customized to support the decisions of the individual or group, whether that is the board, executive management, or line and operations management. ERM dashboard reports should integrate qualitative and quantitative data, internal risk exposures and external drivers, and key performance and risk indicators.

How do we know if risk management is working effectively? This is perhaps one of the most important questions facing boards, executives, regulators, and risk managers today. The most common practice is to evaluate the effectiveness of risk management based on the achievement of key milestones or the lack of policy violations, losses, or other unexpected events. However, qualitative milestones or negative proves should no longer be sufficient. Organizations need to establish performance metrics and feedback loops for risk management. Other corporate and business functions have such measures and feedback loops. For example, business development has sales metrics, customer service has customer satisfaction scores, HR has turnover rates, and so on.

In order to establish a feedback loop for risk management, its objective must first be defined in measurable terms. The objective of risk management could, for instance, be defined as to minimize unexpected earnings volatility. In this case, the purpose of risk management is not to minimize absolute levels of risks or earnings volatility, but to minimize unknown sources of risks or earnings volatility.

Based on this definition, Figure 21.3 provides an example of using earnings volatility analysis as the basis of a feedback loop. At the beginning of the reporting period, the company performs earnings-at-risk analysis and identifies several key factors (business targets, interest rates, oil price, etc.) that may result in a $1 loss per share, compared to an expected $3 earnings per share. At the end of the reporting period, the company performs earnings attribution analysis and determines the actual earnings drivers. The combination of these analyses provides an objective feedback loop on risk management performance. Over time, the organization strives to minimize the earnings impact of unforeseen factors. While this may not be the right feedback loop for an individual organization (i.e., non-profit), every company should establish some feedback loop(s) for risk management.

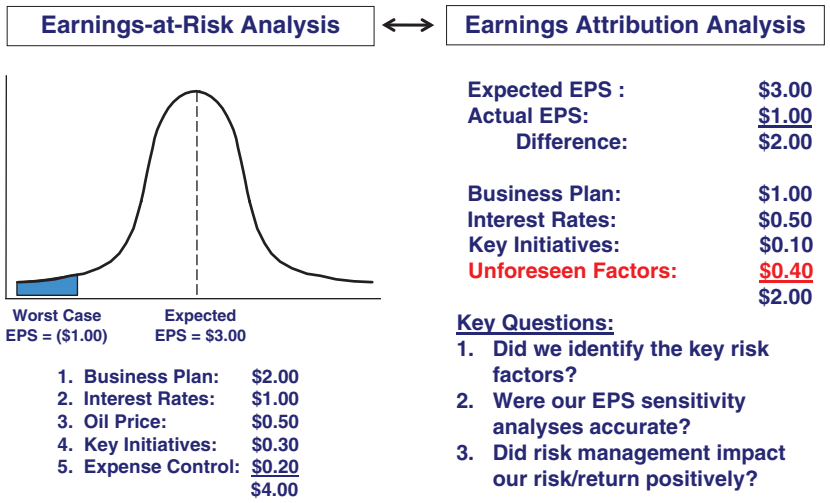


FIGURE 21.3 Example of an Earnings Volatility Analysis

ERM MATURITY MODEL

Previously, we discussed the four building blocks for ERM implementation. However, a company cannot expect to establish these risk management practices all at once or even over a short period of time. ERM is often a multi-year effort. As such, it is helpful for each company to develop an ERM roadmap for the future, articulating where they are, where they want to be, and how they are going to get there. Of course, the ERM road map should be customized for each company based on their current state, future vision, business and regulatory requirements, and available resources. As the ERM roadmap is developed, it is helpful to review the key benchmarks by way of an ERM Maturity Model. The purpose of the ERM Maturity Model is to provide specific industry benchmarks of ERM practices so companies can self assess the maturity and development opportunities of their ERM programs. Since these are general industry benchmarks, it is possible that an organization may have specific ERM practices from a more advanced stage before completing all of the practices in prior stages. Figure 21.4 provides an overview of the five stages of the ERM Maturity Model. Let's review the practices and benchmarks for each stage.

Stage 1: Definition and Planning (White Belt)

In Stage 1 the organization is organizing resources to define the scope and objectives for its ERM program. Key objectives during this phase include

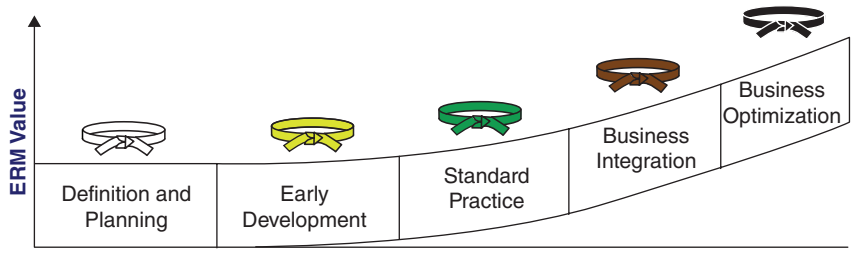


FIGURE 21.4 ERM Maturity Model

identifying an organization's ERM requirements, obtaining board-level and executive support, and developing an overall framework and plan for ERM. Some organizations find it useful to establish a cross-functional taskforce in order to accomplish these objectives. Stage 1 may take 6 to 12 months to complete and typical activities include:

- Researching regulatory requirements and industry practices
- Providing risk briefings for board members and corporate executives
- Appointing a chief risk officer and/or ERM project leader
- Organizing an ERM task force and/or ERM committee
- Conducting benchmarking exercises with other companies
- Assessing the current state of risk management capabilities
- Defining the scope, vision, and overall plan for ERM
- Establishing an ERM framework, including a risk taxonomy

Stage 2: Early Development (Yellow Belt)

In Stage 2 the ERM program is in the early stages of development. Key objectives during this stage include formalizing roles and responsibilities in an ERM policy, identifying key risks through risk assessments, and providing risk education to enhance risk knowledge and awareness. Stage 2 may take one to two years and typical activities include:

- Establishing an ERM policy, which includes roles and responsibilities
- Performing annual risk assessments across business units
- Coordinating risk identification and control processes across risk, audit, and compliance functions
- Providing risk education for the board of directors, as well as risk training for a wider group of employees
- Establishing risk functions across the business units

The development of the ERM policy is arguably the most important aspect at this point, since it sets the stage for the company's movement through the rest of the maturity model. Following the ERM implementation requirements, a standard ERM Policy should include:

- *The Executive Summary* provides the purpose, scope, and objectives for ERM
- *The Statement of Risk Philosophy* discusses the overall approach to risk management, as well as guiding risk principles
- *The Governance Structure* summarizes board committees and charters, management committees and charters, and roles and responsibilities
- *Risk Tolerance Levels* provide a statement of risk appetite, including key risk limits and tolerance levels for critical risk exposures
- *The ERM Framework and Processes* section summarizes the ERM framework, as well as specific requirements across overall risk management
- *Risk Categories and Definitions* provide a risk taxonomy for commonly used terms and concepts

Defining risk tolerance levels may be initially difficult. An organization can establish risk tolerances using different approaches ranging from judgment to quantitative tools—these methods are not mutually exclusive. For instance, risk tolerances might be established as a percentage of quarterly earnings or equity capital, or be model-driven (e.g., through value-at-risk, economic capital, or simulation analysis, to name a few). Regardless, the board and management should ensure that their chosen tolerance levels adhere to regulatory requirements. It may also prove useful to conduct industry benchmarks to see where direct competitors are standing.

Stage 3: Standard Practice (Green Belt)

In Stage 3 the organization is establishing more timely and granular risk analyses. Key objectives during this stage include performing more frequent risk assessments and developing risk quantification processes. This stage may take one to three years and activities may include:

- Updating risk assessments on a quarterly or monthly basis
- Developing risk databases, including loss-event information
- Developing KRIs and reporting on enterprise-wide risks on a monthly basis
- Integrating credit risk and market risk models, and building operational risk models
- Developing risk-adjusted performance measurement methodologies

Stage 4: Business Integration (Brown Belt)

In Stage 4 the focus is on integrating ERM into business management and operational processes. ERM tools and practices become more distributed throughout the organization. It is during this stage that risk and return tradeoffs in business decisions are evaluated more explicitly. Key objectives include quantifying the cost of risk to support pricing and risk transfer decisions, assessing business risks up front as part of business and product development, developing automated risk reporting and escalation technologies, and linking risk and compensation. Stage 4 may take two to four years and include the following activities:

- Expanding the scope of ERM to include business risk
- Allocating economic capital to underlying market, credit, operational, and business risks
- Incorporating the cost of risk into product and relationship pricing, as well as portfolio management and risk transfer strategies
- Integrating risk reviews into new business and product approval processes
- Automating ERM reporting through the use of electronic dashboards, including customized queries and real-time escalations
- Establishing trigger points to make timely business decisions, including risk mitigation and exit strategies
- Developing feedback loops on risk management performance
- Linking risk management performance and executive compensation

Stage 5: Business Optimization (Black Belt)

In the most advanced stage, ERM is applied to optimize business performance and enhance relationships with key stakeholders. Key objectives in Stage 5 include integrating ERM into strategy development and execution, maximizing firm value by optimizing risk-adjusted profitability, providing risk transparency to key stakeholders, and helping customers manage their risks. Stage 5 is an ongoing process and may include the following activities:

- Expanding the scope of ERM to include strategic risk
- Integrating ERM into strategic planning processes
- Maximizing firm value by actively allocating organizational resources at the efficient frontier
- Providing risk transparency to key stakeholders—as discussed in Chapter 11—with respect to current risk exposures and future risk drivers
- Leveraging risk management skills, tools, and information to deepen customer relationships by helping them manage their risks

Given the above benchmarks, and my research and review of published research, I would estimate the following for companies involved in ERM:

- 20 percent of companies are in Stage 1—Definition and Planning (White Belt)
- 40 percent of companies are in Stage 2—Early Development (Yellow Belt)
- 20 percent of companies are in Stage 3—Standard Practice (Green Belt)
- 15 percent of companies are in Stage 4—Business Integration (Brown Belt)
- 5 percent of companies are in Stage 5—Business Optimization (Black Belt)

OTHER ERM MATURITY MODELS

Various professional organizations and consulting firms have created other versions of the ERM Maturity Model. For example, McKinsey & Company has developed a risk maturity system with four stages. Firms in the first stage of initial transparency comply with basic risk management guidelines—this only helps them to reduce losses from minor unexpected setbacks. In the second stage of "systemic risk reduction," firms have professionalized risk management, which provides the stability for further growth, as well as the ability to avoid "large loss events." In the third stage, firms become competitive with industry standards, which allow them to navigate trade-offs, as well as improve their Return on Equity (ROE) requirements. Once a firm reaches the fourth and final stage of this risk maturity system, top management is wholly focused on "risk-adjusted performance."[9]

Deloitte has a maturity model that consists of five stages. The first stage begins with planning, in which risk management is mainly reactive, and depends primarily on the individual capabilities and sharp wits of experienced employees. During the second stage, titled "Siloed," risk management is given structure, in terms of alignment with strategy, though little attention is paid to the links between risks (a traditional departmental approach to risk). In the third "comprehensive" stage, the company has a defined ERM function with dedicated risk professionals, and risk is implemented into end-to-end business processes. The fourth stage is "integrated," in that the interdependencies of risk are analyzed. At this stage, the company also begins to rely on sophisticated risk models. During the last stage, the company becomes "optimized," using early warning indicators to preempt policy violations. Discussion of risk is fully embedded into strategic planning, capital allocation, product development, and the like.[10]

RISK CULTURE

As companies move up in ERM maturity, one of the core issues that the board, senior executives, and regulators are most concerned about is risk culture. What is risk culture? I am often asked by clients and conference audiences to give some hallmarks of good versus bad risk cultures. My reply would often begin with the following:

- In a typical risk culture, people will do the right things when risk policies and controls are in place. They do what they are instructed and trained to do.
- In a good risk culture, people will do the right things even when risk policies and controls are *not* in place. They do what is in the best interest of the company and its stakeholders.
- In a bad risk culture, people will not do the right things regardless of risk policies and controls. They do what is in their own best interest.

The risk culture of a company is an intangible but powerful force that shapes the values, beliefs, norms, and ultimately the risk management behavior of individuals and groups within an organization. Many observers argue that the financial crisis of 2008, the effects of which are still rippling strongly today, was caused by failures in the risk cultures at banks. As an example, these observers would point to the change in culture and risk-taking at investment banks as they converted from private partnerships to publicly traded companies. Would they have acted the same way if they remained private firm and the partners' capital and reputations were on the line?

Given the importance of risk culture, a growing number of companies are conducting risk culture assessment to monitor this intangible but important component of ERM. Risk culture can be affected by—and thus assessed through—a multitude of factors, which include the following:

- *Tone from the top:* Do the company's board members, CEO, and other business leaders set the right tone from the top with respect to their commitment to risk management? Do business leaders (and other key influencers) exhibit the appropriate behavior?
- *Risk awareness:* Are employees throughout the company aware of the key risks, as well as their individual accountabilities for risk assessment and management? Does the company provide the appropriate training and development programs?

- *Organizational incentives:* What are the company's incentive compensation practices, and to what extent is risk management considered? Do rising executives and employees exemplify the appropriate risk management behavior?
- *Change management:* Does the company explicitly address change management issues as part of their ERM build out? Does the ERM function present a clear vision, roadmap, and rationale?
- *Communication and escalation:* Does senior management effectively communicate risk management policies and expectations? Is healthy inquiry and debate on critical risk management issues encouraged? Do employees feel comfortable in escalating critical risk management issues in a timely manner, or is there fear of the shoot the messenger syndrome?

It is important to understand how each of the building blocks of ERM implementation will shape risk culture. In the subsequent chapters, we will discuss each of the four ERM implementation requirements further—the role of the board, risk assessment, risk-based decision making, and dashboard reporting and monitoring.

CHAPTER 22

Role of the Board

A transformation is under way at boards of directors with respect to their role in ERM. In the wake of the global financial crisis of 2008, boards are taking a much more active role in risk oversight. They are reexamining governance structure and roles, risk policies and limits, as well as assurance and reporting processes.

This change indicates a very significant and positive shift in the way corporate boards oversee risk management. Of the key groups that provide independent risk monitoring—boards, auditors, regulators, rating agencies, and institutional investors—the board of directors is the only group with both the direct responsibility and the greatest leverage in ensuring that sound risk management is in place.

At most organizations, corporate management would bend over backward to satisfy board demands. By asking tough questions and establishing board expectations with regard to ERM, the board can set the tone from the top and effect significant change in the risk culture and practices of an organization. Recent surveys have reported that board members recognize the importance of ERM, and even indicate that risk management has replaced accounting issues as the top board concern. For instance, accounting firm Eisner LLP conducted a study in 2010 of more than 100 directors sitting on a variety of cross-industry boards. It revealed that directors ranked both risk assessment and the incorporation of financial models into strategic decision-making processes higher than accounting, in terms of level of interest.[1]

BOARD OVERSIGHT REQUIREMENTS

More importantly, board members recognize that they can play a more effective role in risk oversight. Based on a survey of more than 200 board members, a December 2010 report commission by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) indicated that

71 percent of respondents acknowledged that their boards "are not formally executing mature and robust risk oversight processes."[2]

It is evident that board members are setting higher expectations and requirements for risk oversight. They are not alone. In December 2009, the Securities and Exchange Commission (SEC) established new rules that require disclosures in proxy and information statements about the board governance structure and the board's role in risk oversight. These disclosures also include the relationship between compensation policies and risk management, as well as the extent to which executive compensation may lead to excessive risk taking. These requirements also highlight the necessary qualifications of directors and nominees, in addition to the role that diversity plays in director nominations. The SEC designed these rules to enhance transparency around the role of the board in risk oversight.

In July 2010, the Dodd-Frank Act was signed into law. It requires that a board risk committee be established by all public bank holding companies (and public non-bank financial institutions supervised by the Federal Reserve) with more than $10 billion in assets. The board risk committee is responsible for ERM oversight and practices, and its members must include "at least one risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms."

The Federal Reserve Board may also require a risk committee at smaller publicly traded bank holding companies. There are parallels between Section 165 of the Dodd-Frank Act and Section 407 of the 2002 Sarbanes-Oxley Act (also known as the Public Company Accounting Reform and Investor Protection Act), which called for the creation of audit committees staffed by independent directors and at least one "financial expert." However, unlike the Sarbanes-Oxley rules that define the attributes of a financial expert,[3] the Dodd-Frank Act does not provide specific criteria on what would qualify a board member to be a risk expert—we'll discuss this issue more later.

In December 2010, global banking regulators established Basel III to improve capital adequacy, stress testing, and risk management practices with respect to counterparty, liquidity, and systemic risks. Basel III was specifically designed as a response to the deficiencies in financial regulation during the 2008 financial crisis. The new Basel III requirements will significantly increase the capital and liquidity costs for banks with more than $50 billion in assets. Basel III will also impact the capital management practices and dividend policies throughout the banking industry.

The combined impact of Dodd-Frank, the SEC, Basel III, and other regulatory requirements has far-reaching implications for the overall profitability of banking institutions. A key impact is that these regulatory requirements have created significant demand for bank directors who can assist the board in overseeing complex risks and regulatory requirements, as well as

help executive management in formulating the appropriate business strategies and plans.

CURRENT BOARD PRACTICES

What are the current industry practices in board risk governance? To answer this question, James Lam & Associates, in collaboration with Odgers Berndston, conducted research on the top 100 U.S. banking institutions. Coincidentally, there are almost exactly 100 banks with more than $10 billion in assets, which is the Dodd-Frank threshold for requiring a board risk committee.

As shown in Figure 22.1, the money center banks with more than $1 trillion in assets all have risk committees of the board. They also all have a chief risk officer (CRO) who supports the board risk committee with respect to risk assessment and reporting. For large national banks with between $100 billion and $1 trillion in assets, 71 percent had a board risk committee and 78 percent had a CRO. For large regional banks with between $50 and $1 billion in assets, 88 percent had a board risk committee and 76 percent had a CRO. For regional banks having between $10 and $50 billion in assets, only 55 percent had a board risk committee and 58 percent had a CRO.

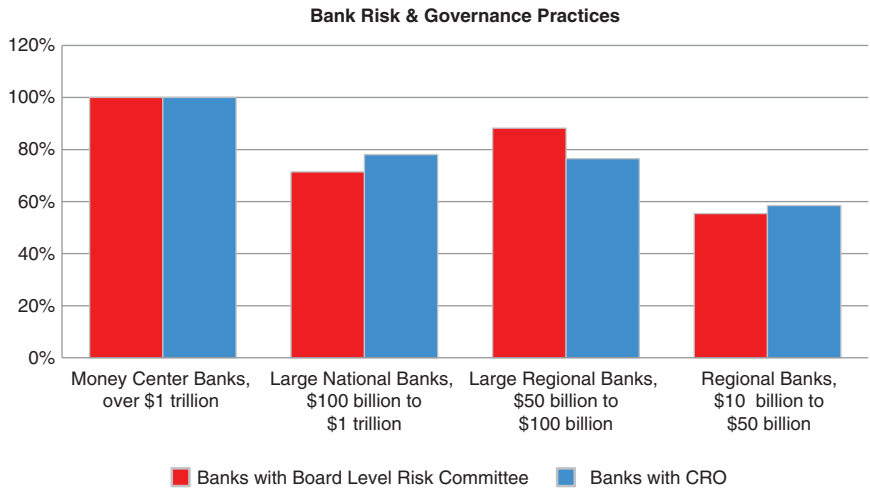


FIGURE 22.1 Percentage of Banks with Risk Committees and/or CROs
Source: James Lam & Associates, Odgers Berndston, 2012

Based on the regulatory requirements discussed above, it is expected that 100 percent of these banks will establish a board risk committee in the next one to two years. It is also likely that nearly all of these banks will have a CRO, given the high correlation between having a board risk committee and a chief risk officer.

It becomes apparent that the presence of directors with significant experience in risk management on the board is an indispensable necessity. What are the credentials found at bank boards today? Researchers from James Lam & Associates reviewed the professional biographies of more than 1,200 directors at the top 100 U.S. banks. Our research and analyses produced the following observations:

- On average, there are 12.7 directors on each bank board.
- Currently 44 percent of bank boards have at least one director who may be considered a risk expert. That means the boards of 56 percent of the top 100 U.S. banks must add one or more risk professionals to their ranks to satisfy Section 165 of the Dodd-Frank Act.

As shown in Figure 22.2, the research found the following distribution of board-member credentials:

- A significant portion of bank board members come from CEO (47 percent), CFO (20 percent), and COO (7 percent) backgrounds.

