ENTERPRISE RISK MANAGEMENT

John Fraser
Betty J. Simkins

The Robert W. Kolb Series in Finance

John Wiley & Sons, Inc.

PART I

Overview

CLARK, ANNETTE 1845BU

CHAPTER 1

Enterprise Risk Management

An Introduction and Overview

JOHN R.S. FRASER
Vice President, Internal Audit & Chief Risk Officer, Hydro One Networks Inc.

BETTY J. SIMKINS
Williams Companies Professor of Business and Professor of Finance, Oklahoma State University

It's not the strongest of the species that survive, nor the most intelligent, but those that are the most responsive to change.

—Charles Darwin

WHAT IS ENTERPRISE RISK MANAGEMENT?

Enterprise risk management (ERM) can be viewed as a natural evolution of the process of risk management. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines enterprise risk management as: "... 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 risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The COSO definition is intentionally broad and deals with risks and opportunities affecting value creation or preservation. Similarly, in this book, we take a broad view of ERM, or what we call—*a holistic approach to ERM*.

Some sources have referred to ERM as a new risk management paradigm. As in the past, many organizations continue to address risk in "silos," with the management of insurance, foreign exchange, operations, credit, and commodities each conducted as narrowly focused and fragmented activities. Under ERM, all risk areas would function as parts of an integrated, strategic, and enterprise-wide system. And while risk management is coordinated with senior-level oversight, employees at all levels of the organization using ERM are encouraged to view risk management as an integral and ongoing part of their jobs.

The purpose of this book is to provide a blend of academic and practical experience on ERM in order to educate practitioners and students alike about this

evolving methodology. Furthermore, our goal is to provide a holistic coverage of ERM, and in this process, provide the "'what," "why," and "how" of ERM to assist firms with the successful implementation of ERM.

The chapters that follow are from some of the leading academics and practitioners of this new methodology, with the in-depth insights into what practitioners of this evolving business practice are actually doing, as well as anticipating what needs to be taught on this topic. The leading experts in this field clearly explain what enterprise risk management is and how you can teach, learn, or implement these leading practices within the context of your business activities.

Enterprise Risk Management introduces you to the wide range of concepts and techniques for managing risk in a holistic way, by correctly identifying risks and prioritizing the appropriate responses. It offers a broad overview of the different types of techniques: the role of the board, risk tolerances, risk profiles, risk workshops, and allocation of resources, while focusing on the principles that determine business success. This comprehensive resource also provides a thorough introduction to enterprise risk management as it relates to credit, market, and operational risks, and covers the evolving requirements of the rating agencies and their importance to the overall risk management in a corporate setting. As well, it offers a wealth of knowledge on the drivers, the techniques, the benefits, and the pitfalls to avoid, in successfully implementing enterprise risk management.

DRIVERS OF ENTERPRISE RISK MANAGEMENT

There are theoretical and practical arguments for the use of ERM. As outlined in Chapter 2 there has been an increasing consciousness in risk literature that a more holistic approach to managing risk makes good business sense.

External drivers for its implementation have been studies such as the Joint Australian/New Zealand Standard for Risk Management,[1] the Committee of Sponsoring Organizations of the Treadway Commission (COSO),[2] the Group of Thirty Report in the United States (following derivatives disasters in the early 1990s),[3] CoCo (the Criteria of Control model developed by the Canadian Institute of Chartered Accountants),[4] the Toronto Stock Exchange Dey Report in Canada following major bankruptcies,[5] and the Cadbury report in the United Kingdom.[6]

Major legal developments such as the New York Stock Exchange Listing Standards and the interpretation of the recent Delaware case law on fiduciary duties, among others, have provided an additional force for ERM.[7] In addition, large pension funds have become more vocal about the need for improved corporate governance, including risk management, and have stated their willingness to pay premiums for stocks of firms with strong independent board governance.[8] ERM has also increased in importance due to the Sarbanes-Oxley Act of 2002—which places greater responsibility on the board of directors to understand and monitor an organization's risks.

Finally, it is important to note that ERM can increase firm value.[9] Security rating agencies such as Moody's and Standard & Poor's include whether a company has an ERM system as a factor in their ratings methodology for insurance, banking, and nonfinancial firms.

SUMMARY OF THE BOOK CHAPTERS

As mentioned earlier, the purpose of this book is to provide a blend of academic and practical experience on ERM in order to educate practitioners and students alike about this evolving methodology. Furthermore, our goal is to provide a holistic coverage of ERM, and in this process, provide the what, why, and how of ERM to assist firms with the successful implementation of ERM. To achieve this goal, the book is organized into the following sections.

Overview
ERM Management, Culture, and Control
ERM Tools and Techniques
Types of Risks
Survey Evidence and Academic Research
Special Topics and Case Studies

A brief description of the author(s) and the chapters is provided below.

Overview

In Chapter 2, "A Brief History of Risk Management," we ask Felix Kloman—retired risk management consultant, conceptual thinker, and lover of sailing—to provide the background and history of risk management and the evolution of enterprise risk management. Felix was ideally suited to do this as someone who has dedicated more than 30 years to sharing stories, raising interesting risk concepts, and generally enjoying the challenges of this entire field. There is no one we know who is better suited or knows more about this topic. He takes us right back literally to some of the earliest recorded thinking on risk management and brings us through the ages to current thinking. Felix goes back to the basic questions of "What is risk management? When and where did we begin applying its precepts? Who were the first to use it?" He provides a highly personal study of this discipline's past and present. It spans the millennia of human history and concludes with a detailed list of contributions in the past century. This is an ideal starting point for anyone new to the topic of risk management or the older scholars who wish to revisit this easy-to-read summary of risk. Felix is adamant in his view that risk must consider opportunities as well as threats.

"ERM and Its Role in Strategic Planning and Strategy Execution" is presented in Chapter 3 by Mark L. Frigo (Director, the Center for Strategy, Execution, and Valuation and Ledger & Quill Alumni Foundation, Distinguished Professor of Strategy and Leadership at the DePaul University Kellstadt Graduate School of Business and School of Accountancy, Chicago) and Mark S. Beasley (Deloitte Professor of Enterprise Risk Management and Professor of Accounting in the College of Management at North Carolina State University, and Director of North Carolina State's Enterprise Risk Management Initiative). The authors have captured the essence of leading ERM and strategic risk management initiatives at their universities as well as their work with hundreds of practice leaders in enterprise risk management. They recognize that one of the major challenges in ensuring that

risk management is adding value is to incorporate ERM in business and strategic planning of organizations. They explain how focusing on strategic risks serves as a filter for management and boards of directors to reduce the breadth of the risk playing field and ensure that they are focused on the right risks. These insights should help respond to the numerous calls following the recent credit crisis for improvements in overall risk oversight, with a particular emphasis on strategic risk management.

In Chapter 4, "The Role of the Board of Directors and Senior Management in Enterprise Risk Management," Bruce Branson (Professor and Associate Director, Enterprise Risk Management Initiative, North Carolina State College of Management) explains that the oversight of the enterprise risk management process employed by an organization is one of the most important and challenging functions of a corporation's board of directors. He notes that a failure to adequately acknowledge and effectively manage risks associated with decisions being made throughout the organization can and often do lead to potentially catastrophic results. Bruce explains the shared responsibility between the members of the board and the senior management team to nurture a risk aware culture in the organization that embraces prudent risk taking within an appetite for risk that aligns with the organization's strategic plan. He identifies the legal and regulatory framework that drives the risk oversight responsibilities of the board. He also clarifies the separate roles of the board and its committees vis-à-vis senior management in the development, approval, and implementation of an enterprise-wide approach to risk management. Finally, the chapter explores optimal board structures to best discharge their risk oversight responsibilities.

ERM Management, Culture, and Control

Anette Mikes (Assistant Professor of Business Administration at Harvard Business School) provides insights into the types of roles that CROs play, based on her personal research in Chapter 5, "Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer." Anette gained her PhD in enterprise risk management from the London School of Economics, and is setting up a program at Harvard Business School with Robert Kaplan to teach ERM. Anette describes the role of chief risk officers (CRO) and different types of ERM methodologies that she sees in practice. She draws on the existing practitioner and academic literature on the role of chief risk officers, and a number of case studies from her ongoing research program on the evolution of the role of the CRO. Anette describes the origins and rise of the CRO, and outlines four major roles that senior risk officers may fulfill: (1) the compliance champion; (2) the modeling expert; (3) the strategic advisor; and (4) the strategic controller. She demonstrates how chief risk officers could improve business decision making and incorporate both good risk analytics and expert judgment, as well as influence risk-taking behavior in the business lines. As she explains: "The art of successful risk management is in getting the executive team to see the light and value the lamp-bearer." This chapter will be of great interest to all CROs and those organizations thinking about how to implement ERM.

"Creating a Risk-Aware Culture" is discussed in Chapter 6 by Doug Brooks (President and CEO, Aegon Canada Inc.). The author draws on his actuarial training and business insights to provide the methods to create a positive culture for risk

management in any organization. The actuarial profession has for several years recognized and been a leading advocate for the research and expansion of ERM into their organizations. Actuaries are by training and experience well versed in managing risks and have expanded into additional areas such as investments and know how best to apply ERM concepts. We wanted to ensure the actuarial profession was included in this book and were delighted when we approached Doug Brooks that he suggested writing about the role of culture in risk management. Doug has been one of the early pioneers in ERM and this has likely added to his continued professional success, as he was recently appointed President and CEO of Aegon Canada Inc. Doug observes that an organization could possess world-class technical capabilities and strong processes for collecting and reporting information, but still have a bankrupt culture so that no value was added through ERM efforts. He considers that there is nothing more crucial to the success of ERM efforts in an organization than an informed and supportive culture. He points out that culture is not merely an intangible concept, but that its elements can be defined and progress in moving toward a desired culture can be measured. He notes that to be successful in risk management, organizations must recognize the importance of encouraging and rewarding disciplined behaviors, as well as openness in communication. Culture is key to ERM and this chapter is helpful to all practitioners who are implementing ERM.

Chapter 7, "ERM Frameworks," is authored by one of the leading authorities on risk frameworks, Professor Emeritus John Shortreed of the University of Waterloo, Canada. Professor Shortreed provides a forward-looking view at the forthcoming international framework for risk management. He is the Canadian representative on the committee that has developed the new ISO 31000 Risk Management Standard (due to be published around the same time as this book). This chapter is a great "companion" for those using the new ISO 31000 standard. Historically, ERM has been molded by the Australian/New Zealand Risk Standard 4360, by COSO's 2004 publication, and recent pronouncements of rating agencies such as Standard & Poor's; however, this new ISO standard is expected to have greater international acceptance in years to come. This chapter describes the new ISO risk management framework, which incorporates best practice from COSO, PMI (Project Management Institute), the Australian and New Zealand Standard (AS/NZS 4360:2004) and other leading international risk management standards. John notes that an ERM framework can often be implemented in a step-by-step way and this approach will assist in building acceptance of ERM and in encouraging a risk culture, particularly if potentially successful areas are selected for the first steps. As the risk management culture matures in the organization there should be noticeable improvements in the ability to discuss risks easily, decision making under uncertainty, comfort levels with risk situations, and achievement of objectives.

Susan Hwang (Associate Partner, Deloitte, Toronto, Canada) provides some original views on the role of Key Risk Indicators (KRIs) in Chapter 8 "Identifying and Communicating Key Risk Indicators." Since 2000 when Hydro One first began practicing ERM, there have not been a lot of new concepts introduced, despite the numerous publications on the topic. A year or two ago, John Fraser was at a presentation made by Susan Hwang on the topic of KRIs and realized that she was describing a concept that we had not seen before. She demonstrated how to

use metrics, or what were often packaged among Key Performance Indicators, as a means of identifying evolving risks that might arise or increase in the future. This is a seemingly simple concept but one that we thought to be important to identifying future key risks. We found that virtually nothing had been written on the topic before, so we asked Susan to write this chapter and share her findings and views. Susan notes that the formal use of KRIs as an ERM tool is an emerging practice. Although many organizations have developed key performance indicators as a measure of progress against the achievement of business goals and strategies, this differs from using KRIs to support risk management and strategic and operational performance. In this chapter, Susan clarifies what KRIs are and demonstrates their practical applications and value to an organization. She outlines the guiding principles for designing KRIs, and discusses implementation and sustainability. The key message she shares is that there are lots of metrics and performance measures in any organization, but the art of ERM is identifying the key ones that will help identify future risks.

ERM Tools and Techniques

"How to Create and Use Corporate Risk Tolerance" is presented in Chapter 9 by Ken Mylrea (Director, Corporate Risk, Canada Deposit Insurance Corporation) and Joshua Lattimore (Policy and Research Advisor, Canada Deposit Insurance Corporation). The authors explore and provide practical examples of the role of risk tolerances. John first learned of Canada Deposit Insurance Corporation (CDIC) in the early 1990s when CDIC issued expectations about the business and financial practices of its member institutions. These principle-based standards were developed by Ken Mylrea and focus on enterprise-wide governance and management. Their underlying premise was that well-managed institutions are less likely to encounter difficulties that could result in CDIC having to pay the claims of depositors. A key feature of the standards was the requirement that institutions' management and board of directors perform a self-assessment against the CDIC control criteria and report the results to the CDIC. In setting the context for this chapter, Ken and Joshua pose the following questions: What is risk tolerance? Why is setting risk tolerance important? What are the factors to consider in setting risk tolerance? And how can you make risk tolerance useful in managing risk? They describe risk tolerance as the risk exposure an organization determines appropriate to take or avoid taking, that is, risk tolerance is about taking calculated risks—namely, taking risks within clearly defined and communicated parameters set by the organization.

In Chapter 10, "How to Plan and Run a Risk Management Workshop," Rob Quail (Outsourcing Program Manager at Hydro One Networks Inc.) provides hard-hitting practical advice on how to actually design and run a risk workshop. Rob was a major reason for the success of ERM at Hydro One and its sustainability to date. He has run more than 200 risk workshops at all levels, including facilitating meetings of up to 800 staff! When we were designing this book we realized that there was nothing we could find documented elsewhere on how to design and run a risk workshop. Rob describes in an easy step-by-step fashion how to design workshops based on the objectives to be achieved, for example, how important is team building versus specific action planning? Rob explains that risk workshops play a vital role in ERM by helping engage executive managers and staff in understanding

the corporate objectives and the risks to achieving these within given tolerances. He goes on to show how workshops not only help identify and address critical risks, but also provide opportunities for participants to learn about organizational objectives, risks, and mitigants. He makes it clear that one size does not fit all and each workshop has to be designed carefully depending on the circumstances and desired outcomes.

In Chapter 11, "How to Prepare a Risk Profile," John Fraser (Vice President, Internal Audit & Chief Risk Officer at Hydro One) provides practical advice on how to prepare a risk profile for executive management and the board of directors. We wanted to have a chapter on risk profiles, and while there is a lot written about risk maps, heat maps, and risk identification, we could not find anything specific about how to actually conduct structured interviews and prepare a risk profile. As a result, we decided to document the Hydro One model, which we have been using since 1999, and which has been proven to be simple and effective. This methodology is based primarily on interviews with executives and risk specialists and complements the results captured by risk workshops. Ideally the results of workshops and interviews (or surveys) should be consolidated and reconciled. It is our hope that these step-by-step instructions will give confidence to risk managers implementing ERM on how best to conduct these interviews effectively. As Sir Graham Day, who was an early champion of ERM at Hydro One, told John "ERM obviously works in practice but can you make it work in theory?"

Chapter 12, "How to Allocate Resources Based on Risk," by Joe Toneguzzo (Director—Implementation & Approvals, Power System Planning, Ontario Power Authority) outlines a business framework for prioritizing resources based on risks, as part of the business planning process. Soon after we began implementing ERM at Hydro One, Joe Toneguzzo—who was responsible for obtaining funding and allocating resources for asset management—worked with the Hydro One Corporate Risk Management Group to determine how best to do so utilizing a risk-based approach. (Joe is now with another organization.) A methodology and supporting business process was developed that has served Hydro One well and is regarded as a leading asset management resource allocation model, as validated in international forums on this subject area. The concept involves identifying the critical business risks and the expenditures proposals available to mitigate them. This is followed by rating all the expenditure proposals in a consistent manner based on the risks that will be mitigated per unit of cost. The expenditures proposals are then dispatched on a priority basis, based on cost/benefit scores (where the benefit is measured in terms of reduced risk) until the resources are exhausted. The advantages of the methodology developed are that it is transparent, consistent, and easy to justify to stakeholders such as regulators, boards of directors, and others. Joe takes us through the theory and practice in an easy-to-follow manner.

John Hargreaves (Managing Director, Hargreaves Risk & Strategy, London, England) explores and provides guidance on the popular topic of quantifying risks in Chapter 13, "Quantitative Risk Assessment in ERM." John Hargreaves has seen his ideas and expertise implemented in various major organizations in England and brings an easy-to-understand introduction to what can become complex theories. John enjoyed a successful career in the real world of finance with major organizations, including being responsible for introducing risk management systems in a major bank following the last U.K. depression. Over the last 10 years, he

has helped implement risk management systems in about 60 organizations. This chapter explains the complex world of quantification of risks in progressive steps to help those who are new to ERM. John provides descriptions of four differing approaches to the quantification of individual risks. Statistical methods for calculating and reporting a company's total corporate risk are described and illustrated by a simple example and he also shows how quantified risks may be incorporated in the business planning process. Note that specialized methods to quantify risks in financial institutions are not covered here. His chapter is a must-read for anyone interested in the theory of practical and workable methods for quantifying risks.

Types of Risks

In Chapter 14, "Market Risk Management and Common Elements with Credit Risk Management," Rick Nason (Partner, RSD Solutions, and Associate Professor of Finance, Dalhousie University, Nova Scotia) explains very sophisticated trading and market risk concepts and risk management methods in an easy-to-understand format. Rick left the exciting world of derivatives trading at a major Canadian bank to join the even more exciting world of academia where he is sharing his experiences through his teaching and consulting activities. Although comfortable with the complex models and math for market risk and derivatives, Rick decided to write this chapter for the general practitioner who wants to learn about market risk management and how it relates to credit risk management. In this chapter, Rick describes how to consider these risks and a framework that provides a focus on market risk. Rick points out that market risk management requires not only an understanding of the tools and techniques, but also of the underlying business in order to successfully implement the market risk function within the enterprise risk management framework of the organization.

Continuing his discussion from the previous chapter, Rick Nason provides the basic elements of credit risk management as well as the more sophisticated concepts every credit risk manager should understand in Chapter 15, "Credit Risk Management." Each year, Rick runs a credit competition at the university, as well as consulting with major banks on ERM and credit risk management. Rick explains that when conducting credit analysis, it is important to remember that, unlike market risk, credit risk is almost always a downside risk; that is, unexpected credit events are almost always negative events and only rarely positive surprises. He also reminds the reader that no one extends credit to a customer, or executes a loan to a counterparty, expecting that it will not be repaid. Rick has crafted this chapter for the general practitioner who wants to learn about credit risk management and for the more experienced credit managers seeking to validate their approach.

Diana Del Bel Belluz (President, Risk Wise Inc.) explains operational risk concepts and methods in an easy-to-read format that will be essential to any student of ERM and helpful to more experienced readers in Chapter 16, "Operational Risk Management." Diana has taught risk management since 1992 and has a background in decision science. With her broad experience from her consulting practice, she understands the challenges of a wide variety of organizations in getting a handle on this multifaceted topic. In this chapter, Diana explains the fundamentals of risk management in an operational setting and how operational risk management can be used to capture the full performance potential of an organization. She explores

what is meant by operational risk and why it is important. She frames her explanations around questions such as: How do you align operational risk management with enterprise risk management? How do you assess operational risks? Why do you need to define risk tolerance for aligned decision making? What can you do to manage operational risk? How do you encourage a culture of risk management at the operational level? This chapter provides a well-rounded introduction to a topic that is becoming of increasing interest.