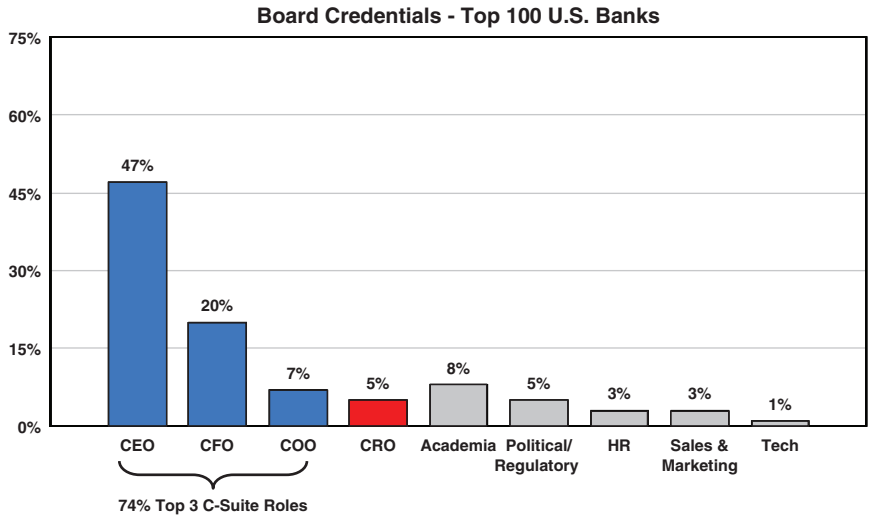


FIGURE 22.2 Distribution of Board Member Credentials
Source: James Lam & Associates, Odgers Berndston, 2012

- Only 5 percent come from CRO or risk backgrounds.
- Other backgrounds include academia (8 percent), political or regulatory entities (5 percent), human resources (3 percent), sales and marketing (3 percent), and technology (1 percent).

Given the above findings, and in order to meet regulatory requirements, the number of risk professionals on the boards of the top of 100 U.S. banks should more than double over the next few years.

As bank boards add risk professionals to their ranks, which skills and experiences should they look for? The Dodd-Frank requirement specified that the risk committee must have "at least one risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms." However, beyond meeting regulatory requirements, banks should recruit directors who can add strategic value to the institution. As such, bank boards should consider the following criteria in their selection process:

- An understanding of risk governance and management practices at banks, including board risk oversight, risk policy and appetite, monitoring and assurance processes, and risk reporting and disclosure requirements.
- Experience as a chief risk officer, and/or actively a chief risk officer, at a large, complex financial institution.
- Knowledge of banking regulations and standards, such as Dodd-Frank, Basel II and III, SEC, FDIC, OCC, and Federal Reserve requirements.
- Working experience in identifying, assessing, and managing the key risks faced by financial institutions, including strategic, business, market, liquidity, credit/counterparty, operational, and systemic risks—plus experience in integrating strategy and risk oversight.
- Knowledge of ERM, including assessment of cross-risk interdependencies and aggregate risk profiles, and the ability to oversee the CRO's implementation of the ERM program.
- Ability to lead or advise the board on major risk governance and policy issues, as well as guide or challenge management on recommended risk strategies, plans, and assumptions.
- Experience in overseeing or executing applications of key risk management tools, including value-at-risk, economic capital, risk-adjusted pricing and profitability models, risk-control assessments, stress testing, and scenario analysis.
- Understanding of both the usefulness and limitations of the above tools, in addition to a solid understanding of derivatives and hedging strategies.

The Directors and Chief Risk Officers Group recently published a white paper entitled "Qualified Risk Director Guidelines" that provided risk director standards with respect to professional experiences, personal attributes, business acumen, and education.[4] According to these standards, directors should be able to act assertively, independently, and with integrity, putting the interests of the company above their own personal interests. The ability to assess multiple outcomes simultaneously is also a crucial characteristic of a competent director. Business acumen is, of course, also of paramount importance; directors should have substantial experience in managing a wide variety of risk, including financial, operational, technological, or market risks, among others. They should be capable of thinking in the long term and so assess risks not only in the context of their potential consequences today, but also in the future. In addition, directors need a background of rigorous education that helps to prepare them for the complex needs of the organization—this education should include some form of specific governance or director training.

Now let's examine the case of JP Morgan Chase—a bank that was widely recognized as a best-practice in risk management. However, that reputation has been tarnished recently,[5] and the bank has been criticized for not having directors with deep risk and banking experience on the board's risk committee.

CASE STUDY: JP MORGAN CHASE

JP Morgan Chase, an investment banking giant and one of the largest banks in the United States, relies on its Chief Investment Office (CIO) for keeping an eye on investment risks. However, in 2012, the firm faced a US$2 billion trading loss that eventually ballooned to around $6.2 billion. A London-based JP Morgan Chase trader, Bruno Iksil—not so affectionately nicknamed the 'London Whale'—made a series of large bets in the debt markets on the recovery of the economy through a rise in the value of corporate bonds. JP Morgan Chase incurred heavy losses when it cut back on these trades.

In truth, Iksil's bets fit in with what seemed to be a general change in the company's attitude toward risk. For example, in early 2012, JP Morgan Chase reduced the funds it put into trades that would protect it from negative market shifts, and instead began to sell credit-default swaps (CDSs). Essentially, JP Morgan Chase was looking to make profits on the "financial health of certain companies."[6]

At the same time, the bank's CIO group altered the company's value-at-risk to more than double its value-at-risk in 2011, which meant

that the bank was increasing its risk appetite in a very short time frame. The bank also tweaked its derivative valuation methods, masking the true amount of risk it was taking on from shareholders. Looking back, CEO James Dimon said that the bank's strategy was "flawed, complex, poorly reviewed, poorly executed, and poorly monitored."[7]

Even after the London Whale incident, JP Morgan Chase's CIO group was allowed to continue expanding the bank's risk appetite, "[blowing] past risk limits and advisories more than 330 times in four months."[8] For example, Ina Drew, head of the CIO at the time, admits to being aware that the company's portfolio had been in violation of risk limits for more than 71 days, though she did not appear to try and stop the portfolio's accelerated growth. Both internal and external audits revealed that risk limits were simply shifted higher to give traders like Bruno Iksil more freedom.

Although the bank's overall performance was not set back by much—it earned $5.38 billion in the first quarter of 2012—it has suffered a reputational impact. Dimon was often touted as the "King of Wall Street" for his sound judgment, but his crown has slipped somewhat after this fiasco. In an investors conference call on April 13 of 2013—a month before the company's losses were publicly disclosed—Dimon dismissed the incident as a "tempest in a teapot," downplaying the significant implications and consequences it had in terms of financial loss and risk management concerns. Later investigations revealed that Dimon was, at the time, already aware of the substantial losses caused by the London Whale, and their continued growth.

The incident also highlighted some issues regarding the members of JP Morgan Chase's risk committee, none of whom had deep risk or recent banking experience. In the aftermath of the London Whale, the bank issued a statement supporting the current board members: "The company strongly endorses the re-election of its current directors . . . The members of the board's risk committee have a diversity and breadth of experiences that have served the company well."[9] While the ISS Proxy Advisory Services have identified three board members—David M. Cote, Ellen V. Futter, and James Crown—as particularly unqualified in terms of risk management experience, a review of the risk committee biographies reveals that the members seem to be lacking in terms of risk and banking expertise:

- James A. Bell served as the Executive Vice President of Boeing
- David M. Cote is the leader of Honeywell International, a diversified industrial firm
- James S. Crown is the President of a private investment company

- Timothy P. Flynn was Chairman of KPMG International
- Ellen V. Futter is the president of the American Museum of Natural History

Lee Raymond, the board's presiding director, defended the company against questions about why director positions were given to executives from industries that were unrelated to finance by highlighting the difficulties of "finding qualified board members who were not conflicted from serving."[10] Since the London Whale incident, JP Morgan Chase has undergone some significant changes, with a turnover of nine top executives leaving the bank, though Ellen Futter, David Cote, and James Crown were narrowly re-elected by shareholders during the bank's annual meeting in May of 2013. However, Futter and Cote have since resigned.[11] During that same annual meeting, shareholders also voted against splitting the CEO/chairman role.

JP Morgan Chase's lapses in judgment also had larger implications for the entire banking industry. To the dismay of most banks, the London Whale incident only seemed to fortify the need for stricter regulation—for example, in the form of the Volcker rule, which was being polished that year. Dimon regretfully noted that the incident "[played] right in to the hands of a whole bunch of pundits out there . . . We will have to deal with that—that's life."[12]

THE LAST LINE OF DEFENSE

To put the role of the board in context, and to provide clarity to risk governance structure and roles, companies should consider adopting the three lines of defense model that is commonly used in the financial services industry. This model organizes risk management into a hierarchal, role-based structure, as follows:

- First line of Defense: Business and operating units
- Second line of Defense: CRO and ERM function (and Compliance)
- Third line of Defense: Board of Directors (and Internal Audit)

Let's briefly look at the first two lines of defense before focusing on the role of the board of directors as the cornerstone of this chapter.

The First Line of Defense

The first line of defense is made up of the business units and operating units (including all profit centers and support units such as IT and HR). They perform day-to-day business processes and support operations,

and as such are at the forefront of risk management. They are ultimately accountable for measuring and managing risk within their unit. For example, business units must assume risk in order to generate profits and growth. In this process, they make daily decisions about which risks to accept and which to avoid. Of course, these decisions should be in line with the company's risk appetite, which is established by the board of directors—we will consider this later, when we discuss the third line of defense. Business units are responsible for executing customer management, product development, and financial plans, as well as monitoring and mitigating resulting risks at a tactical level. Moreover, they are accountable for product pricing. Without the proper incorporation of risk in the pricing process, the firm may not be fully compensated for the risks that it chooses to take on.

The Second Line of Defense

The second line of defense consists of the Chief Risk Officer (CRO), and the ERM and compliance functions. One of their primary duties is to establish and implement risk and compliance programs. These programs include policies that will guide and constrain the decision-making processes of the business units. The second line of defense supports corporate management by establishing the infrastructure and best-practice standards for ERM. This includes developing risk policies and procedures, analytical models, and data resources and reporting processes. The ERM and compliance functions are also held accountable for ongoing risk monitoring and oversight—particularly concerning safeguarding of the company's financial and reputational assets and ensuring compliance with laws and regulations.

The Third Line of Defense

The third line of defense is the board of directors, with the support of the risk and audit committees—the focus of this chapter. As an industry standard, the audit committee usually serves as the third line of defense by itself, but I argue that committees like audit and risk do not have the skill, experience, or mandate necessary to perform this high-level function. Consider the failure of banks such as Lehman Brothers in 2008. While these institutions did have risk management processes in place, they did not capture the subtle, inherent dangers of credit exposure to a single market. This shows how internal auditors may be too focused on putting the company's risk processes through stringent tests and checking minute details to see the bigger picture—which can potentially lead to devastating consequences.

As such, more engaged involvement of the board of directors is needed here to provide direction and perspective on the ERM process. We can categorize the responsibilities of the board as follows:

- *Governance*. Establish an effective governance structure to oversee risk. How should the board be organized to oversee ERM? What is the linkage between strategy and risk management? How can the independence of the risk management function be strengthened?
- *Policy*. Approve and monitor an ERM policy that provides explicit risk tolerance levels for key risks. Do risk management policies and risk tolerance levels effectively capture the board's overall risk appetite and ERM expectations? What is the linkage between risk policies and compensation policies?
- *Assurance*. Establish assurance processes to ensure that an effective ERM program is in place. What are the performance metrics and feedback loops for ERM? How to improve the structure and content of board reports? How should that assurance be disclosed to investors, rating agencies, and regulators?

Let's examine these responsibilities in turn.

Governance It is evident that a fundamental step in providing ERM oversight is to establish an effective risk governance structure at the board level. Beyond the organizational chart, risk governance delineates the oversight roles and decision points for the board and board committees, as well as the relationships with management and management committees. Common issues related to board risk governance include:

- Fragmented and/or ambiguous risk oversight responsibilities across the full board and various subcommittees
- Insufficient risk experience and expertise among board members
- Inconsistencies between the board and management governance structures, or unclear separation of roles
- Lack of integration between strategy and risk management
- Weak independence for the chief risk officer and/or the risk management functions

While the full board generally retains overall responsibility for risk oversight, a growing number of organizations are establishing risk committees. Based on the COSO Report, 47 percent of board members at financial services organizations indicated that they had a risk committee, versus 24 percent at nonfinancial services firms. Given the Dodd-Frank Act and other regulatory reforms, it is likely that these percentages will

increase in the next few years. Regardless of the committee structure, the risk oversight roles of the full board and committees (for example, audit, governance, and compensation) should be clearly defined. Boards should also ensure that they can effectively challenge management on risk issues by appointing board members and/or board advisors with deep risk management expertise. General risk education should also be provided to all board members.

The risk governance structures at the board and management levels should also be fully aligned. This alignment encompasses committee charters, roles and responsibilities, reporting relationships, approval and decision requirements, and information flows. As boards become more active in establishing risk policies and risk appetite, the role of the board versus the role of management should be differentiated with increasing clarity.

Monitoring the organization's strategy and execution has long been the purview of boards. As boards become more active in ERM, the integration of strategy and risk is a logical and desirable outcome. Independent research studies have found that when publicly traded firms suffer a significant decline in market value, 60 percent of the loss events were caused by strategic risks, 30 percent by operational risks, and 10 percent by financial risks. While integrated strategy and risk oversight is arguably a key role for the board, this process is still in its early stage of development. According to the COSO Report, fewer than 15 percent of board members indicated that they were fully satisfied with the board's processes for understanding and challenging the assumptions and risks associated with the business strategy.

Independent risk management is also a core tenet for ERM. The board must ensure that risk management is independent of the business and operational activities of the organization. This includes formalizing the reporting relationship between the chief risk officer and the board or board risk committee. Moreover, under exceptional circumstances (for example, excessive risk taking, major internal fraud, or significant business conflicts), the chief risk officer should be able to escalate risk issues directly to the board without concern about his or her job security or compensation.

Many of the common issues we listed at the beginning of this section stem from two major ambiguities that remain pertaining to the role of the board within the context of the organizational hierarchy:

1. The uncertainty with regard to the necessity of an independent risk committee
2. How to separate the roles and responsibilities of the board and management

A recent cross-industry McKinsey white paper demonstrates that while 96 percent of directors agreed that risk management should be a responsibility of the board, 66 percent of directors said that risk management is delegated to the audit committees—only 21 percent of directors see the need for a "separate risk committee."[13] However, as we have noted before, the financial sector has a much higher occurrence of sophisticated ERM programs, with independent, functional risk committees.

I would recommend that firms clearly define the roles of the board and of management to avoid overlap. Otherwise, the board might be too involved and start to encroach on the territory of the management, or be too passive and not engaged enough. Table 22.1 outlines the key differences between their responsibilities with respect to each aspect of ERM implementation.

An important factor to consider in delineating distinct functions for the board and for the management is that the board represents the interests of shareholders, among other stakeholder groups. As such, while management is responsible for operating the company, the board of directors is present to supply effective oversight, and to engage in credible challenge with respect to management's strategies and plans. In terms of risk management, the board of directors should provide assurance that the existing processes are effective, and, if necessary, initiate new processes.

TABLE 22.1 The different responsibilities of the board and of management

ERM Component	Executive Management	Board of Directors
Risk Governance	Establish management structure and roles	Establish board structure and roles
ERM Vision and Plan	Develop and implement	Support vision; track progress against plan
Risk Tolerance Levels	Establish and conform	Debate and approve
Risk Policies	Develop and implement	Approve and monitor
Business and Risk Strategies	Formulate and execute	Challenge key assumptions; monitor execution
Critical Risks	Manage and measure; optimize risk/return	Provide input and oversight
Risk Reports	Provide context, analysis, and key points	Monitor key exposures, exceptions, and feedback loops
Risk Analytics	Provide qualitative and quantitative analyses	Obtain ERM assurance; conduct board assessments

Policy While risk governance provides the organization with risk management and oversight, the board needs an instrument for communicating its expectations and requirements. Board-approved risk policies represent a critical tool in this regard. As shown in the table, management's responsibility is to develop and execute risk management policies. The board's role is to approve the policies and monitor ongoing compliance and exceptions. Common issues related to risk policies include:

- Absence of explicit limits or tolerance levels for key risks
- Lack of standards across different policies for ERM, credit risk, market risk, operational risk, and so on
- Insufficient reporting and monitoring of policy exceptions and resolutions
- Key policy components are missing, or obscured by detailed procedures

To establish effective risk policies and address the above issues, the board should communicate its expectations and standards with respect to risk policy structure and content. For example, an ERM policy may include the following components:

- *Executive summary:* The executive summary provides a concise description of the purpose, scope, and objectives for ERM. It may also provide a high-level summary of the key limits and risk tolerance levels.
- *Statement of risk philosophy:* The statement of risk philosophy discusses the overall approach to risk management. It should also include guiding risk principles that articulate the desired risk culture of the organization.
- *Governance structure:* The section on governance structure summarizes board committees and charters, and roles and responsibilities. Additionally, it should delineate the delegation of authority, including risk management and oversight responsibilities for key individuals.
- *Risk tolerance levels:* This section provides a statement of risk appetite, including specific limits or tolerance levels for critical risk exposures. It also provides exception management and reporting requirements.
- *Risk framework and processes:* This section summarizes the ERM framework, as well as key processes and specific requirements for overall risk management.
- *Risk policy standards:* This section discusses policy standards for all other risks so that the structure and content of risk policies are consistent across the organization.
- *Risk categories and definitions:* This section provides a taxonomy for commonly used risk terms and concepts, facilitating a common language for risk discussions.

While its role is to approve and monitor risk policies, the board should actively discuss (if not debate) the risk limits or risk tolerance levels that are appropriate for the organization, including the risk/return trade-offs at various risk appetite levels.

The linkage between risk management and compensation policies should be a top board issue. As one board member remarked, "People don't do what you tell them to do; they do what you pay them to do." As such, the board should ensure that risk management performance is considered in a meaningful way (for example, a 20 percent weighting or more) in executive management performance evaluations and incentives. The criteria may be specific risk management goals or an ERM scorecard that includes various quantitative and qualitative indicators. By incorporating ERM into executive management incentives, the board can have a far-reaching impact not only on management actions, but also on the incentives and actions of all employees.

Articulating the company's risk appetite is an essential element of establishing the ERM policy. Companies should specify the amount of risk that they are willing to take on in pursuit of strategic and business objectives. Oftentimes, the terms risk appetite and risk tolerance are used interchangeably, but some companies have found it useful to distinguish the two terms. For each risk, the risk tolerances define the *maximum* amounts of that risk the company is willing to take on. Risk appetite is a subset of risk tolerance that determines the *desirable* amount of that risk the company wants given risk/return opportunities. While risk appetite statements require the approval of the board before they can be implemented, they are developed and defined by corporate management with the assistance of the CRO.

The development of a suitable risk appetite statement is an important aspect of the governance and risk oversight process, since it helps employees throughout the corporate hierarchy to make risk-based decisions. A typical risk appetite statement, as shown in Figure 22.3, is organized by the company's major risk categories (for example, business risk, market risk, credit risk, operational risk, etc.) each with specific, attributed metrics. Each metric is then assigned a range of acceptable values that the company's activities should be confined to. Not only does this help to integrate risk into strategic planning, it also allows the company to track its risk exposures against risk tolerance levels over time.

It is important to note that risk appetite statements are not meant to capture *all* material risks, since that would make it far too unwieldy and granular. By pinpointing the most crucial risk metrics, the risk appetite statement aims to provide an overall, holistic view of the company's risk profile.

Assurance While risk policies articulate board requirements for ERM, the board still needs information and feedback. How does the board know if

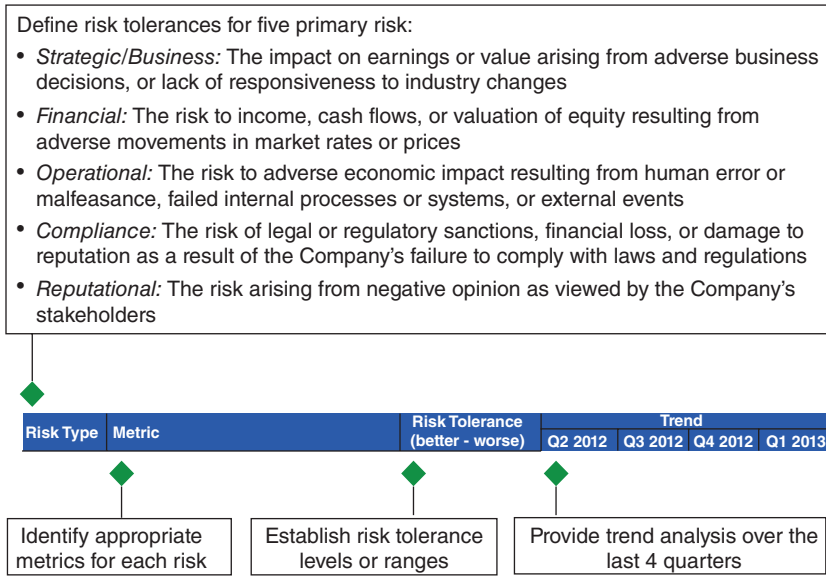


FIGURE 22.3 A Risk Appetite Statement Template

risk management is working effectively? This is perhaps one of the most critical questions facing board members today. The answer lies in the assurance processes established by the organization, including board monitoring and reporting, independent assessments, and objective feedback loops. Common issues related to risk assurance include:

- Ineffective board communication and reporting
- Lack of independent assessments of the ERM program
- Use of subjective indicators to gauge ERM effectiveness

In order to fulfill its mandate to oversee ERM, the board must rely on management to provide critical information with respect to board communications and reports. Board members often criticize the quality and timeliness of board reports. The standards that they want (but are not getting to their satisfaction, or are not getting at all) include:

- A concise executive summary of business/risk performance, as well as the key discussions and decision points for the board
- Management narrative on select data and trends
- Key performance and risk indicators against specific targets or limits
- More discussion with, versus presentation from, management.