In Chapter 17, "Risk Management: Techniques in Search of a Strategy," Joseph V. Rizzi (Senior Investment Strategist, CapGen Financial Group, New York) explores the reasons for the losses that triggered massive shareholder value destruction resulting in dilutive recapitalizations, replacement of whole management teams, the failure of numerous institutions, and the adoption of the $700 billion TARP rescue program, and what can be done to avoid this in future. He suggests that risk management needs to move away from a technical, specialist control function with limited linkage to shareholder value creation. This can be achieved by firms and risk decisions moving from an internal egocentric focus to an external systems approach incorporating the firm within a market context. Further, he states that we need to move beyond risk measurement to risk management that integrates risk into strategic planning, capital management, and governance. Joseph draws on Warren Buffett's principles and numerous practical examples (including Long Term Capital Management) to explain, using charts and models, how governance and ERM can address many of the pitfalls we have seen.

Daniel A. Rogers (Associate Professor of Finance, School of Business Administration, Portland State University) provides in Chapter 18, "Managing Financial Risk and Its Interaction with Enterprise Risk Management," a useful background on financial risk management, namely corporate strategies of employing financial transactions to eliminate or reduce measurable risks. He includes possible definitions and examples of industry applications of financial hedging. He then moves on to a basic review of the theoretical rationales for managing (financial) risk and explores the potential for the interaction of financial hedging with other areas of risk management (such as operational, strategic). He also discusses the lessons that can be applied to ERM from the knowledge base about financial hedging. He points out that active board involvement and buy-in are critical to the implementation of a successful ERM program, and that boards that better understand financial risks are likely to be more receptive to conversations about other significant risks that could negatively affect company performance.

Benton E. Gup (Robert Hunt Cochrane/Alabama Bankers Association Chair of Banking at the University of Alabama) traces the evolution of bank capital requirements in Chapter 19, "Bank Capital Regulation and Enterprise Risk Management," from the 1800s to the complex models used in Basel I and II. He points out that the recent subprime crisis makes it clear that our largest banks and financial institutions do not have adequate risk management as evidenced by problems with major banks and that the models employing economic capital can be subject to large errors. He goes on to introduce enterprise risk management and economic capital, which he believes represent the future of bank capital. He notes that enterprise risk management uses a "building block" approach to aggregate the risks from all lines of business, and that economic capital must be "forward looking," and based on expected scenarios instead of recent history.

In "Legal Risk Post-SOX and the Subprime Fiasco: Back to the Drawing Board" (Chapter 20), Steven Ramirez (Director, Business & Corporate Governance Law Center, Loyola University, Chicago) notes that legal risk should be managed in accordance with basic notions of risk management generally. He points out that it should not exist within a risk silo, but should be managed with a view toward the firm's overall risk tolerance and through coordinated efforts of senior management, as well as the board. Professor Ramirez explains in a "no holds barred" way how the rules of professional responsibility governing lawyers were flawed, corporate law was stunted, whistle-blowing was not encouraged, codes of conduct were wholly optional, and there was insufficient regulation of the audit function. This chapter reviews the most developed framework governing legal and reputational risk (SOX) and suggests innovative and proactive ways that controls could be improved and risk can be reduced in the future.

"Financial Reporting and Disclosure Risk Management" is discussed extensively by Susan Hume, Assistant Professor of Finance and International Business, School of Business, the College of New Jersey) in Chapter 21. The author boils down the key requirements of the extensive regulations for financial reporting and disclosure into an easy-to-understand chapter. Key topics such as reporting on internal controls under Sarbanes-Oxley, accounting for derivatives, and fair value accounting are discussed and explained. Susan explains how ERM reporting and disclosure provides the forum to discuss the key vulnerabilities and risks of the firm and strengthens management accountability. It is for the board and senior management to set the risk policy, establish the key levels of acceptable risk exposure, and communicate these policies to managers and other employees. Implementation and reporting then flows up from the bottom to senior management and to the risk management committee, which may be a subcommittee of the board in the ideal structure. This chapter will be an ideal place to gain an introduction to these complex requirements as well as add helpful insights for the more experienced reader.

Survey Evidence and Academic Research

John Fraser and Betty Simkins (co-editors of this book) teamed with Karen Schoening-Thiessen (Senior Manager of Executive Networks in the Governance and Corporate Responsibility Group at the Conference Board of Canada) to develop and analyze the first survey evidence of risk executives working in the area of ERM about the literature they find most effective in assisting and facilitating the successful implementation of ERM. The study in Chapter 22, "Who Reads What Most Often?" highlights crucial areas of need on ERM, and it is hoped that these will be a starting point to encourage and stimulate more advances in the research and practice of ERM. It highlights excellent opportunities for academics to closely collaborate with practitioners to conduct research in these key areas of need. The chapter also discusses problems and challenges risk executives have encountered that were not addressed in the literature. Detailed listings are provided of the top readings of articles (i.e., surveys, academic studies, and practitioner articles), books, and research reports. This chapter was originally published in the Spring/Summer 2008 issue of the *Journal of Applied Finance.*

Chapter 23, "Academic Research on Enterprise Risk Management," by Subbu Iyer (PhD student, Oklahoma State University), Daniel A. Rogers (Associate Professor, Portland State University), and Betty Simkins (Williams Companies Professor of Finance, Oklahoma State University), provides a summary to date of research on enterprise risk management. To conduct the review, they searched academic journals and other databases of academic research and limited their focus to papers that can be classified as either academic research or case studies that would be appropriate for a classroom setting. After a thorough search of ERM literature, the authors located 10 research studies and 5 case studies to synthesize. Overall, the authors find little in the way of consistent results about ERM. In addition, they find that more case studies on enterprise risk management are needed so that risk executives can learn from the experiences of others who have successfully implemented it.

In Chapter 24 "Enterprise Risk Management: Lessons from the Field," we have the benefit of the knowledge from a trio of experienced ERM experts, namely: William G. Shenkir (William Stamps Farish Professor Emeritus, University of Virginia's McIntire School of Commerce), Thomas L. Barton (Kathryn and Richard Kip Professor of Accounting, University of North Florida) and Paul L. Walker (Associate Professor of Accounting, University of Virginia). The authors of this chapter have been involved in the area of ERM since 1996. They have taught ERM at the undergraduate and graduate levels and for businesses and executives worldwide as well as consulting on ERM implementation. They point out that one of the early lessons that companies glean from ERM is that many layers of the company, including senior management, operating managers, and regular employees do not know or understand the strategies and objectives of the organization and how these, in turn, relate to their daily job and tasks. ERM compels companies to identify and focus on the organization's strategies and objectives. This chapter is illustrated with numerous real-life examples and provides a wonderful lesson in what enterprise risk management is like in real life.

Special Topics and Case Studies

In Chapter 25, "Rating Agencies Impact on Enterprise Risk Management," Mike Moody (Managing Director, Strategic Risk Financing Inc.) provides the history and current published thinking of the major rating agencies. This is an area that we expect will expand and become more established as time goes on. Mike has an MBA in finance, is the Managing Director of a risk consulting firm, and was a risk manager of a Fortune 500 company. He has a broad view of the risk universe and what is happening due to the activities of the rating agencies. The interest taken by the agencies, especially Standard & Poor's (S&P) in recent years, has focused boards and senior management on the need for and the advantages of ERM. Mike notes that one of the primary reasons for the movement of rating agencies into ERM is that they believe companies with an enterprise-wide view of risks, such as that offered by ERM, are better managed. Several have also noted that ERM provides an objective view of hard-to-measure aspects such as management capabilities, strategic rigor, and ability to manage in changing circumstances. He explains that the view of S&P is that positive or negative changes in ERM

programs are considered as leading indicators that show up long before they could be seen in a company's published financial data. This chapter provides a sound base for understanding the background and role of rating agencies in ERM, a story that is likely still evolving.

"Enterprise Risk Management: Current Initiatives and Issues" (Chapter 26), contains a roundtable discussion sponsored and published by the *Journal of Applied Finance,* which includes an expert group of academics and practitioners in the area of risk management. The discussants consisted of Bruce Branson (Associate Director of the Enterprise Risk Management Initiative and Professor in the Department of Accounting at North Carolina State University), Pat Concessi (Partner in Global Energy Markets with Deloitte and Touche, Toronto, Canada), John R.S. Fraser (Chief Risk Officer and Vice President of Internal Audit at Hydro One Inc. in Toronto), Michael Hofmann (Vice President and Chief Risk Officer at Koch Industries, Inc. in Wichita, Kansas), Robert (Bob) Kolb (Frank W. Considine Chair in Applied Ethics at Loyola University Chicago), Todd Perkins (Director of Enterprise Risk at Southern Company, Inc. in Atlanta, Georgia), Joe Rizzi (Senior Investment Strategist at CapGen Financial in New York, but at the time of the roundtable discussion, he was the Managing Director of Enterprise Risk Management at Bank of America and La Salle Bank in Chicago, Illinois), and the moderator Betty J. Simkins (Williams Companies Professor of Business and Associate Professor of Finance in the Spears School of Business at Oklahoma State University). This roundtable explored many avenues, concerns, and possible solutions in this evolving arena of risk management.

Demir Yener, Senior Advisor at Deloitte Consulting, Emerging Markets (Washington D.C.), discusses enterprise risk management applications suitable for, and as they exist in, a number of emerging market corporations in Chapter 27, "Establishing ERM Systems in Emerging Countries." He notes that there is a growing interest in improving corporate governance practices in emerging markets. Following the financial crises in the Far East and Russia, which impacted many other emerging markets in 1997–1998, there was a realization that corporate governance practices had to be improved along with the financial sector infrastructure. The Financial Stability Forum was convened, as a result of which the OECD (Organisation for Economic Co-operation and Development) Principles of Corporate Governance were developed in 1999. Since then the principles have been revised in 2004, and other standards of business conduct had been introduced to provide guidance in a number of critical areas of global cooperation for business and finance among nations. The emerging countries in Demir's sample include Egypt, Jordan, Mongolia, Serbia, Turkey, and Ukraine. The ERM concept is still a new concept in these countries and it is likely to take a while to get the emerging country firms, given the legal and regulatory requirements, to reach the desirable level of risk management practices.

In Chapter 28, "The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One," Tom Aabo (Associate Professor, Aarhus School of Business, Denmark), John R.S. Fraser (Chief Risk Officer, Hydro One Inc.), and Betty J. Simkins (Williams Companies Professor of Business, Oklahoma State University) describe the successful implementation of enterprise risk management (ERM) at Hydro One Inc. over a five-year period. This chapter was first published in the *Journal of Applied Corporate Finance.* Hydro One is a Canadian electric utility

company that has experienced significant changes in its industry and business. Hydro One has been at the forefront of ERM for many years, especially in utilizing a holistic approach to managing risks, and provides a best practices case study for other firms to follow. This chapter describes the process of implementation beginning with the creation of the chief risk officer position, the deployment of a pilot workshop, and the various tools and techniques critical to ERM (e.g., the Delphi Method, risk trends, risk maps, risk tolerances, risk profiles, and risk rankings).

As this brief overview indicates, the chapters in this book present an impressive coverage of crucial issues on enterprise risk management and are written by leading ERM experts globally. We believe that no other book on the market provides such a wide coverage of timely topics—such as ERM management, culture and control, ERM tools and techniques, types of risk from a holistic viewpoint, leading case studies, practitioner survey evidence, and academic research on ERM. The authors of these chapters and we, the editors, invite reader comments and suggestions.

FUTURE OF ERM AND UNRESOLVED ISSUES

As is generally recognized, ERM is still evolving with new techniques and research of best practices being studied and documented on almost a daily basis. Some of the issues that we feel deserve the attention of our readers and those interested in the future of ERM include:

- Why have some companies succeeded and others failed in the implementation of ERM?
- What do we predict for the future of ERM?
- What research issues remain?
- A comment on universities' ERM programs and education.
- What unresolved issues do we see?

The above issues all merit study and more attention than they have received to date. An entire chapter, if not book, could be written on the reasons for failure in the implementation of ERM. Often it appears to be caused in part by confusion over exactly what ERM is and undue expectations of management. Our observation is that too often the skills and techniques are not available and without support from the most senior ranks, ERM is destined to fail.

We expect ERM to continue to grow until, in looking back, future managers will ask "How could you have managed without these basic techniques?" Obviously there has to be more discussion and clarification on what ERM is and what it has to offer. While regulatory interest can force ERM into companies, if not done well, it can become another box-ticking exercise that adds little value.

As highlighted in Chapter 23, the opportunities to study ERM and assist in moving this new methodology forward are limitless and likely to continue. While some analysis can be done based on public information, it will require proactive visionary academics to go into the real world and study what is evolving in real business practices. This is a veritable goldmine for some intrepid academics and a minefield for the more timid.

NOTES

1. The Joint Australian/New Zealand Standard for Risk Management (AS/NSZ 4360: 2004), first edition published in 1995, is the first guide on enterprise risk management that provides practical information. This publication covers the establishment and implementation of the enterprise risk management process.
2. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (September 1992 and September 2004).
3. Group of Thirty, Derivatives: Practices and Principles (Washington, DC: 1993).
4. CoCo (Criteria of Control Board of the Canadian Institute of Chartered Accountants).
5. "Where Were the Directors"—Guidelines for Improved Corporate Governance in Canada, report of the Toronto Stock Exchange Committee on Corporate Governance in Canada (December 1994).
6. Committee on the Financial Aspects of Corporate Governance (Cadbury Committee, final report and Code of Best Practices issued December 1, 2002).
7. NYSE Corporate Governance Rules 7C(iii)(D) www.nyse.com/pdfs/finalcorpgovrules.pdf and Emerging Governance Practices in Enterprise Risk Management, the Conference Board (2007).
8. McKinsey & Company and Institutional Investor, 1996. "Corporate Boards: New Strategies for Adding Value at the Top."
9. Risk management in general has been shown to increase firm value. See Smithson, Charles W., and Betty J. Simkins, "Does Risk Management Add Value? A Survey of the Evidence," *Journal of Applied Corporate Finance* vol. 17, no. 3 (2005): 8–17.

ABOUT THE EDITORS

John Fraser is the Vice President, Internal Audit & Chief Risk Officer of Hydro One Networks Inc., one of North America's largest electricity transmission and distribution companies. He is an Ontario and Canadian Chartered Accountant, a Fellow of the Association of Chartered Certified Accountants (U.K.), a Certified Internal Auditor, and a Certified Information Systems Auditor. He has more than 30 years experience in the risk and control field mostly in the financial services sector, including areas such as finance, fraud, derivatives, safety, environmental, computers, and operations. He is currently Chair of the Advisory Committee of the Conference Board of Canada's Strategic Risk Council, a Practitioner Associate Editor of the *Journal of Applied Finance*, and a past member of the Risk Management and Governance Board of the Canadian Institute of Chartered Accountants. He is a recognized authority on enterprise risk management and has co-authored three academic papers on ERM—published in the *Journal of Applied Corporate Finance* and the *Journal of Applied Finance*.

Betty J. Simkins is Williams Companies Professor of Business and Professor of Finance at Oklahoma State University (OSU). She received her BS in Chemical Engineering from the University of Arkansas, her MBA from OSU, and her PhD from Case Western Reserve University. Betty is also active in the finance profession and currently serves as Vice-Chairman of the Trustees (previously President) of the Eastern Finance Association, on the board of directors for the Financial Management Association (FMA), as co-editor of the *Journal of Applied Finance,*

and as Executive Editor of *FMA Online* (the online journal for the FMA). She has coauthored more than 30 journal articles in publications including the *Journal of Finance*, *Financial Management*, *Financial Review, Journal of International Business Studies, Journal of Futures Markets, Journal of Applied Corporate Finance,* and the *Journal of Financial Research* and has won a number of best paper awards at academic conferences.

CLARK, ANNETTE 1845BU

CHAPTER 2

A Brief History of Risk Management

H. FELIX KLOMAN
President, Seawrack Press Inc.

INTRODUCTION

What *is* risk management (and its alternative title "enterprise risk management")? When and where did we begin applying its precepts? Who were the first to use it? This is a brief and highly personal study of this discipline's past and present. It is a description of some of its emotional and intellectual roots. It spans the millennia of human history and concludes with a detailed list of contributions in the past century.

RISK MANAGEMENT IN ANTIQUITY

Making good decisions in the face of uncertainty and risk probably began during the earliest human existence. Evolution favored those human creatures able to use their experience and minds to reduce the uncertainty of food, warmth, and protection. *Homo sapiens* survived by developing "an expression of an instinctive and constant drive for defense of an organism against the risks that are part of the uncertainty of existence."[1] This "genetic expression" can be construed as the beginning of risk management, a discipline for dealing with uncertainty.

As the millennia passed, our species developed other mechanisms for coping with each day's constant surprises. We invented a pantheon of divine creatures to blame for misfortune, praise for good luck, and to whom we offered sacrifices to mitigate the worst. These gods and goddesses, the personification of heavenly bodies, high mountains, and the deepest seas, led to a dependence on human oracles, soothsayers, priests, priestesses, and astrologers, to predict the future. We created a written language (Mesopotamia, Sumeria, Egypt, Phoenicia) in order to pass knowledge to the future. As our species used language, experience, memory, and deduction to explain random uncertainty, we created an alternative and backup explanatory system.

The classical world of the Greeks and Romans demonstrates the development of written language, providing a significant advantage over oral recitation. At first, Greek memories passed on information from the past. Their written language

extrapolated it into more rational predictions. Homer, capturing memory, sang of Zeus, Hera, Athena, Apollo, and the corps of divinities responsible for the victory at Troy as well as the misadventures of Odysseus on his return home. But by 585 BC, the Greek philosopher Thales used his observations, written data, and deductions to predict an eclipse of the sun, even though he continued to profess a belief in these gods.[2] A century later Herodotus used intelligent "enquiry" to write "history," but he too persisted with the power of divinities. It was finally Thucydides, in the early 400s BC, who proposed a "new penetrating realism," one that "removed the gods as explanations of the course of events." Thucydides was "fascinated by the gap between expectation and outcome, intention and event."[3] Perhaps he should be called the father of risk management.

A few philosophers in classical Greece tried to emphasize observation, deduction, and prediction, but they inevitably collided with the inertia of belief in the long-standing system of divine intervention as the explanation for misfortune as well as good luck. With the growth and dominance of the new monotheistic religions in the Middle East and Mediterranean, it would take another millennium before the ideas Thucydides first advanced grew into the solid body of scientific knowledge to replace myth and superstition.

AFTER THE MIDDLE AGES

Jump ahead another 1,000 years to the emergence of the Renaissance and Enlightenment. Two changes encouraged the idea that we could actually think intelligently about the future. Peter Bernstein described the first, in his *Against the Gods*: "The idea of risk management emerges only when people believe they are to some degree free agents."[4] The second was our growing fascination with numbers. Our increasing disenchantment with the explanation that a "superior power" ordained everything became coupled with the capability of manipulating experience and data into numbers and thence probabilities. We could predict alternative futures! Peter Bernstein's book is a joyful and often lyrical exploration of development of the concept of risk as both threat and opportunity. We became capable of "scrutinizing the past" to suggest future possibilities. He describes those men who first advanced the ideas of probability measurement, introducing us to familiar and unfamiliar names from the Renaissance onward:

Leonardo Pisano (who introduced Arabic numerals)
Luca Paccioli (double-entry bookkeeping)
Girolamo Cardano (measuring the probability of dice)
Blaise Pascal ("fear of harm ought to be proportional not merely to the gravity of the harm, but also to the probability of the event")
John Graunt (who calculated statistical tables)
Daniel Bernoulli (the concept of utility)
Jacob Bernoulli (the "law of large numbers")
Abraham de Moivre (the "bell" curve and standard deviation)
Thomas Bayes (statistical inference)
Francis Galton (regression to the mean)
Jeremy Bentham (the law of supply and demand)

Today's risk management rests, for better or for worse, on these and other fascinating characters.

Where once philosophers and theologians attributed fortune or misfortune to the whims of gods, the efforts of those early thinkers described in Bernstein's book, "have transformed the perception of risk from chance of loss into opportunity for gain, from FATE and ORIGINAL DESIGN to sophisticated, probability-based forecasts of the future, and from helplessness to choice."[5]

Bernstein contrasts the development of more rigorous quantitative approaches to probabilities with recent attempts to understand why "people yield to inconsistencies, myopia, and other forms of distortion throughout the process of decision-making." His story of risk and risk management is one of rationality and human nature, fighting with each other and then cooperating, to provide a better understanding of uncertainty and how to deal with it. ". . . Any decision relating to risk involves two distinct yet inseparable elements: the objective facts and a subjective view about the desirability of what is to be gained, or lost, by the decision. Both objective measurement and subjective degrees of belief are essential; neither is sufficient by itself."