Recently, James Lam & Associates worked with a large financial institution to improve its board communication and reporting. In addition to adopting these standards, the financial institution developed an ERM dashboard that allows high-level charts as well as drill-down capability to underlying data.

As boards retain independent auditors to review and provide assurance for the financial statements, they should also retain an independent party to review and provide assurance for the ERM program. The final product of this review may be an assessment of the organization's ERM program with respect to its relationship to best practices and/or its development against plan.

Finally, the board should establish effective feedback loops to gauge the effectiveness of its ERM program. Companies currently tend to evaluate ERM effectiveness based on measurements such as progress toward key milestones, or the number of policy violations, losses, or surprises. While these metrics are useful, such qualitative markers or negative proofs are no longer adequate on their own for a robust ERM system. The board needs to work with management to establish performance metrics and feedback loops for ERM. In Chapter 21, we discussed the use of earnings-at-risk as a feedback loop on ERM.

The ERM scorecard is another example of a feedback loop, which allows the board to measure the effectiveness of ERM in terms of the following:

- *Achievement of ERM development milestones:* Milestones could include drafting an ERM policy, setting risk tolerance levels, drafting a risk appetite statement, etc.
- *Lack of regulatory/policy violations or other negative events.* Directors and executives would generate include "no surprises"—such as regulatory violations and fines, risk limit breaches, customer or reputational events—as a key success factor in ERM.
- *Minimizing the total cost of risk:* The total cost of risk is defined as the sum of expected loss, unexpected loss (or economic capital), risk transfer costs, and risk management costs.
- *Performance-based feedback loops:* These include minimizing unexpected earnings volatility, minimizing variances between ex-ante risk analytics (e.g., risk assessments and models) and ex-post risk results (actual losses and events), and contributions to shareholder value creation.

Regardless of the metrics and criteria, the board should decide on the appropriate feedback loop(s) for risk management.

Board members are not involved in day-to-day business activities, but they have the ultimate responsibility to ensure that an effective ERM

program is in place. What can they do to effectively oversee ERM and the key risks facing the organization? They have three key levers. First, a well-thought-out governance structure should be put in place to organize risk management and oversight activities. Second, risk policies and risk tolerance levels should be established to articulate the board's expectations and risk appetite. Finally, boards should establish assurance processes and feedback loops to gauge the effectiveness of the ERM program.

CHAPTER 23

Risk Assessment

Risk analytics and assessments provide the information to help the board, corporate management, and business and functional leaders to make more informed business and risk management decisions. In Chapter 9 we discussed the risk analytics that can support enterprise risk management (ERM). However, not all risks can be easily quantified and modeled, which is why risk assessments can be useful. The objective of risk assessment is to identify, quantify, and prioritize an organization's key risks to enable more informed business and risk management decisions. Risk assessment principles are well established in industry frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM, the Dey Report, the Turnbull Report, and ISO 31000.[1]

A 2013 KPMG survey[2] of approximately 1,000 C-level, cross-industry executives found that 80 percent of their respondents said their companies perform some form of risk assessment, while only 20 percent had no formal enterprise-wide risk identification strategy at all. Of the 80 percent of respondents that perform risk assessment, the survey found (multiple answers allowed):

- 48 percent of respondents said their company's risk management function performs an annual risk assessment
- 38 percent said that the individual businesses perform a risk-control self assessment (RCSA)
- 34 percent said that risk assessments of all risk and control functions are aligned to establish a complete risk profile

The diversity of the survey's pool of respondents—which includes executives from operations, risk, legal, technology, compliance, and internal audit functions, from all five continents—demonstrates the growing acceptance of risk assessment as a core ERM practice. In this chapter, we will discuss how risk assessment fits into the overall scheme of ERM implementation, as well as methods of applying risk assessment processes so that

they recognize enterprise-wide risks in an integrated manner. Let's begin by looking at the key steps of typical risk assessments:

1. Establish the business context with respect to organizational objectives and regulatory requirements.
2. Identify the key risks that may negatively (or positively) impact the achievement of business objectives.
3. Evaluate the key risks in terms of probability (likelihood of occurrence) and severity (financial and reputational consequences).
4. Evaluate the effectiveness of controls associated with the key risks.
5. Determine the risk management strategies, including accountabilities and action plans.
6. Prioritize the top risks for further analyses, quantification, and risk mitigation.
7. Provide ongoing reporting and monitoring.

The risk assessment steps outlined above require significant time and resources. Most companies implement GRC (governance, risk, compliance) systems to support their risk assessment and reporting processes. In the implementation of ERM programs, it is important to keep in mind the potential benefits of risk assessment, which include:

- Enhanced awareness and transparency of the key risks facing the organization
- Facilitated cross-functional learning and knowledge transfer for the participants
- Improved risk analytics and quantification processes (by targeting these efforts on the most critical risks)
- Enhanced board and management reporting
- Improved business performance through risk-based decision making

While most organizations have already implemented risk assessment programs for many years, there are common issues that may prevent them from achieving the benefits discussed above. These common issues may include:

- Lack of senior management sponsorship and/or business unit support for the risk assessment program
- Inconsistencies in the risk assessment standards that are used over time; and/or the quality of input throughout the organization
- Inability to develop an overall risk profile due to the vast amount of qualitative data, which may be difficult to aggregate, prioritize, and quantify

- Lack of integration with other ERM processes and/or business activities and operations.
- Difficulty in showing tangible business benefits other than compliance with regulatory and corporate requirements

In this chapter, we will discuss the key phases and processes for developing and implementing risk assessment programs. We will also examine the common, related pitfalls and practical solutions related to each phase of risk assessment. At the end of the chapter, a self-evaluation checklist is provided so companies can benchmark their current risk assessment processes.

RISK ASSESSMENT METHODOLOGY

The specific risk assessment methodology should be customized for the business scope, operating complexity, and risk management maturity of an organization. However, there are common industry processes and practices for risk assessment. Figure 23.1 provides an overall process map of the four phases of risk assessment.

The first phase is *foundation setting*. This should include senior-level sponsorship for risk assessment to ensure business unit participation and candor.

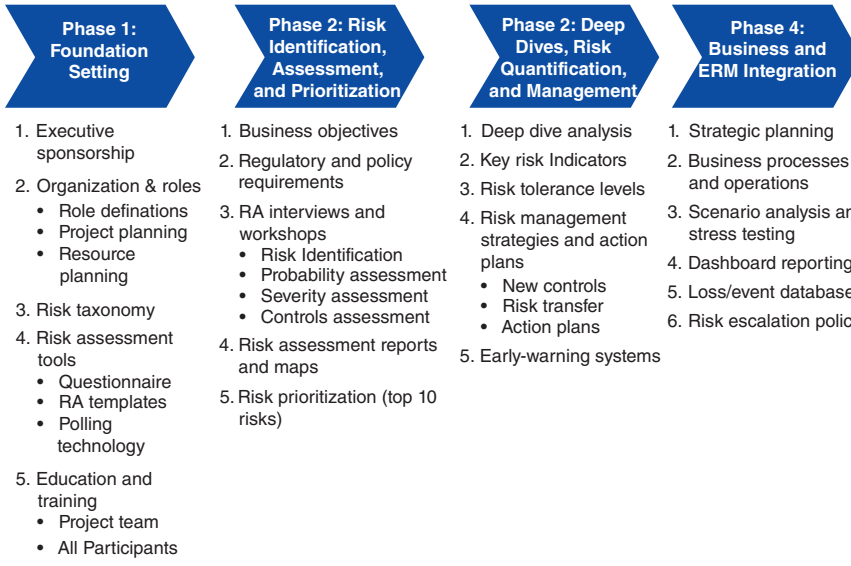


FIGURE 23.1 Risk Assessment (RA) Methodology—Process Map

Other elements include organizing and planning, establishing a risk taxonomy, developing risk assessment tools, and providing education and training.

The second phase is *risk identification, assessment, and prioritization*. This includes establishing the business context in terms of business objectives and regulatory and policy requirements. Given the business context, risk assessment interviews and/or workshops are organized and the key risks are identified, evaluated, and prioritized.

The third phase, *deep dives, risk quantification, and management* includes conducting deep dive analysis, developing key risk indicators, setting risk tolerance levels, and creating risk management strategies and action plans. Such strategies and plans should feature new controls, risk transfer, and guidelines for action in the face of risk. Phase three should also explore early warning systems that can prevent risk events.

The fourth phase, *business and ERM integration*, should include strategic planning, an examination of business processes and operations, scenario analysis and stress testing, dashboard reporting, the creation of a loss/event database, and the production of a comprehensive risk escalation policy.

Let's review each of these phases in turn.

Phase 1: Foundation Setting

The foundation setting phase provides the essential support elements for risk assessment, including senior executive sponsorship, organization and planning, key documents and tools, and education and training. The absence of any of these elements may hinder the efficiency and effectiveness of the risk assessment process.

Executive Sponsorship At the start of the risk assessment cycle, a senior-level sponsor (e.g., CEO, CFO, or CRO) should communicate the board's and executive management's commitment to the risk assessment process, the key objectives and expected benefits, and the expected timeline and milestones. Given the time constraints and other priorities business managers face, it can be difficult to get their full, candid input without senior-level sponsorship. The project sponsor and other corporate leaders should also lead by example by engaging in the risk assessment process and being straightforward in their assessment of risk and control issues. For example, consider Alliant Energy, an energy company in Madison, Wisconsin. Joel Schmidt, Chief Audit, Ethics, and Compliance Officer, leads an annual risk assessment accompanied by a monthly outlook process and discussions between the Vice President of Strategy and Risk and the Board of Directors that occur roughly eight times per year. By frequently discussing risk, Schmidt aims to establish a culture where risk assessment is the basis for operation.[3]

Organization and Roles An overall risk assessment plan should be established in terms of specific tasks, accountabilities, and deadlines. Key roles may include a project sponsor to provide senior management commitment and organizational resources, a project manager to execute the risk assessment project, subject matter experts to provide risk management and technical expertise, a trained facilitator to assist in managing the meetings and discussions, and risk analysts to capture, organize, analyze, and report on the risk assessment results.

Risk Taxonomy The risk taxonomy provides the standard categories and definitions of risk. If a risk taxonomy is not already in place, the project team should develop one to establish a common language in support of effective risk discussions. These categories and definitions should be specific to the company's business profile, but general categories may include strategic risk, business risk, financial risk, operational risk, and legal/compliance risk. In addition to risk types and events, the risk taxonomy should provide clear explanations of key terms and concepts such as probability, severity, risk tolerance levels, and so on. It is also useful to develop subcategories and definitions of risk, as well as examples of actual or potential risk events. For example, subcategories of financial risk may include interest rate risk, foreign exchange (FX) risk, equity risk, commodity risk, liquidity risk, borrower risk, and counterparty risk.

Risk Assessment Tools Some companies have acquired vendor products to support risk assessment, while others develop their own customized processes. Regardless, in preparation for the risk assessment interviews and workshops, the project team should have risk assessment tools, such as a questionnaire for executive interviews, risk assessment templates, and polling technology for the workshops. These tools should be customized for the risk assessment participants. For example, senior executives and board members tend to discuss risk management issues through real-life stories and examples. As such, it may be inappropriate to limit their input by using a standardized template. For executive and board member interviews, it may be more useful to ask open-ended questions in order to facilitate a fuller and more contextualized discussion of the risk issues. An example of questions that may be used for these interviews is shown in Figure 23.2:

Education and Training The foundation-setting process should include education and training sessions for all participants. The project team should be trained on industry best practices for implementing risk assessments, analyzing and aggregating risk assessment results, and providing analyses and reports to management and the board. Other participants should be trained

1. Please summarize the scope of the business or operating unit that you are representing
2. Review the key short-term and long-term business objectives for your business unit
3. Looking back, discuss the major losses, incidents, or near-misses that concerned you the most
4. Looking forward, identify the main risks faced by the company and your specific business unit, including estimated probabilities and consequences
5. Discuss the key controls associated with these main risks (e.g., risk policy and tolerance levels, processes and systems, risk mitigation strategies)
6. Discuss the metrics and reporting associated with these main risks
7. Identify other relevant issues that we have not discussed

FIGURE 23.2 Example of Risk Assessment Executive Questionnaire

on the role of risk assessment in ERM, how they can best participate and contribute, and how they can apply the risk assessment results to mitigate risks and enhance business performance.

In the foundation setting phase, the common pitfalls and practical solutions include:

- *Lack of senior management participation:* As part of the project planning process, senior executives should commit their time to participating in the process. Senior executives should not only be the audience for the risk assessment in terms of receiving the final risk assessment reports, they should be active participants. In addition to communicating executive sponsorship as discussed above, senior management engagement can provide useful input on key risks and controls. As with any enterprise-wide initiatives, there is a high level of correlation between senior management engagement and success in risk assessment.
- *Inappropriate resource planning and allocation:* A critical success factor in the implementation of risk assessment is having the right amount and mix of professional resources. On the one hand, some companies only allocate minimum part-time staff resources to conduct risk assessments. Inadequate resources are likely to result in inaccurate or superficial assessments of risks and controls. On the other hand, some companies over-allocate professional resources. At one mid-size bank, a team of more than 20 full-time risk staff and consultants worked on an annual risk assessment that took about nine months to complete.

In this instance, an over allocation of resources resulted in an excessively bureaucratic process that drained corporate and business unit time and resources. Moreover, the end product was several thick binders of risk assessment information that was not useful for the bank.

- *Insufficient preparation for risk assessment:* Risk assessment is not an ad-hoc process that can be easily implemented. It requires thoughtful planning and organization. As discussed above, the development of risk assessment tools and training programs should be a fundamental step. For most companies, risk assessment is an ongoing annual process that requires significant corporate and business unit time and attention. Thus, thoughtful preparation can go a long way to ensure that the risk assessment process is efficient and effective.

Phase 2: Risk Identification, Assessment, and Prioritization

With the foundation discussed above, the project team is ready to execute the risk assessment process with respect to risk identification, assessment, and prioritization. The key deliverables in this phase include top-down risk assessments from senior executives, bottom-up risk assessments from business and operating units, risk assessment reports and maps, and the prioritization of top enterprise-level risks. Figures 23.3, 23.4, and 23.5 provide examples and benchmarks of ratings for probability, severity, and effectiveness of controls:

Regulatory and Policy Requirements In pursuit of business objectives, businesses must comply with regulations and corporate policies. In fact, compliance with regulations and corporate policies is one of the key objectives of ERM. In risk assessment, it is useful to summarize the regulatory requirements and guidelines, as well as corporate policies and associated risk tolerance levels.

Risk Probability Rating:
1. **Very Low:** Less than 5% likelihood of risk event occurring within 1 year
2. **Low:** 5-20% likelihood of risk event occurring within 1 year
3. **Medium:** 20-50% likelihood of risk event occurring within 1 year
4. **High:** 50-95% likelihood of risk event occurring within 1 year
5. **Very High:** Greater than 95% likelihood of risk event occurring within 1 year

FIGURE 23.3 Example of Probability Ratings

Risk Severity Rating:
1. **Very Low:** Immaterial impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
2. **Low:** Low impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
3. **Medium:** Moderate impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
4. **High:** Significant impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
5. **Very High:** Very significant impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives

FIGURE 23.4 Example of Severity Ratings

Control Effectiveness Rating:
1. **Highly effective –** Risk exposures are within established tolerance levels; controls are tested and functioning effectively; linkage between risk and return is explicitly established (performance based); comprehensive metrics and dashboard reporting in place
2. **Effective –** Risk exposures are within established tolerance levels; controls are tested and functioning effectively; linkage between risk and return is implicitly established (judgment based); some metrics and dashboard reporting in place but development plans are established
3. **Moderately effective –** Risk exposures are generally within established tolerance levels with few exceptions; controls are functioning at an acceptable level but not fully tested; some metrics and dashboard reporting in place
4. **Needs improvement –** Some or material exceptions to established tolerance levels; controls are established but not fully tested; minimum metrics or dashboard reporting in place
5. **Needs significant improvement –** Significant exceptions to established tolerance levels (or tolerance levels are not established); controls are not in place or functioning effectively; minimum or no metrics or dashboard reporting

FIGURE 23.5 Example of Control Effectiveness Ratings

Risk Assessment Interviews and Workshops As discussed previously, it is beneficial to conduct interviews using open-ended questions when working with senior executives on risk assessments. In addition to identifying key risks associated with corporate objectives (i.e., top-down risk assessment), these interviews can gather important institutional knowledge about business strategy and culture, lessons learned from previous risk events, and the kinds of key performance indicators (KPIs) and key risk indicators (KRIs) that senior executives find most useful. For business unit teams, it may be more appropriate to organize workshops to develop bottom-up risk assessments. During the interviews and workshops, participants identify risks or risk events, and assess probability, severity, and effectiveness of controls. They may also decide on risk treatment (e.g., avoid, mitigate, transfer, or accept). Examples of ratings on probability, severity, and controls have been previously provided.

Risk Assessment Reports and Maps The interviews and workshops may result in a large number of risk assessments. It is the responsibility of the project team to aggregate and report on these results. Risk assessment reports generally provide the following information for each risk:

- Description of the risk or risk event
- Assessment and rating of probability (or likelihood)
- Assessment and rating of severity (or impact)
- Assessment and rating of control effectiveness
- Responsible person(s) and oversight committees
- Management response and action plans

In addition to risk assessment reports, the use of risk maps (or heat maps) can be used to help visualize the risk assessment information. Figure 23.6 shows an example of a heat map for a company's top seven areas of risk.

Risk Prioritization Based on the aggregate risk assessment results, the company should identify the most critical risks (e.g., top 10 risks). This is not to say that the company should only pay attention to 10 risks. In fact, each business unit or functional area may identify their top risks and collectively monitor all of the key risks recorded in the risk assessment process. However, it is useful to establish a priority list of risks for the overall company. For example, one large asset management firm reported more than 700 risks. It would be impractical for executive management or the board to review and monitor such a large number of risks. The project team can identify the top-10 risks for the company based on the risk assessment information, and they can confirm their analysis through a separate risk assessment session with executive

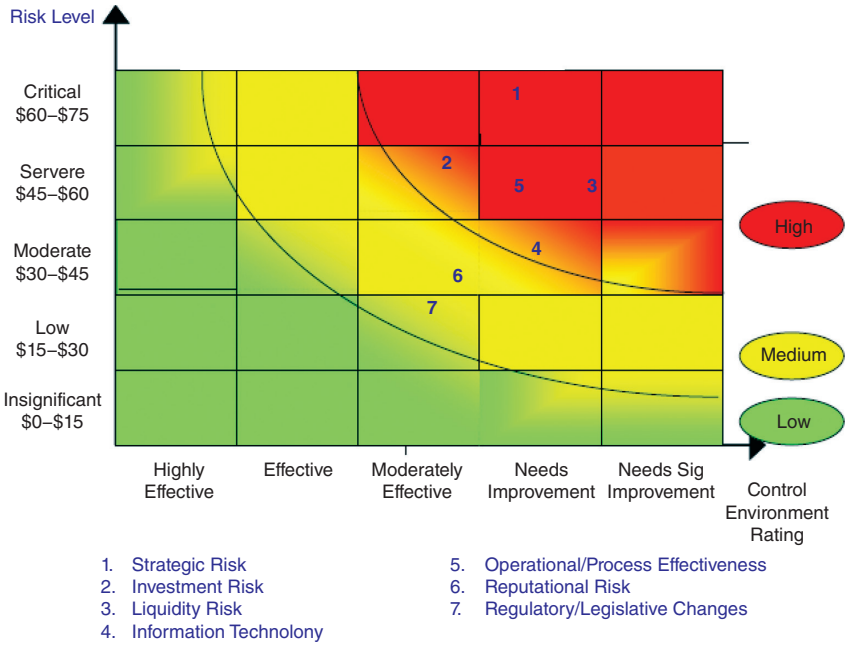


FIGURE 23.6 Heat Map

management. This list should be consistent with the company's risk appetite statement and should aim to protect the key interests of the business. Based on a prioritized set of the most critical risks, a company can develop more in-depth risk assessments, risk quantification, and risk treatment strategies.

In Phase 2, the common pitfalls and practical solutions include:

- *Lack of clear business objectives or risk policy constraints:* Most companies have a clear sense of regulatory requirements and guidelines. However, some companies have not clearly defined their business objectives, and/or have not established explicit risk tolerance levels. For these companies, it may be difficult to assess risks in the context of business objectives and policy constraints. In some instances, the company develops business objectives and risk policies in parallel with the risk assessment process. In other instances, this management issue becomes an identified risk of its own.
- *Defining risks in terms of consequences, and not root causes:* Risks are often erroneously defined based on consequences instead of root causes. Figure 23.7 outlines examples of root causes versus consequences. This can

cause frustration in determining the appropriate risk treatment because consequences are not directly controllable. For example, a company cannot decrease production errors or customer complaints directly, but it can increase process automation and staff training. Likewise, a company cannot determine its debt rating, but it can manage the company's equity level (through stock issuance and dividend policies) to ensure they are adequately capitalized given their target debt rating. Another example is that a company cannot control FX losses, but it can control its FX exposures and monitor FX volatility. During the risk assessment process, the project team must ensure that risks are defined in terms of root causes.

- *Inconsistent estimates of probability and severity:* What is the probability and severity of a risk event? The answers depend on the timeframe and, more importantly, on how bad a worst case the company is willing to consider. Any risk can be conceptualized and, with adequate data, quantified as a distribution or bell curve. That distribution curve represents a range of probabilities and severities. If we take investment portfolio losses as an example, there is a high probability that a company may suffer a small loss and a low probability that it may suffer a large loss. If different people are asked to assess the probability and severity of a risk event, they may be thinking of different levels of worst case. To address this issue, the project team should establish clear guidelines with respect to the worst case, as well as the timeframe for the risk assessment. Companies that allocate economic capital to all key risks may want to harmonize the probability level used for risk assessment and economic capital allocation (e.g., 95 percent or 99 percent). Ultimately, a probability-severity distribution curve can be developed for each risk assessment.

Phase 3: Deep Dives, Risk Quantification, and Management

The top-10 risks identified in the previous phase represent the most critical risks facing the company. A smaller list focuses management time and attention on the appropriate risks. For these risks, management concentrates

Root Causes	Consequences
Lack of automated processes	Production errors
Improperly trained staff	Customer complaints or loss
Ineffective capital management	Ratings downgrade
FX volatility	FX losses

FIGURE 23.7 Root Causes versus Consequences

on further risk assessment, risk quantification, and risk management strategies.

Deep Dives Deep dives are more granular risk assessments. Beyond the information gathered during Phase 2, deep dives may add risk assessments from the next level down in the organization; external benchmarking of the risk and related controls; process maps that clearly document the key business and operational flows; independent assessments from auditors and regulators; and control effectiveness testing. Overall, the purpose of deep dives is to get more granular and actionable information.

Risk Tolerance Levels Risk tolerance levels provide the boundaries to evaluate risk assessments and KRIs, and also represent the company's risk appetite on key risks. Examples of risk tolerance levels include (a) market risk, credit risk, or liquidity risk limits, (b) business performance targets and triggers, (c) operational performance goals and limits, and (d) other benchmarks in terms of desirable and undesirable performance. Ideally, KRIs are tracked against risk tolerance levels so management can clearly see if risk levels are within acceptable ranges.

Risk Management Strategies and Action Plans Without risk management strategies that reshape the company's risk/return profile, every process up to this point would be an intellectual exercise. Based on an assessment of the risk relative to business objectives and risk tolerance levels, management should decide on the appropriate risk management strategy. That strategy may be to avoid, mitigate, transfer, or accept the risk. Any risk acceptance decision should also involve strategies to incorporate the cost of risk into the pricing of the company's products and/or services. The total cost of risk includes expected loss, unexpected loss (i.e., cost of economic capital), risk transfer costs, and administrative costs. It is important to note that all companies take risks in their business activities. However, there is only one point at which they can get compensated for the risks they accept and that is in the pricing of their products and services. To support the execution of the risk management strategies, action plans with clear accountabilities should be developed.

During Phase 3 of the risk assessment process, the common issues and practical solutions include:

- *Lack of prioritization of top risks:* The risk assessment process in Phase 2 may produce a large number of key risks that may impact business objectives. But a key risk for a business unit may not be a key risk for the overall company. It would be too burdensome to develop KRIs, risk tolerance levels, risk management strategies, and early warning systems

for all of these risks. Thus the top risks for the company must be identified so management and the board can focus on a prioritized set of risks. However, this does not preclude business units from developing more granular analysis and action plans for all of their key risks.

- *Insufficient risk quantification:* Information collected from risk assessments is largely qualitative. Even the probability, severity, and control assessment ratings usually represent numeric expression of qualitative inputs. In order to build confidence in the appropriate risk management strategies and actions, objective risk quantification must supplement risk assessments. This stresses the importance of developing KRIs, risk tolerance levels, and early warning indicators.
- *Insufficient risk management strategies and action plans:* One of the biggest complaints about risk assessment is that the process does not result in value-adding strategies and actions. Companies spend significant time and resources to produce and review a large volume of risk assessment reports and maps, but these documents may sit on the shelf until the next risk assessment cycle. The end goal of risk assessment is not to produce better information, but to support more intelligent decision-making based on that information. It is critical that specific risk management strategies and action plans are developed as part of the risk assessment process. Moreover, risk assessment should be integrated into business processes and other ERM practices, as we will discuss in the next section.

Phase 4: Business and ERM Integration

Risk assessment should not be a standalone process. It should be integrated into strategic planning and review processes, business processes and operations, and other ERM processes such as dashboard reporting, loss/event tracking, and risk escalation policies.

Strategic Planning Important linkages between strategic planning and risk assessment should be established. In fact, the integration of strategy and ERM is a key initiative as boards and executive management take a more active role in risk oversight. This integration provides significant benefits. The strategic planning process provides business objectives, which, as discussed throughout this chapter, should drive risk assessment. On the other hand, risk assessment can add value to the strategic planning process with respect to the key risk exposures and the cost of risk, both of which are essential in making risk/ return tradeoff decisions. In addition to strategic planning, risk assessment should be integrated into strategy and business review processes. As companies execute their business strategies, they often organize strategy and business review sessions to consider new information such as competitive

trends, customer data, and business performance. This new information should be used to update risk assessments and related monitoring processes.

Business Processes and Operations On a day-to-day basis, risk assessment should be integrated into key business processes and operations. As discussed above, the pricing of the company's products and services should fully incorporate the price of risk. Risk assessments can also support other business processes such as new product and business development, mergers and acquisitions (M&A) transactions, project management, and capital allocation. Risk assessment should also be integrated into operational processes. For example, a process map can depict where key risks (and actual errors and losses) may occur within an operational process. Management can then embed specific controls and risk monitoring processes into where they are most effective.

Scenario Analysis and Stress Testing Companies should not only be concerned about the worst case scenario of any single risk, but also the possibility of a more consequential scenario of multiple risk events, such as a failed product launch, an economic downturn, and a new competitive threat. Moreover, the company may stress test the combined failure of key controls, such as risk model error, incorrect data, and departure of key risk personnel. While less likely than a single risk event, the confluence of multiple risk events (i.e., the perfect storm) may present the company with critical challenges that it should prepare for. Thus, the company should conduct risk assessments on scenarios where various risk events occur simultaneously.

Dashboard Reporting Risk and return are different sides of the same coin. Therefore, risk assessment results should be reported to senior management and the board as part of an integrated performance and risk reporting process. However, the sheer volume of data from risk assessments, other ERM analytics, and business performance systems can be overwhelming. Dashboard reports should be implemented in order to provide senior management and the board with the appropriate information. These dashboard reports should be designed to support the specific decision-making and informational needs of corporate executives and board members. For example, when asked about the attributes that they want to see on dashboard reports, board members often request:

- A concise executive summary of business/risk performance, as well as external performance drivers
- Streamlined reports, including a focus on key board discussion and decision points
- An integrated view of the organization, versus functional or silo views
- Key performance and risk indicators shown against specific targets or limits

- Actual performance of previous business/risk decisions
- Alternatives to, and rationale for, management recommendations for board decisions
- Drill-down capabilities to underlying data and analysis

We will discuss dashboard reporting further in chapter 25.

Loss/Event Database Every risk loss or event represents a valuable learning opportunity, but only if they are captured and reviewed systematically. Companies should develop and maintain a loss/event database to capture all material losses and incidents. This database can be used to conduct post-mortem analyses in terms of root causes and needed controls; monitor key risk trends and emerging patterns; address risk issues before they become major problems; and provide a feedback loop on the efficacy of risk assessments and dashboard reporting (i.e., are the risks underpinning the actual losses and events identified in risk assessments and monitored in dashboard reporting?).

Risk Escalation Policy Risk events do not occur at regular intervals, but in real time. Thus, annual risk assessments—even if they are updated monthly or quarterly—may not support timely alerts or management responses. A risk escalation policy can mitigate this problem by establishing specific notification triggers for material losses or events (e.g., losses above a certain threshold, risk events that impact a certain number of customers, etc.). A lesson learned from previous corporate disasters is that bad news does not always travel up the organization. A risk escalation policy establishes the explicit expectation and specific criteria for communicating risk events on a timely basis.

In the business- and ERM integration phase, the common pitfalls and practical solutions include:

- *Integration occurs only in back-end reporting:* Some companies simply provide consolidated reporting of various business and risk management processes. However, integrating risk assessment with other ERM and business processes should not only occur in the back end in terms of reporting. It should involve integrated planning and analysis in the front end, as well as on an ongoing basis in terms of performance and risk monitoring.
- *Lack of a change agenda and change management:* At most companies, the integration of risk management with strategy and business activities requires significant change in organizational processes. Different organizational units may have well-established policies and procedures for their business. To implement the necessary change, a clearly defined change agenda should be established. This includes change management strategies to align goals, overcome barriers, and measure and track success.

BEST PRACTICE CASE STUDIES IN RISK ASSESSMENT

For larger institutions, technology can prove helpful in all stages of the risk management process. Bank of America, a large banking institution, has partnered with Microsoft Office to develop a SharePoint Server 2007 that is customized to its risk assessment and reporting needs. The program has multiple-level access, allowing information to be dispersed at various stages of detail to employees based on rank. It allows employees to enter data about risk that is then aggregated and presented to senior management in the form of a risk report.[4]

Best-Practice Example: The Global Risk Report

While there are potential and significant pitfalls associated with risk assessment, there are examples of efforts that produce useful analyses and insights. The Global Risk Report (Report), annually produced by The Global Risk Network, is an example of a highly effective risk assessment process. Since 2004, a global group of sponsors and researchers collaborate each year to create a risk assessment that is published and discussed at the World Economic Forum. Based on the insights of 580 experts from different professions and countries, the 2011 Report demonstrates that it is possible to integrate diverse qualitative input into a cohesive and concise analysis. Let's look at the most commendable aspects of the Report:

- *The ability to integrate various risk assessments and opinions of the experts:* The Report pulls together information from highly diverse sources. The list of participants for the Report includes professors, executives from many different areas of business (from Citigroup to the World Health Organization), economists, and research scientists. The Report manages to sift through the knowledge of these 580 experts to grasp the most fundamental risks, or "Core" Global Risks, that the world economy is likely to face in the coming decade.
- *The reporting method is integrated and effective:* The Report presents its findings using a variety of different methods, from simple bullet-pointed lists to illustrative figures that render complex information accessible to readers with different levels of background knowledge. For example, the "Core" Global Risks are listed as bullet points, but are also detailed further with a diagram, which mapped these risks against axes representing severity (in U.S. dollars) and likelihood, to allow for quick, effective comparison.[5] This is akin to the risk maps that are produced by individual companies.
- *The Report provides analyses of risk interdependencies:* One of the most significant features of The Global Risk Report is a risk interconnection

map that studies the relationships between the various "Core" Global Risks. The map from the 2011 report identified three key risks: the "macro-economic imbalances nexus," the "illegal economy nexus," and the "water-food-energy nexus." A web of contributing risks represents each of these key risk categories. For example, for the "macro-economic imbalances nexus," asset price collapse, fiscal crises, and global imbalances/currency volatility are presented as the contributing risks. The lines of the webs are shaded various gradients to indicate the strength (or, conversely, weakness) of a particular link between two risks.[6]

- *The 2007 Report identified the risks underlying the 2008 financial crisis:* An effective risk assessment should provide forward-looking analysis and early warnings of emerging risk. One of the "Core" Economic risks identified by the 2007 Report was a "blow up in asset prices/excessive indebtedness."[7] This turned out to be a crucial factor behind the 2008 housing bubble, which demonstrates effectiveness of the Global Risk Network's ability to identify the macro risk trends given the experts' opinions.

APPENDIX: RISK ASSESSMENT SELF-EVALUATION CHECKLIST

As companies evaluate and assess their current risk assessment procedures against best practices, the following checklist can serve as a useful framework of standards and suggestions to evolve from one stage to another. Based on the self-evaluation scores, a company can identify critical gaps and determine specific areas for improvement. It may be useful to develop a group-based evaluation by organizing a small cross-functional team to go through this checklist.

The Risk Assessment Self-Evaluation is based on two dimensions in risk assessment:

- *Development and maturity* of risk assessment standards, or to what extent the company has developed a robust and mature risk assessment process
- *Integration and application* of risk assessment results, or to what extent the company is effective in integrating risk assessment into business and ERM processes, and applying the results in making better decisions

Now let's look at the specific steps of the self-evaluation checklist.

Step 1

Please rate your risk assessment processes from 1 to 5. Enter your rating in the last column for each criterion and sum the ratings at the bottom.

FIGURE 23.8 Evaluation of Risk Assessment Development and Maturity

Rating Criteria	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Score
1. **Organizational Alignment and Support.** Our risk assessment process is fully supported by the board and senior management, as well as the business units. Participants are engaged in open discussions and provide candid input on risks and controls.						
2. **Planning and Resources.** We have a well-defined plan to conduct risk assessments. Specific roles are clearly defined and we have the appropriate resources to carry out that plan.						
3. **Risk Taxonomy.** We have established a risk taxonomy with key categories and definitions for risk. Participants use a common language when they discuss risk and control issues.						
4. **Risk Assessment Tools.** We have a robust set of tools to support risk assessment, including standard questionnaires, templates, and software and pooling tools.						
5. **Training and Development.** We have provided training and development programs on risk assessment. These programs are available to new participants.						

Rating Criteria	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Score
6. **Linkage to Business Objectives.** Our risk assessment process is explicitly linked to business objectives, at both the corporate and business unit levels.						
7. **Linkage to Regulatory and Policy Requirements.** Our risk assessment process incorporates the key regulatory and policy requirements for our business.						
8. **Input Quality.** During interviews and workshops, our risk assessment discussions are highly effective. We describe risks based on root causes (not consequences) and we apply consistent definitions for probability, severity, and control effectiveness.						
9. **Output Quality.** The risk assessment reports and risk maps are highly effective. We have a clear risk profile at both the corporate and business unit levels. Participants are highly satisfied with our reports and maps.						
10. **Risk Prioritization.** We have established a systematic methodology to identify our top risks. Deep-dive analyses are performed to obtain more granular and actionable information.						

Total Score on Development and Maturity:
Total Score for Integration and Application:

FIGURE 23.9 Evaluation of Risk Assessment Integration and Application

Rating Criteria	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Score
1. **Key Risk Indicators.** We have integrated risk assessments and KRIs. Risk assessments provide input on the design of KRIs, and KRIs help us monitor our risk exposures and trends.						
2. **Risk Tolerance Levels.** We have established risk tolerance levels for our key risks to ensure that our actual exposures are within acceptable levels.						
3. **Risk Management.** For our key risks, we develop risk management and actions plans, with clear accountabilities for avoiding, mitigating, transferring, or accepting the risks.						
4. **Early Warning Systems.** We have established early warning systems that include leading risk indicators and contingency action plans.						
5. **Strategic Planning and Reviews.** Our risk assessment process is integrated with strategic planning, as well as ongoing strategy and business reviews.						
6. **Business Processes and Operations.** We apply risk assessment results into						

Rating Criteria	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Score
our business processes (e.g., pricing, product development, capital allocation) and day-to-day operations (e.g., call centers, treasury operations, IT).						
7. **Scenario Analysis and Stress Testing.** In addition to individual risks and controls, we conduct scenario analysis and stress tests of a confluence of risk events and/or a failure of multiple key controls.						
8. **Dashboard Reporting.** We have implemented management and board dashboards that provide integrated performance and risk reporting.						
9. **Loss/Event Database.** We have established a database that captures material losses and events. This database supports post-mortem analysis, risk monitoring and response, and continuous improvement of our risk assessments and dashboard reporting.						
10. **Risk Escalation Policy.** To supplement our risk assessments, we have implemented a risk escalation policy with specific notification triggers for material losses or events. This policy ensures that "bad news" travel up the organization.						

Step 2

Sum the total scores for development/maturity and integration/application. For each total, the minimum score is 10 and the maximum score is 50, with a midrange score of 30.

Step 3

Based on the two total scores, identify the quadrant and placement for your company using the matrix laid out in Figure 23.10. The vertical axis is for the total score on development/maturity and the horizontal axis is for the total score on integration/application.

Step 4

Evaluate the results and develop plans to further develop, integrate, and apply risk assessments at your organization. The following guidelines might serve as a starting point for discussion.

Beginners Your company may be in the early stages of conducting risk assessments or you have been implementing risk assessments for a few years, but a lack of priority and resources have prevented you from advancing your risk assessment techniques. This can be seen as an opportunity to make

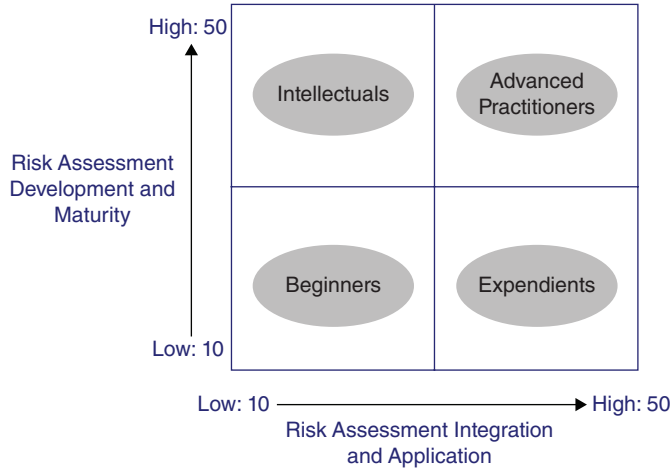


FIGURE 23.10 Self-Evaluation Matrix

progress on developing your risk assessment processes, as well as integrating and applying these processes to make better decisions.

Intellectuals Your company has been developing risk assessment tools, software, reports, and maps for several years. Overall, your risk assessment process is robust and mature. However, the risk assessment process appears to be a standalone exercise that is disconnected from other ERM and business activities. There may be concerns that the risk assessment represents a significant cost without tangible business benefits. You should focus your attention and resources to integrate risk assessment with other ERM tools, as well as strategic and business processes.

Expedients Your company is practical in integrating and applying risk assessments. However, the lack of development of risk assessment tools and processes may hinder your ability to conduct risk assessments in an efficient and consistent manner. It may seem like you are reinventing the wheel each time a risk assessment cycle is executed. Moreover, the lack of standards makes it difficult to evaluate trends over time or compare risk assessments across the company. You should focus your attention and resources to develop more robust risk assessment tools and processes.

Advanced Practitioners Congratulations! Your company is an advanced practitioner in risk assessment and ERM processes. You have developed standardized tools and systematic processes for risk assessment. More importantly, you apply these tools and processes to make better strategic, business, and operational decisions. However, best-practice ERM is a journey and not a destination. You should focus your attention and resources to stay up to date on emerging best practices and maintain your leadership position.

■ ■ ■

In the aftermath of the global financial crisis, risk management has climbed to the top of corporate board and management agendas. Risk assessment represents a critical component of any ERM program. For risk assessments to be effective and value-adding, the company must: establish the appropriate foundation in terms of executive sponsorship, organizational resources, risk assessment toolset, and training; perform the risk assessments on consistent basis; prioritize the company's top risks for more granular analyses, risk quantification, and risk management strategies; and integrate risk assessment into other business and ERM processes.

CHAPTER 24

Risk-Based Decision Making

A few years ago, I led an enterprise risk management (ERM) research project on Asian bank risk management. In one meeting in Beijing I met with the CRO of one of the largest Chinese banks. We reviewed the four components of ERM implementation governance structure and policies, risk assessment and quantification, risk management, and dashboard reporting and monitoring (refer to Figure 21.2). He asked which one of the four components I think is the most important to get right. Before answering his question, I asked him for his opinion. He suggested the risk assessment and quantification component, since it provides accurate identification and analysis of the risks. I respectfully disagreed and instead proposed that risk management is the most important because it is the only one of the four components that actually impacts the risk/return profile of the organization. We debated the question and agreed that while all four components are important, the only way to add economic value to the business is through risk management decisions and actions.

That conversation reinforced what I believe to be one of the greatest challenges in ERM: how do we integrate ERM into business decision-making processes in order to create value? This chapter will specifically address this critical question.