"The essence of risk management," Bernstein concludes, "lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us."

THE PAST 100 YEARS

Experience and new information allowed us to think intelligently about the future and plan for potential unexpected outcomes. Many millennia contributed to our growing ability to distill and use information, but the developments since 1900 are more apparent and useful. Here is a synopsis of these critical events.

The twentieth century began with euphoria, new wealth, relative peace, and industrialization, only to descend into chaotic regional and worldwide wars. These and other catastrophes crushed illusions about the perfectibility of society and our species, leaving us less idealistic and more appreciative of the continuing uncertainty of our future.

Ideas drove change in this century. Stephen Lagerfeld cogently summed it up:[6] "Apart from the almost accidental tragedy of World War I, the great clashings of our bloody century have not been provoked by the hunger for land, or riches, or other traditional sources of national desire, but by *ideas*—about the value of individual dignity and freedom, about the proper organization of society, and ultimately about the possibility of human perfection."

Risk management is one of those ideas that a logical, consistent, and disciplined approach to the future's uncertainties will allow us to live more prudently and productively, avoiding unnecessary waste of resources. It goes beyond faith and luck, the former twin pillars of managing the future, before we learned to measure probability. As Peter Bernstein wrote, "If everything is a matter of luck, risk management is a meaningless exercise. Invoking luck obscures truth, because it separates an event from its cause."[7]

If risk management is an extension of human nature, I should list the most notable political, economic, military, scientific, and technological events of the past

100 years. The major wars (from the Russo-Japanese, World Wars I and II, Korea, the Balkan, the first Gulf War and Iraq, to the numerous regional conflicts) and the advent of the automobile, radio, television, computer and Internet, the Great Depression, global warming, the atom bomb and nuclear power, the rise and fall of communism, housing, the dot-com, derivative, and lending bubbles, and the entire environmental movement affected the development of risk management. Major catastrophes did so more directly: the Titanic (the "unsinkable" ship sinks), the Triangle Shirtwaist fire (the failure to allow sufficient exits), Minimata Bay (mercury poisoning in Japan), Seveso (chemical poisoning of the community in Italy), Bhopal (chemical poisoning in India), Chernobyl (Russian nuclear meltdown), Three Mile Island (potential U.S. nuclear disaster that was contained), *Challenger* (U.S. space shuttle break up), Piper Alpha (North Sea oil production platform explosion and fire), Exxon Valdez (Alaskan ship grounding and oil contamination), to cite some of the more obvious. Earthquakes, tsunamis, typhoons, cyclones, and hurricanes continue to devastate populous regions, and their increasing frequency and severity stimulate new studies on causes, effects, and prediction, all part of the evolution of risk management.

The most significant milestones, in my opinion, are more personal: the new ideas, books, and actions of *individuals* and their *groups* all of whom stimulated the discipline. Here's my list:

1914 Credit and lending officers in the United States create Robert Morris Associates in Philadelphia. By 2000 it changes its name to the Risk Management Association and continues to focus on credit risk in financial institutions. In 2008 it counted 3,000 institutional and 36,000 associate members.[8]

1915 Friedrich Leitner publishes *Die Unternehmensrisiken* in Berlin (Enzelwirt. Abhan. Heft 3), a dissertation on risk and some of its responses, including insurance.

1921 Frank Knight publishes *Risk, Uncertainty and Profit,* a book that becomes a keystone in the risk management library. Knight separates uncertainty, which is not measurable, from risk, which is. He celebrates the prevalence of "surprise" and he cautions against over-reliance on extrapolating past frequencies into the future.[9]

1921 *A Treatise on Probability,* by John Maynard Keynes, appears. He too scorns dependence on the "Law of Great Numbers," emphasizing the importance of relative perception and judgment when determining probabilities.[10]

1928 John von Neumann presents his first paper on a theory of games and strategy at the University of Göttingen, "Zur Theorie der Gesellschaftsspiele," *Mathematische Annalen,* suggesting that the goal of not losing may be superior to that of winning. Later, in 1944, he and Oskar Morgenstern publish *The Theory of Games and Economic Behavior* (Princeton University Press, Princeton, NJ).

The U.S. Congress passes the Glass-Steagall Act, prohibiting common ownership of banks, investment banks, and insurance companies. This Act, finally revoked in late 1999, arguably acted as a brake on the development of financial institutions in the United States and led the risk management discipline in many ways to be more fragmented than integrated. The financial disasters after 2000 cause some to question the wisdom of revocation.

1945 Congress passes the McCarran-Ferguson Act, delegating the regulation of insurance to the various states, rather than to the federal government, even as business became more national and international. This was another needless brake on risk management, as it hamstrung the ability of the insurance industry to become more responsive to the broader risks of its commercial customers.

1952 The *Journal of Finance* (No. 7–, 77–91) publishes "Portfolio Selection," by Dr. Harry Markowitz, who later wins the Nobel Prize in 1990. It explores aspects of return and variance in an investment portfolio, leading to many of the sophisticated measures of financial risk in use today.[11]

1956 The *Harvard Business Review* publishes "Risk Management: A New Phase of Cost Control," by Russell Gallagher, then the insurance manager of Philco Corporation in Philadelphia. This city is the focal point for new "risk management" thinking, from Dr. Wayne Snider, then of the University of Pennsylvania, who suggested in November 1955 that "the professional insurance manager should be a risk manager," to Dr. Herbert Denenberg, another University of Pennsylvania professor who began exploring the idea of risk management using some early writings of Henri Fayol.

1962 In Toronto, Douglas Barlow, the insurance risk manager at Massey Ferguson, develops the idea of "cost-of-risk," comparing the sum of self-funded losses, insurance premiums, loss control costs, and administrative costs to revenues, assets, and equity. This moves insurance risk management thinking away from insurance, but it still fails to cover all forms of financial and political risk.

That same year Rachel Carson's *The Silent Spring* challenges the public to consider seriously the degradation to our air, water, and ground from both inadvertent and deliberate pollution. Her work leads directly to the creation of the Environmental Protection Agency in the United States in 1970, the plethora of today's environmental regulations, and the global Green movement so active today.[12]

1965 The Corvair unmasked! Ralph Nader's *Unsafe at Any Speed* appears and gives birth to the consumer movement, first in the United States and later moving throughout the world, in which *caveat vendor* replaces the old precept of *caveat emptor.* The ensuing wave of litigation and regulation leads to stiffer product, occupational safety, and security regulations in most developed nations. Public outrage at corporate misbehavior also leads to the rise of litigation and the application of punitive damages in U.S. courts.[13]

1966 The Insurance Institute of America develops a set of three examinations that lead to the designation "Associate in Risk Management" (ARM), the first such certification. While heavily oriented toward corporate insurance management, its texts feature a broader risk management concept and are revised continuously, keeping the ARM curriculum up-to-date.[14]

1972 Dr. Kenneth Arrow wins the Nobel Memorial Prize in Economic Science, along with Sir John Hicks. Arrow imagines a perfect world in which every uncertainty is "insurable," a world in which the Law of Large Numbers works without fail. He then points out that our knowledge is always incomplete—it "comes trailing clouds of vagueness"—and that we are

best prepared for risk by accepting its potential as both a stimulant and penalty.

1973 In 1971, a group of insurance company executives meet in Paris to create the International Association for the Study of Insurance Economics. Two years later, the Geneva Association, its more familiar name, holds its first Constitutive Assembly and begins linking risk management, insurance, and economics. Under its first Secretary General and Director, Orio Giarini, the Geneva Association provides intellectual stimulus for the developing discipline.[15]

That same year, Myron Scholes and Fischer Black publish their paper on option valuation in the *Journal of Political Economy* and we begin to learn about derivatives.[16]

1974 Gustav Hamilton, the risk manager for Sweden's Statsforetag, creates a "risk management circle," graphically describing the interaction of all elements of the process, from assessment and control to financing and communication.

1975 In the United States, the American Society of Insurance Management changes its name to the Risk & Insurance Management Society (RIMS), acknowledging the shift toward risk management first suggested by Gallagher, Snider, and Denenberg in Philadelphia 20 years earlier. By 2008, RIMS has almost 11,000 members and a wide range of educational programs and services aimed primarily at insurance risk managers in North America. It links with sister associations in many other countries around the world through IFRIMA, the International Federation of Risk & Insurance Management Associations.[17]

With the support of RIMS, *Fortune* magazine publishes a special article entitled "The Risk Management Revolution." It suggests the coordination of formerly unconnected risk management functions within an organization and acceptance by the board of responsibility for preparing an organizational policy and oversight of the function. Twenty years lapse before many of the ideas in this paper gain general acceptance.

1979 Daniel Kahneman and Amos Tversky publish their "prospect theory," demonstrating that human nature can be perversely irrational, especially in the face of risk, and that the fear of loss often trumps the hope of gain. Three years later they and Paul Slovic write *Judgment Under Uncertainty: Heuristics and Biases*, published by Cambridge University Press. Kahneman wins the Nobel Prize in Economics in 2002.

1980 Public policy, academic and environmental risk management advocates form the Society for Risk Analysis (SRA) in Washington. *Risk Analysis,* its quarterly journal, appears the same year. By 2008, SRA has more than 2,500 members worldwide and active subgroups in Europe and Japan. Through its efforts, the terms risk assessment and risk management are familiar in North American and European legislatures.[18]

1983 William Ruckelshaus delivers his speech on "Science, Risk and Public Policy" to the National Academy of Sciences, launching the risk management idea in public policy. Ruckelshaus had been the first director of the Environmental Protection Agency, from 1970 to 1973, and returned in 1983 to lead EPA into a more principled framework for environmental policy. Risk management reaches the national political agenda.[19]

1986 The Institute for Risk Management begins in London. Several years later, under the guidance of Dr. Gordon Dickson, it begins an international set of examinations leading to the designation, "Fellow of the Institute of Risk Management," the first continuing education program looking at risk management in all its facets. This program is expanded in 2007–2008 for its 2,500 members.[20]

That same year the U.S. Congress passes a revision to the Risk Retention Act of 1982, substantially broadening its application, in light of an insurance cost and availability crisis. By 1999, some 73 "risk retention groups," effectively captive insurance companies under a federal mandate, account for close to $750 million in premiums.

1987 "Black Monday," October 19, 1987, hits the U.S. stock market. Its shock waves are global, reminding all investors of the market's inherent risk and volatility.

That same year Dr. Vernon Grose, a physicist, student of systems methodology, and former member of the National Transportation Safety Board, publishes *Managing Risk: Systematic Loss Prevention for Executives,* a book that remains one of the clearest primers on risk assessment and management.[21]

1990 The United Nations Secretariat authorizes the start of IDNDR, the International Decade for Natural Disaster Reduction, a 10-year effort to study the nature and the effects of natural disasters, particularly on the less-developed areas of the world, and to build a global mitigation effort. IDNDR concludes in 1999 but continues under a new title, ISDR, the International Strategy for Disaster Reduction. Much of its work is detailed in *Natural Disaster Management,* a 319-page synopsis on the nature of hazards, social and community vulnerability, risk assessment, forecasting, emergency management, prevention, science, communication, politics, financial investment, partnerships, and the challenges for the twenty-first century.[22]

1992 The Cadbury Committee issues its report in the United Kingdom, suggesting that governing boards are responsible for setting risk management policy, assuring that the organization understands all its risks, and accepting oversight for the entire process. Its successor committees (Hempel and Turnbull), and similar work in Canada, the United States, South Africa, Germany, and France, establish a new and broader mandate for organizational risk management.[23]

In 1992, British Petroleum turns conventional insurance risk financing topsy-turvy with its decision, based on an academic study by Neil Doherty of the University of Pennsylvania and Clifford Smith of the University of Rochester, to dispense with any commercial insurance on its operations in excess of $10 million. Other large, diversified, transnational corporations immediately study the BP approach.[24]

The Bank for International Settlements issues its Basel I Accord to help financial institutions measure their credit and market risks and set capital accordingly.

The title "Chief Risk Officer" is first used by James Lam at GE Capital to describe a function to manage "all aspects of risk," including risk management, back-office operations, and business and financial planning.

1994 Bankers Trust, in New York, publishes a paper by its CEO, Charles Sanford, entitled "The Risk Management Revolution," from a lecture at MIT. It identifies the discipline as a keystone for financial institution management.[25]

1995 A multidisciplinary task force of Standards Australia and Standards New Zealand publishes the first Risk Management Standard, AS/NZS 4360:1995 (since revised in 1999 and 2004), bringing together for the first time several of the different subdisciplines. This standard is followed by similar efforts in Canada, Japan, and the United Kingdom. While some observers think the effort premature, because of the constantly evolving nature of risk management, most hail it as an important first step toward a common global frame of reference.[26]

That same year Nick Leeson, a trader for Barings Bank, operating in Singapore, finds himself disastrously overextended and manages to topple the bank. This unfortunate event, a combination of greed, hubris, and inexcusable control failures, receives world headlines and becomes the "poster child" for fresh interest in operational risk management.

1996 The Global Association of Risk Professionals (GARP), representing credit, currency, interest rate, and investment risk managers, starts in New York and London. By 2008, it has more than 74,000 members, plus an extensive global certification examination program.[27]

Risk and risk management make the best-seller lists in North America and Europe with the publication of Peter Bernstein's *Against the Gods: The Remarkable Story of Risk*. Bernstein's book, while first a history of the development of the idea of risk and its management, is also, and perhaps more importantly, a warning about the overreliance on quantification: "The mathematically driven apparatus of modern risk management contains the seeds of a dehumanizing and self-destructive technology."[28] He makes a similar warning about the replacement of "old-world superstitions" with a "dangerous reliance on numbers," in "The New Religion of Risk Management," in the March–April 1996 issue of *The Harvard Business Review.*

1998 The collapse of Long-Term Capital Management, a four-year-old hedge fund, in Greenwich, Connecticut, and its bailout by the Federal Reserve, illustrate the failure of overreliance on supposedly sophisticated financial models.

2000 The widely heralded Y2K bug fails to materialize, in large measure because of billions spent to update software systems. It is considered a success for risk management.

The terrorism of September 11, 2001, and the collapse of Enron remind the world that nothing is too big for collapse. These catastrophes reinvigorate risk management.

PRMIA, the Professional Risk Manager's International Association, starts in the United States and United Kingdom. By 2008, it counts 2,500 paid and 48,000 associate members. It, too, sponsors a global certification examination program.[29]

In July, the U.S. Congress passes the Sarbanes-Oxley Act, in response to the Enron collapse and other financial scandals, to apply to all public

companies. It is an impetus to combine risk management with governance and regulatory compliance. Opinion is mixed on this change. Some see this combination as a step backward, emphasizing only the negative side of risk, while others consider it a stimulus for risk management at the board level.

2004 The Basel Committee on Banking Supervision publishes the Basel II Accords, extending its global capital guidelines into operational risk (Basel I covered credit and market risks). Some observers argue that while worldwide adoption of these guidelines may reduce individual financial institution risk, it may increase systemic risk. These global accords may lead to similar guidelines for nonfinancial organizations.[30]

2005 The International Organization for Standardization creates an international working group to write a new global "guideline" for the definition, application, and practice of risk management, with a target date of 2009 for approval and publication.[31]

2007 Nassim Nicolas Taleb's *The Black Swan* is published by Random House in New York. It is a warning that "our world is dominated by the extreme, the unknown, and the very improbable . . . while we spend our time engaged in small talk, focusing on the known and the repeated."[32] Taleb's 2001 book, *Fooled by Randomness* (Textere, New York) was an earlier paean to the importance of skepticism on models.

2008 The United States Federal Reserve bailout of Bear Stearns appears to many to be an admission of the failure of conventional risk management in financial institutions.

Perhaps Peter Bernstein's *Against the Gods* is a fitting end to this list of risk management milestones. It illustrates the importance of communication. Too often, new ideas have been unnecessarily restricted to the cognoscenti. Arcane mathematics, academic prose, and the secretiveness of current risk management "guilds," each protecting their own turf, discourage needed interdisciplinary discussion. Peter's lucid prose, compelling syntheses of difficult concepts, personal portraits of creative people, and particularly his warnings of the perils of excess quantification, bring us an appreciation of both the potential and perils of risk management. No matter what title we attach to this thinking process (risk management; enterprise risk management; strategic risk management; etc.), it will continue to be a part of the human experience.

None of this retrospection has any meaning or value unless it acts as a stimulant for a more prudent, intelligent, and optimistic use of the ideas and tools of past innovators.

Step out and create some new risk milestones.

Paradoxically, the very mortality that bears each of us along to a finite conclusion also gives us, through its unfolding, the means to repossess what we believe we have lost. It is in memory, given its true shape through the imagination, that we can truly possess our lives, if we will only strive to regain them.

—Louis D. Rubin Jr., *Small Craft Advisory*
Atlantic Monthly Press, New York, 1991

Risk and time are opposite sides of the same coin, for if there were no tomorrow there would be no risk. Time transforms risk, and the nature of risk is shaped by the time horizon: the future is the playing field.

—Peter Bernstein, *Against the Gods,* John Wiley & Sons, New York, 1996 (Revision September 2008. An earlier version of this brief history appeared in the December 1999 issue of *Risk Management Reports.*)

NOTES

1. Douglas Barlow, in letter to the author, January 8, 1998. Barlow was, for many years, the risk manager for Canada's Massey Ferguson Company.
2. Robin Lane Fox, *The Classical World* (New York: Basic Books, 2006) 49.
3. Ibid., 157.
4. Peter L. Bernstein, *Against the Gods* (New York: John Wiley & Sons, 1996) xxxv.
5. Ibid., 337.
6. Stephen Lagerfeld, "Editor's Comment," *Wilson Quarterly* (Autumn 1999).
7. Bernstein, op. cit., 197.
8. See www.rmahq.org for more information about RMA.
9. See 1985 reprint from the University of Chicago Press and first edition, 1921, Hart, Schaffner, and Marx, Boston.
10. See 1963 reprint from Macmillan.
11. See www.afajof.org.
12. See 1952 original and 2003 reprint from Houghton Mifflin, Boston.
13. See Grossman Publishers, New York, 1965.
14. See www.aicpcu.org.
15. See www.genevaassociation.org for more information on the Geneva Association.
16. See www.journals.uchicago.edu.
17. See www.rims.org for more information on RIMS.
18. See www.sra.org for more information about SRA.
19. See *Science*, vol. 221, no. 4615, September 9, 1983, and www.science.mag.org.
20. See www.theirm.org for more information about IRM.
21. Prentice-Hall, Englewood Cliffs, NJ, 1993.
22. See www.unisdr.org for more information on ISDR.
23. See www.archive.official-documents.co.uk.
24. See *Journal of Applied Corporate Finance*, vol. 6, no. 3 (Fall 1993) www.blackwell-synergy.com.
25. See www.terry.uga.edu/sanford/vita.html.
26. See www.standards.com.au.
27. See www.garp.org for more information about GARP.
28. Bernstein, op. cit., 7.
29. See www.prmia.org for more information about PRMIA.
30. See www.bis.org.
31. See www.iso.org.
32. Nassim Nicholas Taleb, *The Black Swan* (New York: Random House, 2007) xxvii.

ABOUT THE AUTHOR

Felix Kloman is President of Seawrack Press, Inc. and a retired principal of Towers Perrin, an international management consulting firm. His experience includes serving as Editor and Publisher of *Risk Management Reports* for 33 years, from 1974 to 2007, and more than 40 years in risk management consulting with Risk Planning Group (Darien, CT), Tillinghast (Stamford, CT), and Towers Perrin (Stamford, CT). He is the author of *Mumpsimus Revisited* (2005), and *The Fantods of Risk* (2008), both sets of essays on risk management. He is a Fellow of the Institute of Risk Management (London), a past director of the Nonprofit Risk Management Center, a past and founding director of the Public Entity Risk Institute, past chairman of the Risk Management & Insurance Committee for the U.S. Sailing Association, and a charter member of the Society for Risk Analysis. He received the Dorothy and Harry Goodell Award from the Risk & Insurance Management Society in 1994.