ERM DECISIONS AND ACTIONS

In the design and implementation of ERM, it is critical to support the decision-making processes of the organization. The Pareto principle, also known as the 80/20 rule, states the general observation that 80 percent of the effects come from 20 percent of the causes. We see this in both everyday life and business. For example, 80 percent of your free time is spent with 20 percent of your friends, or 80 percent of sales come from 20 percent of the customers. The 80/20 rule can also apply to risk management. As illustrated in Figure 24.1, the risk management function might spend 80 percent

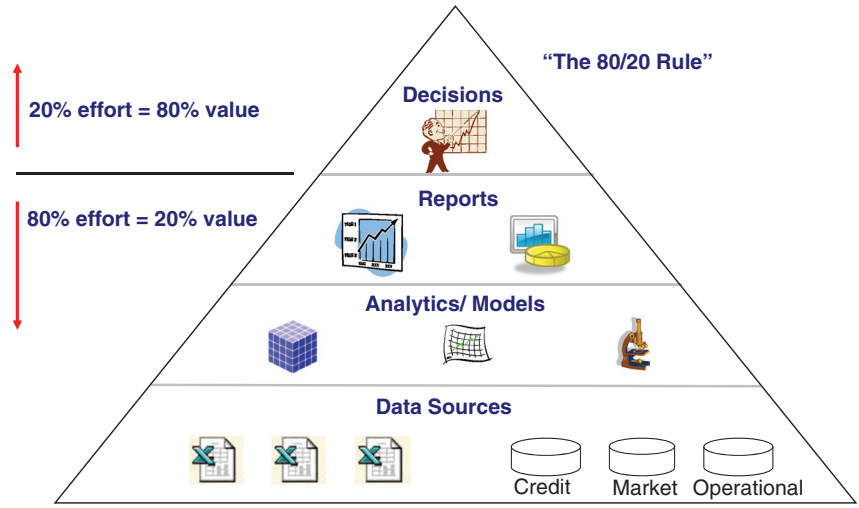


FIGURE 24.1 The 80/20 Rule of ERM

of its efforts in gathering the data, developing risk analytical models, and producing board and management reports. However, this work may only produce 20 percent of the value in terms of better information. On the other hand, risk-based decision making, which we will cover in this chapter, might take only 20 percent of the effort, and yet produce 80 percent of the value with respect to more informed business decisions.

Let's examine a typical risk system implementation process to illustrate the necessity of focusing on decision-making. In general, risk managers apply a bottom-up approach to implementing a risk system, as shown in Figure 21.1. They might begin with risk modeling and data requirements by defining the analytical capabilities, systems functionality, and data sources. Based on these requirements, they may implement the new risk system using vendor-based or in-house programs, or some combination of the two. As part of the implementation process, risk reports are produced for, and delivered to, the various groups within the organization.

However, this is the point at which the value-creation process often breaks down. The individuals or groups receiving these risk reports may not have deep risk management backgrounds. Moreover, the risk reports may have been prepackaged vendor-based reports, or designed without their decision-making needs in mind. As such, there is a steep learning curve to simply understand the metrics and analyses, let alone make critical decisions based on them. In the end, the new risk system supports mainly risk

reporting for informational and compliance purposes, but it has insignificant impact on decision-making.

Alternatively, a more efficient and effective way of implementing a risk system is to take a top-down approach. The first step is to identify the business and risk management decisions of various committees, functions, and individuals, as well as the decision-support requirements of the decision makers. In other words, how do these committees, functions, and individuals make decisions? How can we establish the appropriate structure and content in the risk reports to support these decisions? If the risk system implementation team doesn't fully understand these requirements, they need to ask. This may involve interviewing board members, corporate employees, and business executives to understand their decision-making needs. The second step is to design easy-to-understand and concise risk reports, and use rapid prototyping, interim reviews, and interactive discussions to ensure the final risk reports are useful to the decision makers. The final step is to implement the risk analytical models and develop the data sources that will support the generation of the risk reports. By taking a top-down approach and supporting the key decisions, risk management can achieve its full value.

General Risk Decision Choices

What are the decision choices an organization can make in risk management? In general, the following are the key risk management decisions:

- *Risk acceptance or avoidance:* The organization can decide to increase or decrease a specific risk exposure through its core business, mergers and acquisitions (M&A), and financial transactions. This includes new product development, market expansion, acquisitions and divestitures, and capital budgeting and financing activities.
- *Risk mitigation:* An organization can establish risk control processes and strategies in order to manage a specific risk within a defined risk tolerance level. This includes constructing a risk appetite statement with explicit risk tolerance levels, corporate risk policies, risk measurement and monitoring systems, and risk control strategies and contingency plans.
- *Risk-based pricing:* All firms take risks in order to be in business, but there is only one point at which they can get compensated for the risks that they take. That is in the pricing of their products and/or services, which should fully incorporate the cost of risk. The full cost of risk should be incorporated into the pricing of products and services, and be used to measure the risk-adjusted profitability of customers and business units. We will discuss examples of risk-based pricing in the next section.

- *Risk transfer:* An organization can decide to execute risk transfer strategies through the insurance or capital markets if risk exposures are excessive and/or if the cost of risk transfer is lower than the cost of risk retention. Risk transfer strategies include hedging with derivative products, corporate insurance and captive insurance strategies, and securitization programs.
- *Resource allocation:* An organization can allocate human and financial resources to business activities that produce the highest risk-adjusted returns in order to maximize firm value. This includes rationalizing the allocation of staff resources, economic capital, and financial budgets based on projected risk-adjusted performance.

Roles of the Board, Corporate Management, and Business Units

While it is important to understand the general risk decision choices an organization can make as discussed above, in practice, risk management decisions are made by a specific committee, function, or individual. These decision makers can be the board, corporate management, or business and functional units. Figure 24.2 provides a summary of key risk management decisions based on the three lines of defense model.

FIGURE 24.2 Risk Management Decisions

Business Units and Support Functions Business units and support functions (e.g., information technology or human resources) represent the first line of defense, and they are ultimately accountable for measuring and managing the risks inherent in their businesses and operations. However, they must assume some level of risk to generate profits and growth, and achieve their business objectives. Key business and risk management decisions would include accepting or avoiding risks in day-to-day business activities and operations; establishing risk-based product pricing and managing customer relationships; and implementing tactical risk mitigation strategies and contingency plans in response to risk events.

Corporate Management Corporate management, supported by the CRO, ERM, and compliance functions, represents the second line of defense. They are responsible for establishing and implementing risk and compliance programs, including risk policies and standards, risk appetite and tolerances, and board and management reporting processes. The second line of defense is accountable for ongoing risk monitoring and oversight. Key business and risk management decisions include allocating financial and human capital resources to business activities that produce the highest risk-adjusted profitability; implementing organic and/or acquisition-based growth strategies; and risk transfer strategies to reduce excessive or uneconomic risk exposures.

The Board of Directors The board of directors, with the support of the audit function, represents the third line of defense. They are responsible for establishing board risk governance structure and oversight processes; reviewing, challenging, and approving risk policies; and overseeing strategy execution, risk management, and executive compensation programs. The third line of defense is accountable for the periodic review and assurance of risk management effectiveness. Key business and risk management decisions would include establishing the statement of risk appetite and risk tolerance levels; reviewing and approving management recommendations with respect to capital structure, dividend policy, and target debt ratings; and reviewing and approving strategic risk management decisions, including major investments and transactions.

CREATING VALUE THROUGH ERM

In Chapter 21, we examined several empirical research studies that indicate significant improvements in financial performance and shareholder return are associated with stronger corporate governance and ERM programs. While these studies provide encouraging evidence that value can be created

through ERM, an individual company would be more interested in specific examples of value-creating strategies. Figure 24.3 provides a diagram of the key drivers of shareholder value. The two main drivers are return on equity (ROE) and growth. ROE is determined by net income (revenue minus expenses and losses and taxes) divided by equity; growth is driven by new business, M&A, and business diversification strategy.

In the context of these value drivers, let's review how the scope of risk management has expanded with ERM. Prior to the late 1980s, companies practiced risk management in a silo-based manner. The objective was mainly to develop cost-effective insurance and hedging strategies and minimize financial and operational write offs (numbers 5 and 6 on Figure 24.3). In the later 1980s and early 1990s, companies began to practice the integrated management of financial risks (i.e., credit risk, market risk, liquidity risk) and apply economic capital techniques. The scope of risk management expanded to include establishing cost-effective risk oversight functions and efficient allocation of capital resources. Since the mid-1990s, ERM has continued to increase the reach of risk management to include strategy and business risks so that the risk function can have an impact on all 10 drivers.

In the remainder of the chapter, let's focus our discussion on four of these key drivers:

- Risk-based pricing
- Mergers and acquisitions
- Risk transfer
- Strategic risk management

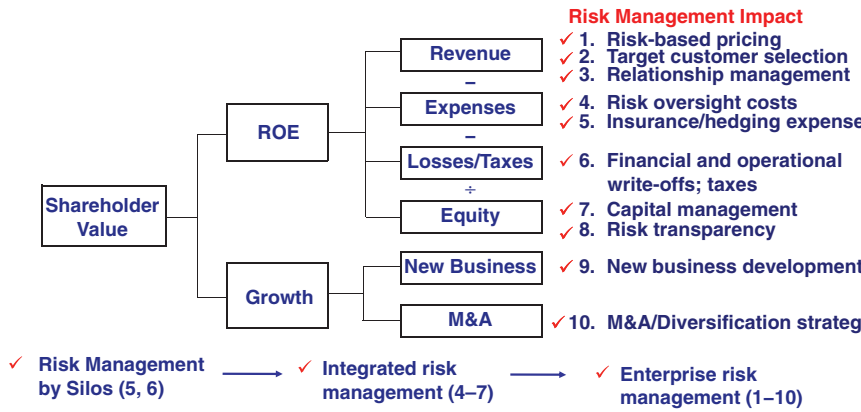


FIGURE 24.3 Value Drivers

Risk-Based Pricing

As we touched on earlier, the most effective way for companies to ensure a return on the risks they have accepted is to incorporate the cost of risk into their pricing methodologies. If the cost of risk is not fully reflected in the initial pricing (e.g., the product or transaction is underpriced relative to the risk), then there is nothing the company can do to recover its costs. Risks that are underpriced may increase revenue and growth in the short term, but over time they will destroy shareholder value. When quantifying the total cost of risk, companies should include:

- Expected loss (EL), or average loss per year
- Unexpected loss (UL), which can be defined as economic capital × Ke (cost of equity capital)
- Risk transfer costs (i.e., of hedging or insurance)
- Risk management costs (i.e., that pertain to maintaining staff, systems, etc.)

Figure 24.4 provides an example of risk-based pricing. The building blocks for the typical income statement go from right to left; start with net revenue, and subtract from it risk losses, expenses, and taxes to compute net income, and then divide net income by equity to quantify ROE. Risk-based pricing basically reverse-engineers the traditional income statement. In other words, the building blocks go from left to right. With risk-based pricing,

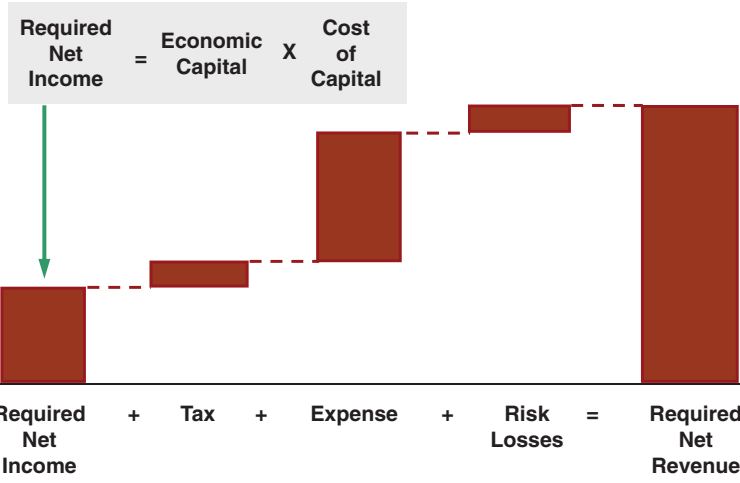


FIGURE 24.4 Risk-Based Pricing

we actually start by multiplying economic capital and the cost of capital to determine the required net income. We then add to it taxes, expenses, and risk losses to calculate the required net revenue.

Let's look at a numerical example of risk-based pricing, and see how the same methodology can be used to calculate RAROC and pricing. In the first column in Table 24.1, Calculate RAROC, the math works from top to bottom. We have a $100 million transaction and a 2.5 percent margin, resulting in $2.5 million in revenue. Pre-tax net income of $1.0 million is derived after subtracting risk losses (i.e., expected loss) of $0.5 million and expenses of $1.0 million. Assuming a 40 percent tax rate, net income of $0.6 million is calculated. In this example, $2.0 million of economic capital is allocated based on the underlying risks of the transaction. Finally, a 30 percent RAROC is quantified by dividing net income by economic capital. This 30 percent RAROC metric can be very useful in decision making in two ways:

- First, it can support product and customer management strategy. If RAROC is above Ke then the transaction or customer is creating shareholder value and the company should do more of this business. Conversely, if RAROC is below Ke then the transaction is destroying shareholder value and the company should discontinue this business, increase pricing of future transactions, or cross-sell more profitable products to the same customer to bring the overall RAROC of the relationship above Ke.
- Second, it can support business management and resource allocation. The calculated RAROCs of different business units can be compared against each other because they provide a consistent risk-adjusted measurement of profitability. Other profitability measures—such as profit margin, return on assets (ROA), ROE—are not risk-adjusted, so any comparisons might lead to wrong conclusions. For example, a business unit with marginally lower ROA and ROE might be more attractive than another business unit if the former has a substantially lower risk profile. RAROC analyses support management decisions regarding which businesses to grow, maintain, fix, shrink, or exit.

In the above example, how should the company respond if a close competitor decides to introduce a discount pricing strategy by charging a 2.3 percent margin (instead of 2.5 percent)? Risk-based pricing can be used to support that business decision. This is demonstrated in the second column, Calculate Pricing, where the math works backward or from bottom to top. Say the company decides that a 20 percent RAROC is the minimum hurdle rate of profitability that it wants to achieve for this business. By applying the same methodology but in reverse, a 2.2 percent margin is calculated as the risk-based pricing that would achieve a 20 percent RAROC.

TABLE 24.1 Calculating RAROC and Risk-Based Pricing

	Calculate RAROC		Calculate Pricing	
[1] Exposure	$100 mm		$100 mm	
[2] Margin	2.5%		2.2%	[3] ÷ [1]
[3] Revenue	$2.5 mm	[1] × [2]	$2.2 mm	[6] + [5] + [4]
[4] Risk Losses	<0.5 mm>		<0.5 mm>	
[5] Expenses	<1.0mm>		<1.0 mm>	
[6] Pre-tax Net Income	$1.0 mm	[3] – [4] – [5]	$0.7 mm	[8] + [7]
[7] Tax (40% tax rate)	<0.4 mm>		<0.3 mm>	
[8] Net Income	$0.6 mm	[6] – [7]	$0.4 mm	[10] × [9]
[9] Economic Capital	$2.0 mm		$2.0 mm	
[10] RAROC	30%	[8] ÷ [9]	20%	

For over 20 years, banks have applied economic capital, risk-based pricing, and RAROC analysis in managing their businesses. Banks use these tools to measure risk-adjusted profitability and pricing for a wide range of products and services, including commercial loans, consumer loans, derivative products, and investment banking and brokerage services. However, as we have discussed in the Microsoft and Airbus case studies at the end of Chapter 18, non-financial corporations must also fully incorporate the cost of risk in their product pricing.

Mergers & Acquisitions

M&A transactions can have a profound impact on the fortunes of companies. A good deal can help a company leapfrog its competitors, while a bad one can set it back for many years. The ERM function can support critical decisions in M&A by assessing the risk profile of the target company and the risk/return economies of the combined organization.

Traditional merger analysis is based on financial projections of the companies operating as independent entities as well as a combined company. Based on these financial projections, potential earnings dilution/accretion can be estimated assuming a range of acquisition prices. However, traditional earning dilution/accretion analysis does not fully adjust for risk. As such, it can lead to the wrong M&A decisions with dire strategic and financial consequences.

Let's examine how ERM can help a company make better M&A decisions. Figure 24.5 provides an example of an M&A analysis. In this example, Company A is considering acquiring either Company B or Company C. To simplify this example, we will assume that both companies can be acquired for the same price. Based on traditional financial analysis, Company C appears to be the more attractive because it has a higher RAROC and a higher market-to-book (M/B) ratio than Company B. In M&A parlance, acquiring Company C would be anti-dilutive (no earnings dilution) while acquiring Company B would be dilutive.

However, we have not considered the effects of diversification benefits (i.e., risk correlations). ERM incorporates these factors in evaluating the two potential acquisitions. The impact of the diversification benefits can be seen in the economic capital line of the combined entities. Acquiring Company B would result in a 30 percent diversification benefit: the economic capital of A+B is 210 compared to 300 before the merger (200 for Company A and 100 for Company B). On the other hand, acquiring Company B would result in a 10 percent diversification benefit: the economic capital of A+C is 270 compared to 300 before that merger (200 for Company A and 100 for Company C). As such, the acquisition of Company B would result in a higher RAROC and a higher M/B ratio.

Risk Transfer

Within a company, ERM has represented a holistic risk program that integrates the management activities for strategic risk, market risk, credit risk, and operational risk, often under the leadership of a CRO. Within the

FIGURE 24.5 M & A Analysis

	A	B	C	A + B	A + C
Revenue	100	50	50	150	150
Expense	50	30	25	80	75
Pre-Tax	50	20	25	70	75
Tax	20	8	10	28	30
Net Income	30	12	15	42	45
Economic Capital	200	100	100	210	270
RAROC	15%	12%	15%	20%	17%
M/B Ratio*	1.00	0.67	1.00	1.50	1.20

* M/B Ratio = (RAROC – g) ÷ (Ke – g); assumes Ke = 15% and g = 5%

capital markets, ERM has signified the convergence of financial and insurance products, resulting in a whole new class of innovative risk transfer solutions, such as credit derivatives, insurance-linked securities, and other alternative risk transfer (ART) products.[1]

As we have discussed throughout this book, the silo approach to risk management is fundamentally flawed when it comes to how a company organizes its internal processes to deal with interdependent risks. By extension, the silo approach is also flawed when it comes to risk transfer.

Traditionally, risk transfer has been viewed by companies as a way to solve specific micro-risk issues. There are generally two reasons behind a firm's rationale for implementing risk transfers: either the firm's exposures are too excessive, and they need to shed risk, or it is more financially efficient for that risk to be taken on by a third party, such as a hedge fund or insurance provider. Within a company, for example, the treasurer may use financial futures and swaps to hedge interest rate and foreign exchange (FX) risk exposures, while the insurance manager might purchase product liability and property and casualty (P&C) insurance to protect against certain business and operational risks. Both the treasurer and the insurance manager have specific risk problems they seek to address through risk transfer. They will evaluate various proposals from product providers and then make a decision based on the best structure and price.

However, even in a risk silo, the cost of risk transfer can be greatly reduced when individual positions are grouped into portfolios. For example, the treasurer can reduce hedging costs for interest rate risk by macro-hedging the overall balance sheet as opposed to micro-hedging individual assets and liabilities. Similarly, insurance managers have realized significant premium savings by taking advantage of internal diversification and transferring the residual risks using multi-risk, multi-year insurance policies.

ERM takes diversification a step further by integrating the risk silos into a firm-wide risk portfolio. The benefits of diversification, or internal hedges, can then be maximized by considering the volatility and correlation of all risk exposures. As such, the company can integrate its risk transfer activities and focus on its net risk exposures. Taking an ERM approach to risk transfer produces four key benefits:

- Incorporation of the full impact of diversification and thereby reducing the notional amount of coverage and cost of risk transfer
- Rationalization of various risk transfer strategies to avoid the over- and under-hedging of different risks
- Optimization of the limits and attachment points for insurance/reinsurance policies, as well as the hedging structures for derivative transactions

- Minimization of the cost of risk transfer by arbitraging between traditional and alternative risk transfer products, as well as between product providers

It is important to note that while ART products can be highly effective, their use is not required in ERM to achieve the above benefits. A company can gain efficiency simply by taking an ERM perspective in assessing its portfolio of risks before executing traditional derivative or insurance transactions.

The economic capital and RAROC methodology discussed above for risk-based pricing is also a useful tool for evaluating the impact of different risk transfer strategies. For example, the economic benefits of executing any risk transfer strategy include lower expected losses and reduced loss volatility, while the economic costs include insurance premium or hedging costs, as well as higher counterparty credit and operational risk exposures. In a sense, the company is ceding both risk and return, resulting in a ceded RAROC. By comparing the ceded RAROCs of various risk transfer strategies, a company can compare different structures, prices, and counterparties on an apples-to-apples basis and select the most optimal transaction(s).