He is a graduate of Princeton University, 1955, with an AB in History.

CLARK, ANNETTE 1845BU

CHAPTER 3

ERM and Its Role in Strategic Planning and Strategy Execution

MARK S. BEASLEY, PhD, CPA
Deloitte Professor of Enterprise Risk Management and Director of the ERM Initiative, College of Management, North Carolina State University

MARK L. FRIGO, PhD, CPA, CMA
Director, The Center for Strategy, Execution, and Valuation and Ledger & Quill Alumni Foundation Distinguished Professor of Strategy and Leadership at the DePaul University Kellstadt Graduate School of Business and School of Accountancy

Enterprise risk management (ERM) has rightfully become a top priority for directors and executive management. The current economic crisis highlights the disastrous results when risks associated with strategies are ignored or ineffectively managed. Coming out of the crisis are numerous calls for improvements in overall risk oversight, with a particular emphasis on strategic risk management.

One of the major challenges in ensuring that risk management is adding value is to incorporate ERM in business and strategic planning of organizations. The "silos" that separate risk management functions in organizations also create barriers that separate strategic planning from ERM. In many cases, risk management activities are not linked or integrated with strategic planning, and strategic risks can be overlooked, creating dangerous "blind spots" in strategy execution and risk management that can be catastrophic.

The challenge, as well as opportunity, for organizations is to embed risk thinking and risk management explicitly into the strategy development and strategy execution processes of an organization so that strategy and risk mindsets are one in the same. This chapter is based on articles, cases, and research by the authors in leading ERM and Strategic Risk Management initiatives at North Carolina State University and DePaul University, respectively, and their work with hundreds of practice leaders in enterprise risk management.

RISING EXPECTATIONS FOR STRATEGIC RISK MANAGEMENT

The expectations that boards of directors and senior executives are effectively managing risks facing an enterprise are at all-time highs.[1] Much of this shift in expectations was prompted initially by corporate scandals and resulting changes in corporate governance requirements, such as the Sarbanes-Oxley Act of 2002 (SOX) and the NYSE Corporate Governance Rules updated in 2004. Debt-rating agencies such as Standard & Poor's, Moody's, and Fitch now examine enterprise-wide risk management practices of institutions as part of their overall credit-rating assessment processes. Their particular focus is on understanding the risk management culture and the overall strategic risk management processes in place.[1]

The economic crisis that began in 2007 and still continues is now shining a huge spotlight on the board and senior management's enterprise-wide risk management processes. Reform proponents are pointing to failures in the overall risk oversight processes, including unaware boards, overreliance on sophisticated models, and underreliance on sound judgment. Critics argue that because returns on certain strategic initiatives were so great, risks that were present were either unknown or ignored.[2] Numerous calls are now arising for drastic improvements in risk management, with a specific call for more formal risk considerations in managing an organization's deployment of specific strategic initiatives.

This sentiment is evidenced by Federal Reserve Governor Randall S. Kroszner's October 2008 speech where he argued that financial institutions must improve the linkage between overall corporate strategy and risk management given that "survivability will hinge on such an integration." Governor Kroszner noted that many firms have forgotten the critical importance of undertaking an adequate assessment of risks associated with the overall corporate strategies.[3]

This shift toward greater expectations for effective enterprise-wide risk management oversight is complicated by the fact that the volume and complexities of risks affecting an enterprise are increasing as well. Rapid changes in information technologies, the explosion of globalization and outsourcing, the sophistication of business transactions, and increased competition make it that much more difficult for boards and senior executives to effectively oversee the constantly evolving complex portfolio of risks.

Even before the recent financial crisis, board members believed that risks were increasing. Ernst & Young's 2006 report, "Board Members on Risk," found that 72 percent of board members surveyed believed that the overall level of risk that companies face has increased in the past two years, with 41 percent indicating that overall levels of risk have increased significantly.[4] Given recent events, that concern is only heightened. Similarly, management has a comparable observation. IBM's 2008 "Global CFO Study" reported that 62 percent of enterprises with revenues greater than $5 billion encountered a major risk event that substantially affected operations or results in the last three years and nearly half (42 percent) stated that they were not adequately prepared.[5]

Many of the risks threatening an enterprise are difficult to see and manage, given their systemic nature. However, while many risks may be unknown, they often have a similar impact. Management and boards of directors are increasingly

being held accountable for considering the probabilities and impact of various possible risk scenarios tied to their overall business strategies, even for risk events that may not be foreseeable. For example, the events of 9/11 and the catastrophic impact of Hurricane Katrina, although "unknown" by most, had similar impacts: loss of employees, destroyed operations, damaged IT infrastructure, lack of cash flow, and so on. Management and boards are not expected to predict the next 9/11–type event, but they are expected to consider and be proactive about thinking of responses to events (whatever the cause) that might have a similar impact. That is, management should have a plan for any significant scenario that might lead to consequences that might be detrimental to its core strategy, such as a loss of employees, destroyed operations, damaged IT infrastructure, lack of cash flow, drastic shift in regulations, and so on.

The rise in the volume and complexities of risks is complicated by the fact that many of the techniques used by boards and senior executives are dated, lack sophistication, and are often ad hoc. Few boards and senior executives have robust key risk indicators that provide adequate data to recognize shifts in risks patterns within and external to their organizations, resulting in an inability to proactively alter strategic initiatives in advance of risk events occurring. This has created an "expectations gap" between what stakeholders expect boards and senior executives to do regarding enterprise-wide risk management and what they actually are doing.

In response to these changing trends, organizations are embracing ERM because it emphasizes a top-down, holistic approach to effective risk management for the entire enterprise. The goal of ERM is to increase the likelihood that an organization will achieve its objectives by managing risks to be within the stakeholders' appetite for risk. ERM done correctly should ultimately not only protect but also create stakeholder value.

ERM Positioned as Value-Adding

ERM differs from a traditional risk management approach, frequently referred to as a "silo" or "stovepipe" approach, where risks are often managed in isolation. In those environments, risks are managed by business unit leaders with minimal oversight or communication of how particular risk management responses might affect other risk aspects of the enterprise, including strategic risks. Instead, ERM seeks to strategically consider the interactive effects of various risk events with the goal of balancing an enterprise's portfolio of risks to be within the stakeholders' appetite for risk. The ultimate objective is to increase the likelihood that strategic objectives are realized and value is preserved and enhanced.

Several conceptual frameworks have been developed in recent years that provide an overview of the core principles for effective ERM processes. In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its "Enterprise Risk Management—Integrated Framework," with this definition of ERM (see www.coso.org):

> *Enterprise risk management is a process, effected by the 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 the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

Note that ERM is directly related to "strategy setting." For ERM to be value creating, it must be embedded in and connected directly to the enterprise's strategy. Another part of this definition refers to the goal of ERM, which is to help the enterprise achieve its core objectives. So, to be effective, ERM must be part of the strategic planning process and strategy execution processes.

The Conference Board's 2007 research study, "Emerging Governance Practices in Enterprise Risk Management," notes that while many organizations are engaging in some form of ERM, only a few have full-fledged ERM program infrastructures.[6] Many of these organizations initially launched their ERM efforts out of a compliance function, such as compliance with SOX, emerging privacy legislation, and environmental regulations. More boards and senior executives are now working to shift their ERM approach from a compliance orientation to a *strategic orientation*, consistent with the view that an enterprise-wide approach to risk management should be value enhancing. A 2008 survey, "The 2008 Financial Crisis: A Wake-Up Call for Enterprise Risk Management," by the Risk and Insurance Management Society (RIMS) found that about 65 percent of the businesses surveyed have begun or plan to implement a strategic risk management system.[7]

Board Demands for More Strategic Risk Management

Boards are feeling an increasing pressure to strengthen their overall oversight of the enterprise's risk management processes, with a stronger emphasis on strategic risk management. Recent reports, such as the Conference Board's "Overseeing Risk Management and Executive Compensation" report issued in December 2008, note that while companies report some progress in developing an enterprise-wide risk management program, it has yet to be adequately embedded in strategy execution and entity culture.[8]

Boards are becoming more aggressive at pushing management to reassess vulnerabilities in existing risk management processes and to begin strengthening the soundness of its risk management analysis to the company's strategic setting activities. Benchmarking surveys about the state of ERM consistently find that the launch of ERM is often tied to the board's (more specifically the audit committee's) demand for more robust risk management processes. Boards are now asking management about their risk oversight processes and they are adding formal risk discussions to their agendas on a regular basis.[9] Boards are also seeking to take a strategic view of Governance, Risk and Compliance (GRC) by setting and articulating the organization's "Enterprise Risk Policy and Appetite" and the role of each GRC function.[10] Despite these emerging trends, board members still believe they need to have a better handle around issues affecting *strategic risk*.

INTEGRATING RISK INTO STRATEGIC PLANNING

Successful deployments of ERM in strategic planning seek to maximize value when setting strategic goals by finding an optimal balance between performance goals and targets and related risks. As management evaluates various strategic alternatives designed to reach performance goals, it includes related risks across each alternative in that evaluation process to determine whether the potential returns are commensurate with the associated risks that each alternative brings. It also considers how one strategic initiative might introduce risks that are counterproductive

to goals associated with another strategy. At that point, management is in a better position to evaluate various strategic alternatives to ensure that the combined risks that the entity might take on are within the stakeholders' appetite for risk and that they collectively support the strategic direction desired.

Considering risk during strategy planning also creates an ability to seize risk opportunities. Again, the goal of ERM is to preserve and enhance value. In some situations, ERM may reveal areas where the enterprise is being too risk averse or is ineffectively responding to similar risks that exist across multiple silos of the enterprise. In other situations, ERM may identify risk opportunities that may create potential increased returns to the enterprise. If risks are ignored in strategy, risk opportunities may be overlooked.

A consumer products company's experience illustrates the advantage of connecting strategy and risks. As part of its sales strategy, the company sought to increase revenues by strategically aligning with a key distributor customer through electronic reordering systems. As part of this alliance, the consumer products company entered into contracts requiring the automatic shipment of products to the retail customer's distribution warehouses within two-hour increments upon receipt of the customer's electronic reorder purchase request.