Ceded RAROC is calculated by dividing the incremental change in return by the incremental change in economic capital. In essence, it represents the effective cost of risk transfer. If the ceded RAROC is below the cost of equity capital (Ke), then the risk transfer creates shareholder value. If, conversely, the ceded RAROC is above Ke, then the risk transfer is actually destroying shareholder value.

ERM can support risk transfer decisions in two important ways. The first is to analyze the net risk exposures of the company, including natural hedges, diversification benefits, and cross-risk correlations. The second is to analyze the economic costs of various risk transfer strategies, and also to compare the cost of risk transfer (ceded RAROC) versus the cost of risk retention (Ke).

Strategic Risk Management

The integration of strategy and ERM, or strategic risk management, is now considered by many as the next frontier in risk management. This recognition is driven by the elevation of ERM as a board and executive management issue, heightened regulatory and stakeholder expectations, as well as numerous empirical studies that indicate when companies suffer a significant drop in market value, the majority of the time it is due to strategic risk, and not financial or operational risks.

James Lam & Associates (JLA) addressed this question in 2004 by performing an original research study on the main cause for financial distress at

publicly traded companies. The research question was straightforward: when a company suffers a major decline in market value (defined as a 30 percent relative decline), what was the root cause? Through the analysis of the market value data of S&P500 companies between 1982 and 2003, the JLA research team found that 76 companies had experienced a 30 percent or more relative value decline in one month. In other words, if the S&P500 dropped by 10 percent in a given month, these companies would have dropped by 40 percent or more. The 76 companies encompassed a cross section of major industries, including energy, materials, industrials, telecommunications, consumer products, health care, utilities, and financials. For each of these 76 occurrences, the JLA research team reviewed news reports, regulatory filings, and company statements to determine the root cause. In summary, the research project found that 61 percent of the occurrences were due to strategic risks (e.g., consumer demand, M&A, competitive threats), 30 percent were due to operational risks (e.g., accounting irregularities, supply chain disruptions), and 9 percent were due to financial risks (e.g., commodity prices, FX, interest rates).

The Corporate Executive Board and Deloitte Research conducted similar studies, using different groups of companies, time periods, and definitions of major decline in market value. As summarized in Figure 24.6, these three independent research studies resulted in comparable findings. When companies suffer a significant drop in market value, strategic risk is the main culprit, followed by operational risk and financial risk.

Given the importance of strategic risk, how should companies manage it? Let's use GE Capital's Policy 6.0 as a best-practice example. As discussed in Chapter 21, I joined GE Capital to launch a new capital markets business in 1993. At GE Capital, Policy 6.0 is a strategic risk management framework that applies to all new businesses, products, and investments. Prior to obtaining corporate approval, Policy 6.0 requires a detailed analysis of the strategic risks associated with the new business. It also requires quarterly business/risk reviews between the business leaders and GE corporate executives to ensure that the business is performing at or above expectations. As shown in Figure 24.7, the major components of Policy 6.0 include:

- *Key Assumptions:* In many respects, the key assumptions of a business plan represent the most critical strategic risks. These assumptions may include business trends, customer needs, and disruptive technologies. The new business is required to identify the key assumptions that support the feasibility of the new business.
- *Monitoring Systems:* For each assumption, the business must identify the monitoring systems with respect to key performance indicators, key

FIGURE 24.6 Risks Causing Large Declines in Market Value

Organization	Research Methodology	Key Findings
James Lam & Associates (2004)	■ S&P 500 (1982-2003). ■ One-month stock price decline of 30% or greater relative to the S&P 500	■ 61% were exposed to strategic risks ■ 30% were exposed to operational risks ■ 9% were exposed to financial risks
The Corporate Executive Board (2005)	■ Fortune 1000 companies (1998-2002) ■ Top 20% of companies with the greatest market value declines	■ 65% were exposed to strategic risks ■ 20% were exposed to operational risks ■ 15% were exposed to financial risks
Deloitte Research (2005)	■ Thomson Financial Global 1000 Companies (1994-2003) ■ One-month stock price decline relative to the Morgan Stanley Financial World Index	Among the 100 largest declines: ■ 66 involved strategic risks ■ 62 involved external events ■ 61 involved operational risks ■ 37 involved financial risks

risk indicators, and early warning indicators. Moreover, the individuals responsible for oversight need to be specified.

- *Trigger Points:* With respect to the most critical metrics, the business is required to establish pre-defined positive, expected, and negative trigger points. These trigger points initiate management actions or reviews in between the quarterly business/risk reviews. If significant thresholds are breached, they may trigger immediate escalations and special reviews.

FIGURE 24.7 GE's Capital Policy 6.0

Key Assumptions	Monitoring Systems	Trigger-Points	Management Decision or Action
■ Business/economic ■ Customer needs ■ Technology trends	What metrics? By Whom?	+ Expected –	√ Accelerate Maintain Exit

- *Management Decision and Action:* Positive trigger points mean things are going better than planned, which indicates that management may consider accelerating the business plan or accept more risks. Negative trigger points may initiate risk mitigation strategies, or, if key metrics and trends are well below expectations, then an exit strategy may be considered.

Based on my direct experience, GE Capital's Policy 6.0 is a simple but effective strategic risk management framework that enables thoughtful analyses and disciplined management responses. Various research studies have indicated that up to 70 percent of new business initiatives fail to meet management expectations. A strategic risk management framework supports management decisions and corrective actions to ensure that scarce human and financial resources are reallocated to the other 30 percent in a timely manner.

CASE STUDY: DUKE ENERGY

In July 2000, Duke Energy's senior executives gathered for a two-day strategy meeting to discuss the future of the energy business. They reviewed three possible scenarios:

- Economic Treadmill, in which U.S. economic growth slips to 1 percent per year
- Market.com, in which the internet revolutionizes the relationships between buyers and sellers
- Flawed Competition, in which uneven deregulation will continue in the energy industry, resulting in significant price volatility.

Duke Energy's consideration of these different scenarios is a great example of the stress-testing strategies that we discussed in earlier chapters. It was particularly pertinent of Duke Energy to consider these issues in the year 2000, when confidence in the U.S. economy's boom was starting to wane—the beginnings of the confidence slide that would culminate in the bursting of the internet bubble.

To help manage the company's strategic and business uncertainties, Duke Energy appointed Richard Osborne as its first CRO earlier that year. As early warning indicators for these three scenarios, management established specific signposts, including macroeconomic indicators, regulatory trends, technology changes, environmental issues, competitive moves, and patterns of consolidation in the energy industry.[2] Over time, Duke Energy began to

notice that a large number of the signposts for the Flawed Competition scenario were being flagged, and so they acted accordingly, under the assumption that this was the scenario most likely to occur.

There was a general lack of consensus within the energy industry with regard to what the future would hold, which meant that having a concrete direction gave Duke Energy the important advantage of being able to take action. With a set vision, Duke Energy was able to focus and streamline its strategic, long-term plans. Instead of recklessly capitalizing on the increase in power demand through rapid expansion, as many other comparable companies were doing in the early 2000s, Duke Energy decided to rearrange and solidify its existing assets instead. For example, fearing that the electricity market in Texas would be over supplied in coming years, Duke Energy sold some of its plant assets in Texas even before they were completely built.[3]

Duke Energy's hard work has ultimately paid off, and it has continued to perform well relative to its competitors. For the five-year period ending December 2012, Duke Energy delivered a shareholder return of 6.7 percent, which is significantly higher than the 1.7 percent return in the S&P 500 Index and the 0.1 percent return in the Philadelphia Utility Index.[4] Duke Energy's excellent performance has been widely recognized over the years. For instance, Duke Energy was named the Most Admired Energy Company by *Fortune Magazine* consecutively between 1998 and 2002. Likewise, *Site Selection* magazine identified Duke Energy in 2012 as a top-10 best utility company in the United States for the fourteenth year in a row.[5] Duke Energy's success demonstrates that effective ERM implementation, which is often seen as a profit inhibitor, can actually yield highly profitable results.

CHAPTER 25

Dashboard Reporting

One of the key objectives of enterprise risk management (ERM) is to promote risk transparency, both in terms of internal risk reporting and external public disclosure. The old adage what gets measured gets managed holds true in risk management. A 2011 Deloitte study of approximately 1,500 cross-industry executives indicated that 86 percent of survey respondents identified "risk information reporting" as of high or moderate priority, making it the most highly prioritized of 13 risk initiative options. The second and third most prioritized initiatives were "risk data quality and management" at 76 percent and "operational risk measurement system" at 69 percent.[1] This study clearly demonstrates that establishing a robust risk measurement and reporting system is critical to ERM success.

However, many companies still approach risk reporting from the wrong angle. The reader may recall the 80/20 rule from the previous chapter, where data sources, analytics, models, and reports make up the base of the ERM process pyramid, with decision making on top. It would seem logical to start from the bottom of the pyramid and work our way up. Nevertheless dashboard reporting becomes much more effective when we start from the top, and first define business and risk management decision-making needs. Who is our audience? What kind of decisions do they make? From there, we can determine the metrics, analyses, and reports needed to support those decisions (and then which systems will produce those reports, as well as the data that these systems need, in turn).

When designing the structure and content of an ERM report, and the functionality of a dashboard reporting system, it is useful to start by articulating the key questions that the report is meant to address. For example, the ERM dashboard for the board and senior management may address the following five basic questions:

1. Are any of our business objectives at risk?

   The ERM dashboard should organize risk information (e.g., quantitative metrics, qualitative risk assessments, early warning indicators) in the

context of key strategic and business objectives. For each objective, the dashboard report would show green, yellow, or red indicators to signal that its achievement is on track, threatened, or off track, respectively. For objectives with yellow or red indicators, the board and management can then drill down to the underlying analyses.

2. Are we in compliance with policies, regulations, and laws?

   The ERM dashboard should include a compliance monitor that shows at a glance the company's compliance status with key policies, regulations, and laws. Traffic light signals would highlight whether the company is in full compliance (green), near violation (yellow), or in violation (red). Drill-down capabilities would enable further analysis with respect to more detained compliance metrics and reports.

3. What risk incidents have been escalated?

   In real time, the ERM dashboard should escalate critical risk incidents to the appropriate board members, executives, or managers. In order to support this feature, risk incidents that meet a defined threshold (e.g., customer impact, financial exposure, reputational impact, etc.) need to be captured throughout the company. Moreover, the ERM dashboard needs to have an embedded algorithm that would sort the risk incidents and escalate them to the right individuals.[2] The most sensitive and time-critical incidents should be pushed to the individuals' computers or smart phones as alerts to enhance timely communication and rapid response.

4. What key performance indicators (KPIs), key risk indicators (KRIs), or early warning indicators require attention?

   The ERM dashboard will report on the quantitative metrics that are the most relevant to the informational and decision-making needs of the audience. Ideally, each metric would include performance thresholds and/or risk tolerance levels against which the metric can be evaluated. Trend analysis and expert commentary should also be provided for the most important metric.

5. What risk assessments need to be reviewed?

   Risk assessments may include top-down risk assessments, bottom-up risk/control self assessments (RCSAs), regulatory examinations, and audit reports. Given that these assessments include mainly qualitative information, the key findings and analyses should be summarized. The risk assessment section of the ERM dashboard should provide an executive summary of these risk assessments, and highlight whether they meet board and management expectations (green), are near expectations (yellow), or are below expectations (red). The actual risk assessments and reports would be available for more detailed reviews.

For a typical company, it might take days or weeks to gather the required information to answer these five questions on an enterprise-wide basis. The fundamental problem is that the information is stored in different systems, databases, spreadsheets, and reports. Additionally, current approaches to risk reporting can be described as risk measurement by silos, with static reports that provide risk information for different risks separately. Static reports require significant manual work, resulting in more data integrity issues and less time for risk analysis and decision making.

With an effective dashboard reporting system, the board and management should be able to answer all five of these questions in a few minutes. A dashboard reporting system would provide executive reporting of enterprise-wide risks and drill-down capabilities so that all key risks can be monitored centrally. The key attributes of a dashboard reporting system include:

- A single point of access to all critical risk information that may reside in disparate risk systems and data sources.
- Executive reporting of enterprise-wide risks combined with drill-down capabilities to more granular risk data and analyses.
- Just-in-time risk information, delivered from real-time risk alerts to monthly credit reports to quarterly risk assessments.
- Quantitative KRIs integrated with qualitative risk assessments, policy documents, and external market data.
- The opportunity for users to provide commentary or analysis to the risk information presented by the dashboard reporting system.

TRADITIONAL VERSUS DASHBOARD REPORTING

It may be useful to distinguish dashboard reporting from traditional risk reporting. The main features of each type of reporting are summarized in Figure 25.1. Let's compare and contrast the key differences between traditional risk reporting and ERM dashboard reporting:

- *Approach to analysis:* Traditional risk reporting provides risk information in silos such as risk types, business units, and functional units. On the other hand, ERM dashboard risk reporting allows for a more integrated approach by evaluating the impact of risk on strategic objectives or examining the impact of one risk scenario (e.g. recession, counterparty default, or an extreme weather event) across all the risk types and business units of the organization.
- *Information reported:* Traditional risk reporting tends to focus on historical data and internal information. Since the ERM dashboard has

aggregated such information, the risk function has more time to focus on forward-looking analyses and early warning indicators, as well as external market data and macroeconomic trends.

- *Reporting flexibility:* With traditional reporting there is a trade-off between more or less information. Board members and executives may want more concise analysis and reports (i.e., executive summaries), while business and functional managers require more granular information to perform their operations. The drill-down capability of dashboard reporting eliminates this trade-off, allowing the board and executive management to view high-level risk information and analysis, while also providing the more granular information needed by the business and functional units.
- *Questions asked:* While traditional risk reporting considers mainly what-if questions (such as what if commodity prices go down), dashboard reporting can address more decision-oriented questions: So what if commodity prices go down? What should we do about it? With more advanced ERM dashboards that integrate not only information but also analytics, the board and management can review current risk sensitivities, as well as the impact of alternative strategies in real time. In other words, traditional reporting is data-driven while dashboard reporting is more action driven.
- *Interaction with information:* Traditional reporting is akin to reading a book while dashboard reporting is similar to searching for information on Google. With a book, you have to flip through the pages from beginning to end to find the information that you need, but it is difficult to get the specific information that you need in a timely manner. With Google, you can type in your search terms, which allows you to filter the vast amounts of information available so that you can find exactly what you need efficiently. As discussed earlier, the ERM dashboard should be able to address key questions, as well as provide summary and detail information, in order to meet the decision-making needs of the individual that is using it. Today, few people would go to the library instead of using Google to find information. Similarly, the board and management should have access to an efficient ERM dashboard instead of going through stacks of reports to get critical risk information.

GENERAL DASHBOARD APPLICATIONS

Dashboard reporting is becoming more common on all business levels from individual investors to corporate CEOs. According to Keithe Gile, an analyst from Forrester Research, Inc., approximately 40 percent of

FIGURE 25.1 Key Distinctions between Traditional Risk Reporting and Dashboard Reporting

the 2,000 largest companies had developed some form of dashboard reporting by 2006.[3] In fact, dashboards are becoming more common at the consumer level. Various forms of dashboards range from a personal data tool provided by Google to a service offered by JP Morgan to its investment customers. The JP Morgan service, called ACCESS Dashboard, combines information on market performance with links to the customer's investment portfolio. The dashboard application allows users to have a general view of their investment portfolios or to drill through detailed information.

Let's look at two other examples of dashboard reporting applications.

CNN Magic Map

My favorite example of dashboard reporting is the CNN magic map, which has been used during U.S. presidential elections since 2008. Originally developed by Jeff Han as a military tool, it was adopted by the cable news channel to provide viewers with election information in a highly visual and accessible manner. The map presents an image of the United States, with each state's color reflecting voter preferences for democrat or republican candidates. The map allows for a high-level view of the country's voting distribution as well as the opportunity to dig deeper if the viewer desires more information. By clicking on an individual state, the commentator can provide voting statistics by local districts, demographic segments, and even historical voting patterns. The CNN magic map is a great analog for dashboard reporting in its ability to display synthesized information as well as granular detail.

GE's Cockpit

Dashboard reports are being used with increasing frequency to improve communication within companies. For instance, CEOs and high-level executives across the board are also relying more and more on dashboard reporting to stay in the loop on company performance. James P. Campbell, Chief of General Electric's (GE) Consumer and Industrial Division, uses dashboard reports regularly: "I look at the digital dashboard the first thing in the morning so I have a quick global view of sales and service levels across the organization."[4] The value of the technology is that it is convenient and gives Campbell a broad picture of how GE is doing. After taking a look at the dashboard, Campbell can prioritize future actions.

GE Capital does not use a single dashboard report, but rather implements an entire system of different dashboards. Each business unit has a customized dashboard that fits in with their business structure. This dashboard reporting system, otherwise known as the cockpit, provides a general report on business unit performance to managers and was first implemented in 2001. Mike Stout, GE Capital's former Vice President and Chief Technology and Information Officer, describes the advantages of such a system: "It gives a tremendous amount of power to a general manager to manage a business by."[5] The dashboard system provides information on sales broken down by day, week, and month. It can also notify managers when loans are going into default or when customer service is lagging behind. Perhaps most valuable is the risk mitigation and response opportunity provided by the dashboard system. In creating a way to gather data on performance, the dashboard offers managers a chance to act to avoid future problems.

ERM DASHBOARD IMPLEMENTATION

While the implementation of ERM dashboards brings many challenges, the result can provide important benefits. We have already discussed how dashboard reporting can enhance enterprise-wide risk monitoring, board and management reporting, and decision support. With less time spent on gathering data and generating reports, another key benefit is that it would free up resources for the risk function to focus on developing more advanced analyses and risk strategies. The following are some useful steps to keep in mind in the implementation of an ERM dashboard system:

- *Assess the decision-making support needs of the audience:* Companies should first identify the needs of decision makers by drafting a prototype dashboard report and circulating it around the organization for specific feedback.

- *Develop KRIs:* Based on the feedback gathered in the previous step, companies should then develop the appropriate KRIs. These KRIs should provide quantitative metrics on risk exposures and early warning indicators.
- *Ascertain dashboard functionality:* The overall structure and functionality should be defined. These business requirements will then drive the selection and development of the appropriate technologies.
- *Avoid common pitfalls:* Finally, there are some common pitfalls associated with ERM dashboard implementation. We will review some of the key common pitfalls and how to avoid them.

Let's look at each step in turn.

Assessing Decision-Making Support Needs

The first and most important step in ERM dashboard implementation is to truly understand the decision-making requirements of the intended audience. In Chapter 24 we reviewed the general risk management decisions at the board, executive management, and business- and functional-unit levels. However, these decisions and the roles of specific committees, functions, and individuals are unique to each organization. As such, the ERM dashboard implementation team should take the following steps in assessing these decision-support requirements:

- Review current corporate risk policies, including policies that cover risk tolerance levels and limits (e.g., statement of risk appetite), delegation of authority, and risk escalation policy. A key area in these policies is the reporting requirements, including exception management and reporting.
- Review the charters of board and management risk committees and functions, including reports and minutes that may document the key discussions and decisions that these committees and functions have made in the past.
- Review existing reports, metrics, and risk assessments. It would be useful to highlight the specific risk analyses that are often used to support key decisions. The team should also review key performance goals and objectives of various risk committees and functions.
- Based on a solid understanding of reporting practices and requirements, select board members and managers should be interviewed to gather additional attributes and requirements.

Next the implementation team should design a paper ERM paper dashboard that is manually developed to document the desired structure and content in a working prototype (refer to Figure 3.1 for an example of a paper dashboard). This prototype should be socialized across the organization for

feedback. Prototype dashboard reports not only provide companies with a methodology of presenting information in a clear, dynamic manner, but also help them to identify critical gaps within existing reporting processes.

Developing Key Risk Indicators

The development of effective KRIs is a key challenge for most companies. Financial institutions usually have an abundance of credit risk and market risk indicators, but they are challenged in aggregating this data as well as developing operational risk indicators. On the other hand, non-financial institutions may have significant business and quality information derived from balanced scorecard and quality initiatives, but they may experience difficulties in developing KRIs for financial risk or technology risk. All companies face the challenge of establishing leading indicators that can effectively provide early warnings of potential future losses.

While the development of effective KRIs is a significant challenge, there are some readily available sources from which KRIs can be derived. Figure 25.2 provides an overview of the characteristics and sources of effective KRIs. The sources include:

- *Policies and regulations:* Regulations that govern the business activities of the company, as well as the corporate policies and limits established by management and the board, provide useful compliance KRIs. These KRIs may include risk exposures against limits or compliance with regulatory requirements and standards.

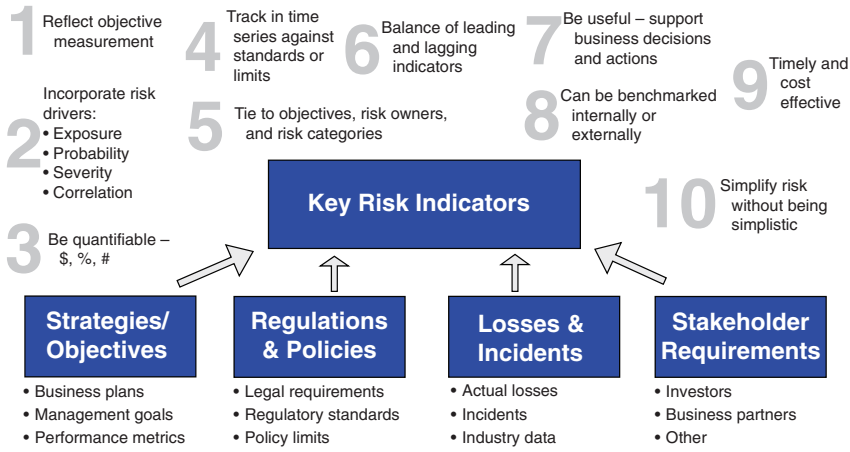


FIGURE 25.2 Sources and Characteristics of Effective KRIs

- *Strategies and objectives:* The corporate and business strategies established by senior management, and their associated performance metrics, are another good source. Note that performance metrics are designed to measure expected performance, whereas KRIs should be designed to measure downside risk or volatility of performance.
- *Previous losses and incidents:* Many companies have compiled loss/event databases that capture historical losses and incidents. These databases, or even anecdotal evidence, can provide useful input on what processes or events can cause financial or reputational loss. KRIs can then be developed for these processes and events.
- *Stakeholder requirements:* Beyond regulators, the expectations and requirements of other stakeholders—customers, rating agencies, stock analysts, business partners—can help in the development of KRIs based on variables that are important to these key groups.
- *Risk assessments:* Risk assessments performed by the company—including audit assessments, risk-control self assessments, and Sarbanes-Oxley tests—can provide valuable input on the business entities, processes, or risks where KRIs are needed.

Given the various sources for KRIs, the objective should be to develop a high-quality set of KRIs, rather than a high quantity of them. The following are ten key characteristics of effective KRIs:

1. Based on consistent methodologies and standards.
2. Incorporate risk drivers: exposure, probability, severity, and correlation.[6]
3. Be quantifiable: $, %, or #.
4. Track in time series against standards or limits.
5. Tie to objectives, risk owners, and standard risk categories.
6. Balance of leading and lagging indicators.
7. Be useful in supporting management decisions and actions.
8. Can be benchmarked internally and externally.
9. Timely and cost effective.
10. Simplify risk, without being simplistic.

ERM Functionality

While dashboard reports should be tailored to fit the specific needs of the organization, there are a few general functions that should be considered:

- *Basic and advanced statistical calculations:* Dashboard reports should provide basic statistical calculations, including mean, maximum, minimum, standard deviation, and confidence level. Beyond basic statistics,

dashboard reports should also provide data on positive and negative correlations and regressions (i.e., time-lagged regression).

- *Linkage between qualitative and quantitative data:* Dashboard reports should provide decision-makers with the means of combining qualitative and quantitative data in order to link business strategies, objectives, and KRIs.
- *Risk accountability and ownership:* Dashboard reports play a large part in monitoring risk escalation processes. In this regard, dashboard reports should track risk escalation policy violations through to resolution, explicitly assign monitoring, management, and oversight responsibilities, and also track risk mitigation projects.
- *Customized reporting and analysis:* Dashboard reports should be flexible in nature and be capable of presenting data in a multitude of different formats to suit the audience. While the ERM dashboard provides centralized risk reporting, the dashboard reports produced should be role-based. In other words, the reports made available to board members, senior executives, and business managers should be customized based on their informational and decision-making requirements.

Avoid Common Mistakes

With respect to dashboard reporting implementation, there are four common pitfalls that companies should avoid. These pitfalls, and strategies to overcome them, are as follows:

- Don't just integrate risks—break down organizational silos.
  - Dashboard reporting and, indeed, ERM in general, are not just about integrating the key risks—strategic, business, credit, market, and operational—into a common framework. They are also about breaking down organizational silos in order to identify interdependencies and make trade-off decisions. Most companies have established oversight functions such as risk management, audit, compliance, legal, treasury, and other oversight groups. The ERM dashboard should help break down organizational and reporting silos by facilitating a unified view of enterprise-wide risks.
- Don't boil the ocean—focus the dashboard reporting process on what is most important.
  - Given the wide scope of the dashboard implementation process, many companies are overwhelmed with their risk identification, assessment, documentation, and reporting procedures. The objective of dashboard reporting should not be to address all of the risks

faced by the company. Truthfully, it would be impossible to identify *all* of the company's risks because that list is infinite. The objective of dashboard reporting should be to support decisions on the critical risks and opportunities for the board of directors, executive management, and business and operational units. An effective dashboard reporting system should prioritize risk information for the company's key decision makers. As such, an indication of dashboard reporting success is not to say "We have identified 720 risks across the company, and fully documented related controls and risk assessments," but to say "We have identified the major risks that require the attention of various management groups, and supported their decisions for these major risks."

- Don't just tell me, show me—quantify risks through effective key risk indicators.
  - Many risk assessment processes produce large volumes of qualitative information that are not conducive to board and management decision making. In order to support policy and business decisions, critical risks must be quantified and reported in a concise and effective manner. That is not to say that quantitative information is more valuable than qualitative data, but there should be a balance in dashboard reporting. For the company's most critical risks, quantitative analysis can be used to show trends, risk-adjusted metrics, compliance with policy limits, and performance against established standards. For the same risks, qualitative analysis can be used to provide expert risk assessments, alternative strategies and actions, management recommendations, and other contextual information.
- Don't produce volumes of data and reports.
  - A dashboard report should not be a 50-page report that takes the risk committee two hours to simply walk through. A common complaint from board members and senior executives is that they cannot see the forest for the trees. Companies should develop an ERM dashboard that provides role-based information to key decision makers. During a board or management risk committee meeting, the ERM dashboard would enable board members and senior executives to first see high-level risk information. In addition, it should allow them to drill down to more granular data if they want to see more details. An exciting possibility is to develop the ERM dashboard so that it not only provides dynamic access to risk information, but also to risk analytical models. As such, it should also enable board members and senior executives to perform real-time scenario analysis, such as "How would a 30 percent increase in crude oil price impact our quarterly earnings, as well as market risk and credit risk exposures?"

EVOLVING BEST PRACTICES

In the past 10 years, technology applications have been focused on risk *quantification* in terms of analytical models, such as asset/liability models, Value-at-Risk (VaR) models, credit default models, and so forth. However, we are beginning to see a shift in technology toward focusing more on risk *communication* in terms of ERM reporting systems. An ERM reporting system, such as a dashboard, will provide board members, corporate executives, and risk professionals with a single point of access to all critical risk information—including objectives at risk, early warning indicators, KRIs against policy limits or performance standards, risk assessments and audit findings, escalations of issues and incidents, and risk-adjusted return performance. The time interval for enterprise-wide risk measurement and reporting will move from monthly to weekly to daily, and ultimately to real-time in the form of an electronic dashboard that updates itself.

The value of risk information is not in its development, but in its application. As such, to realize the full potential of ERM, risk professionals must deliver the right information, to the right decision makers, at the right time.

Notes

CHAPTER 1

1. Rawls, S. Waite III, and Charles W. Smithson (1990). "Strategic Risk Management," *Journal of Applied Corporate Finance* 2, no. 4 (Winter).
2. Tufano, P. (1998). "The Determinants of Stock Price Exposure: Financial Engineering and the Gold Mining Industry," *Journal of Finance* 53, 1015–1052.
3. Jin, Yanbo, and Philippe Jorion. "Does Hedging Increase Firm Value? Evidence from the Gold Mining Industry," July, 2007, 15. California State University.
4. Mancini, Massimo. "Corporate Risk Hedging Strategies and Shareholders' Value Creation: The Southwest Airlines Case," June 2, 2009, 9. Kellogg School of Management.
5. Stewart, James B. "The Omen," *The New Yorker,* October 20, 2008.
6. Ibid.
7. Luchetti, Aaron, et al. "A Year Later, All Eyes Still on 'Edie'," *Wall Street Journal,* October 30, 2012.
8. Rapoport, Michael, "MF Global Masked Debt Risks," *Wall Street Journal,* November 4, 2011.
9. Ibid.
10. Sherter, Alain. "Jon Corzine Resigns as MF Global Scandal Deepens," *CBS News,* November 4, 2011.

CHAPTER 3

1. In this context, new business includes mergers and acquisitions.
2. See Chapter 9 for a more detailed discussion on expected loss, unexpected loss, and economic capital.
3. For example, a loan or security that is downgraded (widening in credit spread) would incur a mark-to-market loss even though no defaults or charge-offs have occurred. Marking the credit portfolio to market using credit spreads provides an economic assessment of credit losses.

CHAPTER 4

1. Other popular terms used to describe enterprise risk management include firm-wide risk management, integrated risk management, and holistic risk management.
2. Winokur, L. A. "The Rise of the Risk Leader: A Reappraisal," *Risk Professional*, April 2012, 20.
3. Davy, Peter. "Cinderella Moment," *Wall Street Journal*, October 5, 2010.

4. Lam, James. "Structuring for Accountability," *Risk Professional*, June 2009, 44.
5. Banham, Russ. "Disaster Averted," *CFO Magazine*, April 1, 2011, 2.
6. Ibid.
7. Winokur, L. A. "The Rise of the Risk Leader: A Reappraisal," *Risk Professional*, April 2012, 17.
8. Hofmann, Mark A. "Average Chief Risk Officer's Salary Nearly $184,000: RIMS," *Business Insider*, April 24, 2013.

CHAPTER 5

1. Robert A.G. Monks and Nell Minow, Corporate Governance (United Kingdom: Blackwell Business, 1995).
2. "CalPERS' Corporate Governance Core Principles and Guidelines," 1995, p. 3.
3. Toronto Stock Exchange Committee on Corporate Governance and the Institute of Corporate Directors, "Report on Corporate Governance, 1999: Five Years to the Dey," 1999, co-chair's letter.
4. Financial Reporting Council, "Developments in Corporate Governance 2011: The Impact and Implementation of the UK Corporate Governance and Stewardship Codes," December, 2011, p. 1.
5. The term stakeholders here refers not only to corporate shareholders, but also to employees, suppliers, and the general public wherever they have a direct interest in the affairs of the corporation.
6. Charles J. Woelfel, Encyclopedia of Banking and Finance, 10th ed. (Chicago: Probus Publishing Company, 1994), p. 939.
7. "The Cadbury Report 4.12," 1992, p. 22.
8. "The Combined Code," 2000, Principle A.2.
9. "CalPERS' Corporate Governance Core Principles and Guidelines," 1995, p. 5.
10. "The Dey Report," 1994, Guideline 12.
11. "General Motors Board Guidelines," 1994, Guideline 22.
12. "1996 NACD Report," p. 4.
13. "The Dey Report," 1994, Guideline 5.
14. "1996 NACD Report," p. 23.
15. Toronto Stock Exchange Committee on Corporate Governance and the Institute of Corporate Directors, "Report on Corporate Governance, 1999: Five Years to the Dey," 1999, p. 19.
16. Jeff Cossette, "Can Board Self-Assessment Work?," *Insider Investor Relations,* Feb 1, 2005.
17. "General Motors Board Guidelines," 1994, Guideline 15.
18. "Non-US Firms Compete Through Good Governance," Investor Relations Business, March 6, 2000.
19. Ibid.
20. "1996 NACD Report," p. 6.
21. "General Motors Board Guidelines," 1994, Guideline 36.
22. "Campbell Soup Company Corporate Governance Standards," October 1, 2012, Guideline 39.
23. For example, see the National Association of Corporate Directors' "1995 Report of the NACD Blue Ribbon Commission on Director Compensation" and

the Conference Board of Canada's "Compensation of Boards of Directors," 1998 and every 2 years previously for approximately 20 years.
24. "The Combined Code," 2000, Principle D.1.
25. "The Dey Report," 1994, Guideline 8.
26. General Motors Company Board of Directors: Corporate Governance Guidelines (Index), Guideline 19.
27. "GE Proxy Statement 2007: Non-management Directors' Compensation for Fiscal 2006," February 28, 2007.
28. "Bank of Montreal 1998 Annual Report," p. 101.
29. "The Dey Report," Guideline 1(ii) and the "OECD Principles of Corporate Governance, 2004, Principle D7.
30. Toronto Stock Exchange Committee on Corporate Governance and the Institute of Corporate Directors, "Report on Corporate Governance, 1999: Five Years to the Dey," 1999, p. 8.
31. Brown, David, Debra Brown, and Kimberley Birkbeck, Canadian Directorship Practices 1997: A Quantum Leap in Governance (Ottawa: The Conference Board of Canada, 1998).
32. Strategic Risk Council, www.conferenceboard.ca/networks/src/membership.aspx.
33. "JP Morgan Chase & Co. 2011 Annual Report," p. 125.
34. Author's note: While JP Morgan Chase has long been recognized as a leading institution in ERM, it faced its share of challenges in the "London Whale" incident in 2012. The events and lessons learned will be discussed in Chapter 22.
35. "CompuTrac Announces Restructuring of CEO's Compensation," *Business Wire*, December 11, 1998.
36. Brodeur, André, Gunnar Pritsch, "Making Risk Management a Value-Adding Function in the Boardroom," *McKinsey & Company,* working paper, September, 2008, p. 4.

CHAPTER 6

1. Lam, James. "Custom-Built for Success," *Risk Magazine*, Enterprise-Wide Risk Management Supplement, November 1997.
2. China Briefing. "Avon Bribery Case May Face U.S. Grand Jury Investigation," *China Briefing*, February 14, 2012.
3. Connor, Michael. "Daimler Agrees to Pay $185 Million to Settle Bribery Charges," *Business Ethics*, March 26, 2010.
4. U.S. Securities and Exchange Commission, "SEC Approves Enhanced Disclosure About Risk, Compensation and Corporate Governance," Rule 2009-268, December 16, 2009.
5. White, Martha C. "Clawback Provisions Go Mainstream, Add Reach," *NBC-News.com*, 2012.

CHAPTER 7

1. Markowitz, Harry. "Portfolio Selection," *Journal of Finance* 7, no. 1, (1952), 77–91.
2. Mintz, Steven. "The Gurus," *CFO Magazine (online edition)*, January 2000.
3. Jastrow, David. "Ikon Delivers in the Eye of the Storm," *Computer Reseller News*, September 27, (1999), 65.

CHAPTER 8

1. "Insurance Market Report 2013," *Marsh & McLennan Companies,* February 2013, 4.
2. Group of Thirty. *Global Institutions, National Supervision and Systemic Risk*, 1997, 9.
3. Westover, Kate. "Appreciating Benefits of Finite Risk Products," *Business Insurance,* February 20, 2005.
4. Conley, John. "Risk Coverage Coup," *Global Finance*, Volume 13, Issue 4, April 1999.
5. Banham, Russ. "Kit and Caboodle," *CFO: The Magazine for Senior Financial Executives*, April 1999.
6. Carlson, Neil F. "Global Risk Management," *Strategic Finance*, Volume 81, Issue 2, August 1999.
7. Banham, Russ. "Kit and Caboodle," *CFO: The Magazine for Senior Financial Executives*, April 1999.
8. Ibid.
9. Watkins, Mary. "Barclays Bond a Key Test for CoCo Market," *Financial Times,* November 22, 2012.

CHAPTER 9

1. "Guidance on Stress Testing for Banking Organizations with Total Consolidated Assets of More Than $10 Billion." *Board of Governors of the Federal Reserve System.* May 14, 2012. Available at http://www.federalreserve.gov/bankinforeg/srletters/sr1207a1.pdf.
2. Board of Governors of the Federal Reserve System, "Comprehensive Capital Analysis and Review 2013: Summary Instructions and Guidance," November 9, 2012, p. 1.
3. "Comprehensive Capital Analysis and Review 2012: Methodology and Results for Stress Scenario Projections." *Board of Governors of the Federal Reserve System.* March 13, 2012. Available at http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20120313a1.pdf.
4. "Dodd-Frank Act Stress Test 2013: Supervisory Stress Test Methodology and Results." *Board of Governors of the Federal Reserve System.* March 2013. Available at http://www.federalreserve.gov/newsevents/press/bcreg/dfast_2013_results_20130314.pdf, p. 1.
5. Ibid., 15.
6. Ibid., 9.
7. Torres, Craig, and Joshua Zumbrun."Fed Stress Tests Show 17 of 18 Banks Weathering Severe Slump. *Bloomberg*. March 7, 2013. http://www.bloomberg.com/news/2013-03-07/fed-stress-tests-show-17-of-18-banks-weathering-severe-recession.html.
8. Merton, Robert C. "On the Pricing of Corporate Debt: The Risk Structure of Interest Rates." *The Journal of Finance*, 29, (1974), 449–470.
9. Bumiller, Elisabeth. "Corporate Conduct: The President; Bush Signs Bill Aimed at Fraud in Corporations," *The New York Times,* July 31, 2002.
10. Proctor, Paul E. "MarketScope for IT Governance, Risk and Compliance Management," *Gartner,* June 7, 2013.

CHAPTER 11

1. Reichheld, Frederick F. *The Loyalty Effect* (Cambridge: HBS, 1996), 4.
2. "PwC 16th Annual Global CEO Survey," 2013, 22.
3. Levering, Robert, and Milton Moskowitz. "Beyond Perks: Lessons from Tracking the '100 Best'," *Fortune,* January 20, 2011.
4. "Changes in the Labor Market Leads to Increase in Free Agent Workforce, According to Kelly Services, Inc.," *Kelly Services,* August 15, 2011.
5. Bernstein, Aaron. "What Price Peace?" *Business Week*, August 10, 1998, 24–25.
6. Drucker, Peter F. "The New Society of Organizations," *Harvard Business Review*, September–October 1992, 100.
7. "Don't Let the Talent Crunch Hurt Your Company's Chance for Success," *PR Newswire*, June 8, 1999.
8. "100 Best Companies to Work For: Snapshots," *Fortune,* 2012.
9. Ibid.
10. Branch, Shelly. "The 100 Best Companies to Work for in America." *Fortune,* January 11, 1999, 119.
11. DuBois, Shelley. "Internal Competition at Work: Worth the Risk?" *Fortune,* January 25, 2012.
12. Hymowitz, Carol, and Matt Murray. "How GE's Chief Rates and Spurs His Employees," *Wall Street Journal,* June 21, 1999, B1.
13. Frenz, Helena. "Don: Need to Ensure that Customers Are Fully Satisfied," *Business Times*, 8 February 1999, 3.
14. Reichheld, Frederick F. *The Loyalty Effect.* (Cambridge: HBS, 1996), 33–37; Victor L. Hunter, *Business to Business Marketing: Creating a Community of Customers,* (NTC Business Books, 1997).
15. Genesys, "The Cost of Poor Customer Service: The Economic Impact of the Customer Experience and Engagement in 16 Key Economies," November 2009, 2.
16. Ibid., 4.
17. Ibid., 5.
18. Hart, Christopher W. "Beating the Market with Customer Satisfaction," *Harvard Business Review,* March 2007.
19. Foster, Graham, and Karin Newman. "What Is Service Quality When Service Equals Regulations?" *Service Industries Journal Vol. 18 No. 4*, October 1998, 51–65.
20. Anderson, Jeff . "Automotive Industry Insights," *Experian,* 2013, 29.
21. "Point of View: New SEC Rule Prompts Companies to Disclose How Their Boards Oversee Risks," *PricewaterhouseCoopers,* May 2010.
22. "Over-Regulated America," *The Economist,* February 18, 2012.
23. Fitzpatrick, Dan, et al. "Banks Present Plan for Crisis Response," *The Wall Street Journal,* June 24, 2013.
24. "North American and Bermudan Insurers Continue to Step Up Their ERM Efforts," *Standard & Poor's*, May 3, 2011, 3.
25. "Evaluating the Enterprise Risk Management Practices of Insurance Companies," *Standard & Poor's*, October 17, 2005, 4.
26. Ibid., 5.

27. "Evaluating the Enterprise Risk Management Practices of Insurance Companies," *Standard & Poor's*, October 17, 2005, 8.
28. "Methodology: Assessing Management's Commitment to and Execution of Enterprise Risk Management Processes," *Standard & Poor's*, December 17, 2009, 4–5.
29. "Enterprise Risk Management Continues to Show Its Value for North American and Bermudan Insurers," *Standard & Poor's*, February 1, 2010, 2.
30. CtW Investment Group, "Who We Are," http://www.ctwinvestmentgroup.com/index.php?id=1.
31. Copland, James R. "Politicized Proxy Advisers vs. Individual Investors," *Wall Street Journal,* October 7, 2012.
32. Ibid.
33. Moyer, Liz. "Goldman World Apart from J.P. Morgan as Investor Meeting Looms," *Wall Street Journal,* May 23, 2013.
34. Tribbett, Charles. "Splitting the CEO and Chairman Roles—Yes or No?." Directors & Boards, December 2012, 5.
35. Ibid., 3.
36. "Institutional Shareholder Services Annual Survey," *Ethic Intelligence*, September 2012.
37. Dunn, Gibson. "Institutional Shareholder Services (ISS) and Glass Lewis Proxy Voting Policies and Other Developments for the 2013 Proxy Season," January 29, 2013.
38. Ibid.
39. Harper, Pamela S., and D. Scott Harper, "Building Powerful Strategic Alliances: How Companies of All Sizes Can Increase Their ROI," 2012, 3.
40. Rock, Glen. "Reasons for Failure and Success of Strategic Alliances Revealed by New In-Depth Study from Business Advancement, Inc.," *Yahoo! Finance,* November 28, 2012.
41. Sanger, Deborah. "Why Joint Ventures Fail," *Saul Ewing LLP,* January 2004.
42. For a more in-depth treatment of these issues, see C. Christopher Baughn, Johannes G. Denekamp, John H. Stevens, and Richard N. Osborn, "Protecting Intellectual Capital in International Alliances," *Journal of World Business* 32, no. 2 (1997): 103–115.

CHAPTER 12

1. "Principles for the Management of Credit Risk", Consultative paper by the Basel Committee on Banking Supervision, July 1999.
2. Note that we always assume that the exposure is at best zero but never negative; if the firm represents an exposure to the counterparty it is highly unlikely that the firm will benefit from the counterparty's default: either a successor entity or a court appointed administrator will eventually collect.
3. Economic capital is defined as the level of capital that is needed to cover unexpected losses, whereas book capital is the actual capital on the balance sheet and regulatory capital is based on capital requirements from the regulators.
4. Some lending institutions incorporate warrants or other equity-like features into their lending programs in order to capture some upside.

5. The short-term interest rate has a long-term reversion to a mean of 6 percent; its adjusted volatility is 7.5 percent.
6. "Trading Activities Manual—Part 1," Federal Reserve System, March 1994, 1–74.
7. Today, commercial agencies rate more than 2,000 U.S. companies and corporate issues are rated, but only around 250 European companies are rated.
8. "Principles for the Management of Credit Risk," Consultative Paper issued by the Basel Committee on Banking Supervision, July 1999.
9. A downgrade trigger would allow any one of the counterparties to terminate a transaction if the other's credit rating falls below a certain level.
10. A netting agreement would allow two counterparties to net their payment obligations.
11. A commercial loan held on the balance sheet of a financial institution is subject to double taxation given that both the financial institution and its equity holder must pay income tax. In contrast, an investor of the same loan held in a mutual fund or hedge fund is taxed only once.
12. Basel Committee on Banking Supervision, *A New Capital Adequacy Framework*, Basel, June 1999.
13. Ibid.
14. "Basel III Summary—Guide to the Changes," *Basel II Risk*, August 24, 2012.
15. Accenture, "Basel III Handbook," 2012, 16.
16. Ibid., 25.
17. Auer, Michael, Jacek Kochanowicz, and Georg von Pfoetsl, "Basel III and Its Consequences: Confronting a New Regulatory Environment," 2011, 5.
18. Hårle, Philipp, et al., "Basel III and European Banking: Its Impact, How Banks Might Respond, and the Challenges of Implementation," working paper, 2.
19. "Basel III: Issues and Implications," *KPMG*, 2011.
20. "Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems," *Bank for International Settlements*, December 2010, 9.
21. Ibid., 15–16.
22. Ibid., 11–12.
23. "Basel III Tackles Systemic Risk and Counterparty Risk," *Risk.net*.
24. Salmon, Felix. "The Biggest Weakness of Basel III," *Reuters,* September 15, 2010.
25. Millman, Noah, "Third Time's the Charm?" *The Economist,* September 13, 2010.
26. Ibid.

CHAPTER 13

1. Klayman, Ben and Deppa Seetharaman. "GM to Cut about One-Fourth of U.S. Pension Liability," *Chicago Tribune,* June 1, 2012.
2. Muller, Joann, "Ford's Leaky Pension Boat Is a Multi-Billion Dollar Problem," *Forbes,* January 31, 2013.
3. RiskMetrics is a set of tools developed by J.P. Morgan that enables participants in the financial markets to estimate their exposure to market risk under the Value-at-Risk framework.
4. Linear means that if the value of the portfolio changes by x when a rate changes by 1 percent, then the change due to a 2 percent move is 2x.

5. Chase Manhattan Corporation 1998 *Annual Report*.
6. Carver, Laurie. "Basel Committee Proposes Scraping VaR," *Risk Magazine,* May 3, 2012.
7. Ibid.
8. Ibid.
9. Carver, Laurie. "Basel Committee Proposes Scraping VaR," *Risk Magazine,* May 3, 2012.

CHAPTER 14

1. Deloitte, "Global Risk Management Survey, 7th Edition: Navigating in a Changed World," February 2011, 42.
2. Deloitte, Management of Operational Risks in Insurance, June 2007.
3. Schrage, Michael. "UBS Systems Failed the 'Too Big to Fail' Bank." *Harvard Business Review,* September 20, 2011.
4. Ibid.
5. Basel Committee on Banking Supervision, "Principles for the Sound Management of Operational Risk," June 2011, 3.
6. Thomson Reuters, "Why You Should Worry About Operational Risk," December 2012, 4.
7. *Capital Markets Report*, March 24, 1999.
8. Fishkin, Charles A. "Controlling the Documentation Vortex," *MiddleOffice* Spring 2000, 13–17.
9. Davidson, Clive. "Knight Capital Losses Spur Focus on Algo Risk Management," *Risk Magazine,* September 6, 2012.
10. Ibid.
11. Smith, Ned. "Retail Inventory Shrinkage Has Shrunk." *Business News Daily,* November 28, 2012.
12. *Risk Budgeting*. (London: Risk Books) 2000.
13. Campbell, Alexander. "OpRisk North America: Billion Dollar Losses Are the Result of Op Risk Failure," *Risk.net,* March 21, 2013.
14. See Paul Embrechts, et al, *Modelling Extreme Events for Insurance and Finance* (1997) for details.
15. Stamford Risk Analytics, Home Page.
16. Wladawsky, Irving. "Spotting Black Swans with Data Science," *Wall Street Journal*, May 17, 2013.
17. Stamford Risk Analytics, Home Page.
18. Department of Defense, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013, 2.
19. Martinez, Luis. "Intel Heads Now Fear Cyber Attack More Than Terror." *ABC News,* March 13, 2013.
20. Barlyn, Suzanne. "Cyber Attack Briefly Shutters Charles Schwab Website," "*Yahoo! News,* April 23, 2013.
21. Roman, Jeffrey. "Cybersecurity: The Role of DHS," *Bank Info Security,* March 4, 2013.
22. Raul, Alan Charles. "Cybersecurity—It's Not Just About 'National Security' Anymore: "Director's Desk" and Other Incidents Sound Wake-up Call for the Executive Suite and Board Room." *Privacy and Security Law Report,* 4.

23. Department of Defense, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," 82–83.
24. Columbus, Louis. "Making Cloud Computing Pay," *Forbes,* April 10, 2013.
25. Chan, Warren, Eugene Leung, and Heidi Pili. "Enterprise Risk Management for Cloud Computing." June 2012, 8.
26. Ibid., 12.
27. Crouse, Becca. "Social Media Negatively Impacts Employee Productivity: Surprise, Surprise!." *March Communications,* September 28, 2012.
28. Ibid., 4.

CHAPTER 16

1. While our focus in this chapter is on banks, thrifts, securities firms, and insurance companies, the issues discussed are directly relevant to the financial and insurance operations of any corporation.
2. FDIC, "Statistics at a Glance," December, 2012.
3. Standard & Poor's Industry Surveys—Banking. November 7, 2002.
4. PwC, "Balancing Uncertainty and Opportunity: 2012 Financial Services, M&A Insights," March 2012, 3.
5. Avraham, Dafna, Patricia Selvaggi, and James Vickery. "A Structural View of U.S. Bank Holding Companies," FRBNY Economic Policy Review, July 2012, 65.
6. Morgan Stanley Dean Witter Insurance Industry Quarterly Review on Insurance Brokers, March 10, 1999.
7. Roberts, Sally. "Consolidation Among Brokerages Builds Global Capabilities," *Business Insurance*, October 7, 2007.
8. Heffernan, Margaret. "Why Mergers Fail," *CBS News*, April 23, 2012.
9. Towers Watson, "US Acquirers Lag Behind Asia-Pacific and European Peers," 2012, 2.
10. Case 9-897-177, Harvard Business School Publishing.
11. FDIC, "FDIC Community Banking Study," December 2012, 1.
12. PaineWebber Industry Report, April 13, 1999.
13. Davies, Howard. "The Financial Crisis: Who's to Blame?" London School of Economics, September 28, 2010.
14. Ibid.
15. The Federal Reserve Board. "Remarks by Chairman Alan Greenspan," October 19, 2004.
16. Mollencamp, Carrick, et al. "Behind AIG's Fall, Risk Models Failed to Pass Real-World Test," *Wall Street Journal*, October 31, 2008.
17. The Federal Reserve Board. "Four Questions about the Financial Crisis," April 14, 2009.
18. Steele, David A. "The New Financial Deal: Understanding the Dodd-Frank Act and Its (Unintended) Consequences," Wiley: 2010, abstract.
19. Section 165, Dodd-Frank Wall Street Reform and Consumer Protection Act.
20. Section 1851, United States Code, 2011 Edition.
21. Chambers, Matthew A., et al. "SEC Adopts Compensation, Corporate Governance and Risk Disclosure Changes," December 18, 2009.

22. Ibid.
23. Wilmarth, Jr., Arthur E. "The Dodd-Frank Act: A Flawed and Inadequate Response to the Too-Big-To-Fail Problem," April 19, 2011, abstract.
24. Ibid.
25. Ernst & Young, "The Road to Re-Regulation: Views from the Financial Services Industry," 2010, 2.
26. Ibid., 2.

CHAPTER 17

1. "What Is the Future for Oil and Gas?" *World Energy Outlook 2012 Fact Sheet 2012.*
2. "Gas Boom Projected to Grow for Decades," *Wall Street Journal,* February 28, 2013.
3. Holmes, Jamie. "The Natural Gas Myth," *Slate Magazine,* November 15, 2012.
4. *Energy Central*, April 5, 1999.
5. Deloitte, "Risk Intelligence in the Energy & Resources Industry," 2010, 12.
6. Ibid., 11.
7. Deloitte, "Risk Intelligence in the Energy & Resources Industry," 2010, 6.
8. See Chapter 10 for detailed discussions of VaR models.
9. Labuszewski, John W., et al. "Volatility Monitor: 1st Quarter, 2013," April 2, 2013, 5.
10. Smith, Rebecca. "Overloaded Circuits: Outage Signals Major Weakness in U.S. Power Grid," *Wall Street Journal,* August 18, 2003.
11. Plumer, Brad. "Bad News: The U.S. Power Grid Is Getting Pricier, Less Reliable," Washington Post, March 8, 2013.
12. Krauss, Clifford, et al. "BP Will Plead Guilty and Pay Over $4 Billion," *New York Times*, November 15, 2012.
13. *Atmospheric and Environmental Research,* 2012.
14. Ibid., 2.
15. Calvert Investments, "Physical Risks from Climate Change," May 2012, 2.
16. Ibid., 12.
17. Ibid., 13.
18. Ibid., 18.
19. Ibid., 18.
20. Ibid., 19.
21. "The Facts about Fracking," *Wall Street Journal,* June 25, 2011.
22. "Should the Federal Government Regulate Fracking?" *Wall Street Journal,* April 12, 2013.
23. Ibid.
24. "Question of the Day: Should Fracking Be Allowed in Your State, and with What Kind of Regulation?" *Wall Street Journal,* June 3, 2013.
25. "Should the Federal Government Regulate Fracking?," *Wall Street Journal,* April 12, 2013.
26. Ibid.
27. Harvey, Fiona. " 'Golden Age of Gas' Threatens Renewable Energy, IEA Warns." *The Guardian,* May 29, 2012.
28. Inman, Mason. "Shale Gas: A Boon that Could Stunt Alternatives, Study Say," *National Geographic,* January 17, 2012.

29. Casselman, Ben, and Russel Gold. "BP Decisions Set Stage for Disaster," *Wall Street Journal,* May 27, 2010.
30. Berzon, Alexandra, et al. "There Was 'Nobody in Charge'," *Wall Street Journal,* May 28, 2010.
31. Ibid.
32. "Black Swan of Black Sheep? Risk Management Lessons from the Gulf Oil Spill," *Risk Management Magazine,* April 1, 2011.

CHAPTER 18

1. For further information on FAS 133, please refer to the web site: www.fas133.com.
2. "Big Chemical Firms To Halt Operations On New Year's Eve," *The Wall Street Journal,* October 3, 1999.
3. "Exxon-Mobil Merger Faces Legal Threat: Wednesday Deadline Set for Accord on Asset Sale," *The Dallas Morning News,* September 24, 1999.
4. Cole, Jeff. "Ante Up! Big Gambles in the New Economy—Flight of Fancy: Airbus Prepares to 'Bet the Company' as It Builds a Huge New Jet," *The Wall Street Journal,* November 3, 1999.
5. Spence, Katie. "Boeing vs. Airbus: Who Will Win the "Mini-Jumbo" Battle?" *Daily Finance,* May 4, 2013.
6. Ibid.
7. Daft, Richard L. *Organization Theory and Design*. (Cincinnati: South-Western College Publishing) 1998, 4.
8. Monga,Vipal. "Lightening the Pension Load." *Wall Street Journal,* November 6, 2012.
9. Ibid.
10. Monga, Vipal. "Dealing with the Pension Deficit," *Wall Street Journal,* November 12, 2012.
11. Deloitte, "2012 Global Outsourcing and Insourcing Survey: Executive Summary," February 2012, 7.
12. Basel Committee on Banking Supervision "Outsourcing in Financial Services," February 2005, 5.
13. Levick, Richard. "Spotlight on Outsourcing: Boeing Scrambles as Toyota Triumphs," *Forbes,* January 30, 2013.
14. Ensign, Rachel Louise. "How Can Companies Keep Outsourced Data Safe?" *Forbes,* May 24, 2013.
15. Tomkins, Richard. "Assessing a Name's Worth," *Financial Times*, Tuesday, June 22, 1999.
16. "Rat Poison Probe Under Way at French Coca-Cola Plant," *Financial Times*, June 24, 1999; and Neil Buckley, Michael Smith and Robert Graham, "Coca-Cola Apology to Belgian Consumer," *Financial Times*, Tuesday, June 22, 1999.
17. "Coca-Cola 21% Down on Earnings," *Financial Times*, July 16, 1999.
18. "Coke Recall Cost Is Put at Dollars 60m," *Financial Times*, June 25, 1999.
19. www.bloomberg.com
20. Teach, Edward. "Microsoft's Universe of Risk," *CFO, The Magazine for Senior Financial Executives*, March 1997.

21. Lange, Scott. "Going 'Full Bandwidth' at Microsoft," *Risk Management*, July 1996.
22. Teach, Edward. "Microsoft's Universe of Risk," *CFO, The Magazine for Senior Financial Executives*, March 1997.
23. Lange, Scott. "Going 'Full Bandwidth' at Microsoft," *Risk Management*, July 1996.
24. Banham, Russ. "Kit and Caboodle," *CFO: The Magazine for Senior Financial Executives*, April 1999.
25. Lange, Scott. "Going 'Full Bandwidth' at Microsoft," *Risk Management*, July 1996.
26. Ibid.
27. Ceniceros, Robert. "Sharing, Integrating Risk Management Information Made Even Easier with Companywide Intranet," *Business Insurance*, December 1997.
28. Birkbeck, Kimberley. *Integrating Risk Management: Strategically Galvanizing Resources in the Organization, Proceedings of the 1998 International Conference on Risk Management*, The Conference Board of Canada, Ottawa, April 1998.
29. Trudell, Craig. "Ford CEO Mulally Reiterates Plan to Lead Company through 2014," *Bloomberg Businessweek,* May 9, 2013.
30. Hammond, Lou Ann. "How Ford Stayed Strong Through the Financial Crisis," *CNN Money,* January 13, 2011.
31. Clark, Andrew. "Automotive Industry: Carmaker Ford Facing Dire Financial Crisis," *The Guardian,* June 20, 2008.
32. Hammond, Lou Ann. "How Ford Stayed Strong Through the Financial Crisis," *CNN Money,* January 13, 2011.
33. Michaels, Daniel. "Hit by Delays, Airbus Tries New Ways of Building Planes," *Wall Street Journal,* July 22, 2012.
34. Ibid.
35. "Airbus Officials Cite Problems," *Wall Street Journal,* June 10, 2010.

CHAPTER 19

1. Scotti, Bill. "Risk Management Predictions: A Look Back," *Risk Professional,* June, 2012.

CHAPTER 21

1. "Investor Opinion Survey," McKinsey & Company, July 8, 2002.
2. The Corporate Governance Quotient is an Institutional Shareholder Services metric designed to measure the effectiveness of a company's corporate governance structure.
3. Brown, Lawrence D., and Marcus L. Caylor. "Corporate Governance Study: The Correlation between Corporate Governance and Company Performance: Abstract," 2004, 1.
4. Cheng, Daniel, and Yi-Yen Wu. "Evolving Corporate Governance and Equity Prices: The Recent Evidence," 2005, 1.

5. Brown, Lawrence D., and Marcus L. Caylor. "Corporate Governance Study: The Correlation between Corporate Governance and Company Performance: Abstract," 2004, 5.
6. Ibid.
7. Hoyt, Robert E., and Andre P. Liebenberg. "The Value of Enterprise Risk Management," *Journal of Risk and Insurance*, July 30, 2009.
8. "Enterprise Risk Management Continues To Show Its Value for North American and Bermudian Insurers," Standard & Poor's, February 1, 2010.
9. Pergler, Martin. "What's Different in the Corporate World," *McKinsey & Cos.*, December 2012, 2.
10. Crish, Michele, et al. "Enterprise Risk Management for Internal Auditors," *Deloitte,* May 18, 2012.

CHAPTER 22

1. "Concerns about Risks Confronting Boards: First Annual Board of Directors Survey," *Eisner LLP,* 9.
2. "Board Risk Oversight: A Progress Report," *Protiviti,* December 2010, 4.
3. See "SEC Adopts Rules on Provisions of Sarbanes-Oxley Act," SEC 2003-6, January 15, 2003.
4. The Directors and Chief Risk Officers Group, "Qualified Risk Director Guidelines," June 3, 2013.
5. In addition to the London Whale incident discussed here, in July 2013, J.P. Morgan agreed to pay $410 million to settle U.S. Federal Energy Regulatory Commission allegations that the bank manipulated power markets.
6. Ibid.
7. Fitzpatrick, Dan, et al. "J.P. Morgan's $2 Billion Blunder," *Wall Street Journal,* May 11, 2012.
8. Rapport, Michael. "J.P. Morgan Risk Management Is Assailed," *Wall Street Journal,* March 14, 2013.
9. Craig, Susanne, and Jessica Silver-Greenberg. "A Call for New Blood on the JPMorgan Board," *Wall Street Journal,* May 5, 2013.
10. Ibid.
11. Abelson, Max. "JP Morgan's Risk Committee Cut in Half as Futter, Cote Exit Board," *Bloomsberg Businessweek,* July 19, 2013.
12. Fitzpatrick, Dan, et al. "J.P. Morgan's $2 Billion Blunder," *Wall Street Journal,* May 11, 2012.
13. Brodeur, André, and Gunnar Pritsch. "Making Risk Management a Value-Adding Function in the Boardroom," *McKinsey & Company,* working paper, September 2008, 6.

CHAPTER 23

1. Lam, James. "Risk Assessment Guide," Association for Financial Professionals, 2011.
2. "Expectations of Risk Management Outpacing Capabilities—It's Time For Action." KPMG 2013.

3. "Enterprise Risk Management in Practice," Protiviti, 2007, 6.
4. "Global Financial Leader Deploys Solution for Compliance and Operational Advantages," Microsoft, July 2008.
5. Ibid., 8.
6. "Global Risks 2011, Sixth Edition." World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_ExecutiveSummary_2011_EN.pdf
7. "Global Risks 2007." World Economic Forum, 6.

CHAPTER 24

1. See Chapter 8 for more details on specific ART products.
2. Bernard Wysocki Jr., "Power Grid: Soft Landing or Hard?" *Wall Street Journal,* July 7, 2000.
3. Ibid.
4. "2012 Annual Report and Form 10-K," *Duke Energy,* 2012, p. 5.
5. Ibid.

CHAPTER 25

1. "Global Risk Management Survey, 7th Edition: Navigating in a Changed World," *Deloitte,* February, 2011, p. 42.
2. Ideally, a risk escalation policy is established that will provide the criteria for how risk incidents are reported to various levels of the organization.
3. "Giving the Boss the Big Picture," *Bloomberg Businessweek,* February 12, 2006.
4. Ibid.
5. Whiting, Rick, "GE Capital's Dashboard Drives Metrics To Desktops," InformationWeek, April 22, 2002.
6. Two of the most useful KRIs used in ERM—value-at risk and economic capital—can incorporate all four risk drivers.

Index