As the consumer products company began to launch its ERM processes, senior management quickly discovered a huge potential threat to this strategic arrangement with the retail customer. The company's information technology (IT) disaster recovery processes were set to be within acceptable tolerance limits established by the IT group. In an effort to balance costs with perceived IT needs, the IT group had put recovery procedures in place to fully restore IT-based sales systems within a two-day (not two-hour) period. When core sales executives learned about this recovery time frame, they quickly partnered with IT to reduce recovery thresholds to shorter windows of time. Had they not linked IT's disaster recovery response risks with the sales strategies to fulfill customer orders within two-hour increments, a looming IT disaster could have significantly affected their ability to achieve sales goals, thus compromising the enterprise's ability to achieve strategic goals. Needless to say, this discovery also prevented other risks that might have been triggered by a disaster, including legal risks tied to contract violations, cash flow losses due to idle sales functions, and reputation risks that could have been realized given the large size and visibility of both the consumer products company and retailer customer.

Recognizing Strategic Business Risk

Strategic risk management can help companies avoid the problem of not recognizing risks soon enough and can help management take swift action to deal with those risks that do occur. What initially appeared to be a minor disruption in the value chain for Nokia and Ericsson in March 2000 turned out to be a critical event for both companies. On Friday, March 17, 2000, a line of thunderstorms appeared in Albuquerque, New Mexico. A lightning bolt struck a Philips semiconductor plant, causing a fire in a plant that made chips for both Nokia and Ericsson and presented similar risks to both companies. The fire was minor, lasting only 10 minutes, and the damage at first appeared to be limited, so Philips expected to be back in operation within a week. As it turns out, the disruption to the plant was months rather than weeks, and the impact on production was significant.

Nokia quickly noticed the problem with the supply of the parts even before Philips told them there was a real problem. They took fast action to address the situation once they determined that the potential impact of the disruption in the supply of chips from the Philips plant could translate into an inability to produce 4 million handsets, representing 5 percent of the company's sales at the time.

In contrast, Ericsson responded slowly and didn't have alternative sourcing options. By the time management realized the extent of the problem, they had nowhere else to turn for several key parts. This partly stemmed from the company's strategy in the mid-1990s, when it simplified its supply chain to cut costs and in the process weakened its supply backup. One manager at Ericsson said: "We did not have a Plan B." Underestimating the risk of the disruption in supply from the Philips plant and being unable to manage the problem were major factors that led to Ericsson exiting the phone headset production market in 2001.[11]

What lessons do these contrasting cases offer about integrating strategies and risk management surrounding the supply chain?[12]

- Link the potential impact of supply chain disruptions to revenue and earnings to prioritize and manage risk.
- Build in the necessary levels of redundancy and backup and maintain supply chain intelligence and relationships.
- Continuously monitor supply chain performance measures to quickly identify problems so that countermeasures can be taken.
- Share information and foster communication at the first instance of a problem.

Evaluating Strategic Business Risk

The first step in strategic risk management is finding a way to systematically evaluate a company's strategic business risk. That has to begin with first making sure that management and the board understand the entity's key strategies that are designed to preserve and create stakeholder value. For a for-profit entity, key strategies are generally linked to increasing shareholder value through initiatives designed to boost revenues, to maintain or reduce costs, or to pursue growth through mergers and acquisitions. A thorough understanding of specific drivers of shareholder value that management and the board are pursuing is necessary before risks surrounding those drivers can be accurately and completely considered. And, that understanding of specific strategy drivers has to permeate leadership across the organization if risks are to be managed effectively.

The next step to strategic risk management surrounds defining the entity's use of the term "risk." Michael Porter's definition in his landmark book, *Competitive Advantage*, is useful: "Risk is a function of how poorly a strategy will perform if the 'wrong' scenario occurs."[13] Thus, strategic risk management begins by identifying and evaluating how a wide range of possible events and scenarios will impact a business's strategy execution, including the ultimate impact on the valuation of the company.

Before management can effectively manage risks that might be identified by various scenario analyses, they need to define an overriding risk management goal.

Risk appetites can vary across industries and entities. Without an understanding of stakeholder appetites for risks, neither management nor the board know what strategic risks are to be managed and what risks are to be accepted.

The Return Driven Strategy framework is an effective tool for integrating strategic goals and risk management goals. The framework is the result of more than a decade of research and application, involving the study of thousands of companies and the identification of strategic activities that separate the best performers from the worst. The Return Driven Strategy framework describes the hierarchy of strategic activities of best performing companies in terms of financial impact and shareholder value.

The Return Driven Strategy is comprised of 11 core tenets and 3 foundations that together form a hierarchy of interrelated activities that companies must perform to deliver superior financial performance. These tenets and foundations summarize the common activities of high-performance companies and identify flawed strategies of marginal performers. Here is a list of the 11 tenets and 3 foundations of Return Driven Strategy.[14]

11 Tenets of the Return Driven Framework

The Commitment Tenet

1. Ethically maximize wealth.
   Management must understand, define, and then align all activities toward the shareholder wealth creation objectives and ensure that the business operates within the ethical parameters set by its communities.

Two Goal Tenets

2. Fulfill otherwise unmet customer needs.
3. Target and dominate appropriate customer groups.
   To avoid commoditization, management must focus on fulfilling otherwise unmet customer needs. The path to business success is through the customer—sufficiently large enough groups of customers. This means targeting economically profitable customer groups that have sufficient size and growth opportunities while fulfilling otherwise unmet needs which are not commoditized.

Three Competency Tenets

4. Deliver offerings.
5. Innovate offerings.
6. Brand offerings.
   Through synchronization of these three competency tenets, offerings are created that target customer needs. Management needs to consider the *executability* of plans at the outset, with the three higher tenets as primary goals. Continuous innovation of the entirety of the offerings to develop offerings designed to enhance needs currently unfulfilled. Branding of the offerings to bridge the customer's explicitly understood need to the offering that uniquely fulfills it.

Five Supporting Tenets

7. Partner deliberately.
8. Map and redesign processes.
9. Engage employees and others.

10. Balance focus and options.
11. Communicate holistically.

    The supporting activities are done to support the achievement of the higher level tenets: the competency tenet, goal tenet, and commitment tenet.

There are three foundations that are critical to the Return Driven Strategy:

1. Genuine assets.

   The 11 tenets are the "verbs" of strategy. Genuine assets are the "nouns." Genuine assets are the building blocks of sustainable competitive advantage. Activities are copied by competitors, leading to price competition and reduced cash flow returns. This can be defended only by leveraging unique assets to create unique offerings that cannot be copied (patents, brands, scale and scope, etc.).
2. Vigilance to forces of change.

   The ability and agility to capitalize on opportunities and avoid threats is foundational. Management must take advantage of opportunities and avoid threats in each of the three tenets arising from (1) government, legal, and other regulatory change, (2) demographic and cultural shifts, (3) scientific and technological breakthroughs.
3. Disciplined performance measurement and valuation.

   A discipline that links strategy to ultimate financial results is necessary for measuring the achievement of strategic goals. Performance measures must be in place to support the achievement of the strategy and its resulting value creation.

This framework describes how an enterprise's strategy can be aligned with the ultimate objective to "Ethically Maximize Shareholder Wealth." This is a valid goal for a business entity: to create shareholder wealth, to strive to maximize it, and to do so while adhering to the ethical parameters of stakeholders and communities.[15]

That ultimate strategic goal can work simultaneously as the entity's risk management goal as well. That is, management must understand, define, and then align risk management activities toward ethical shareholder wealth creation objectives. In doing so, risk management activities must be justified in terms of shareholder wealth creation. If wealth preservation or creation isn't linked to risk management activities, then particular risk management activities should be challenged.

We believe that, to be effective, a framework for strategic risk management needs to include these three characteristics:

1. Alignment with a commitment to ethically create shareholder wealth. Risk management must have a strong alignment with protecting and creating shareholder value. Rule No. 1 of strategic risk management should read: "First, don't destroy shareholder value." But to add value, strategic risk management should be firmly aligned with the creation of shareholder wealth and have a focus on risk opportunities (e.g., the "upside" of risk). Of course, shareholder wealth should be created within the ethical parameters of the constituents and the communities in which the company operates.

Any framework for strategic risk management should have the ability to make the connection among the strategy of the organization, its execution and related risk management, and the valuation of the entity.[16]

2. Holistic. Strategic risk management should be holistic and broad enough to encompass the spectrum of entity-wide activities needed to achieve an organization's strategy. A framework for strategic risk management needs to be integrated so that various facets of strategic business risk can be linked with the overall goals of the business. This is where an ERM approach to risk management helps provide value through its emphasis on viewing risk-related scenarios using a top-down, holistic portfolio approach to determining how various silo risk events might interact to limit or destroy value. A holistic approach to strategic risk management helps connect various business unit goals and objectives and related risks to the overall goal of maximizing shareholder wealth. Without a holistic view, strategic activities within one aspect of the enterprise may be creating strategic risks for another part of the business.
   For example, Harley Davidson's recent letter to shareholders describes one of its strategic goals to expand into international markets, particularly China and Japan. The letter also describes another strategic goal to enhance its "H.O.G." brand mystique and motorcycling lifestyle. In this case, the strategic desire to expand into Asian cultures, if left unmanaged, has the potential to create risks associated with its strategic desire to expand the Harley mystique if changes are made to Harley products to satisfy the motorcycling preferences of riders in different cultures. To effectively manage strategic risks, management needs to monitor how each strategic initiative might be throwing off counterproductive risks impeding other strategic objectives.[17]
3. Capable of identifying and evaluating events and forces of change. Strategic risk management has to be an ongoing, continual process. It can't be an activity that happens only occasionally. Risks are constantly evolving, which means an organization's strategies may need to evolve as well, so effective strategic business risk management must be capable of regularly identifying and evaluating how events, scenarios, and forces of change will impact the business strategy and its performance. Management's dashboard of key performance metrics should also include key risk indicators that provide leading information about changing risk conditions so that management is better prepared to adjust strategies ahead of the risk curve in a proactive manner, rather than be blindsided by shifting risk conditions that are realized too late to adjust deployments of key strategies, such as the situation at Ericsson. Robust management scorecard-reporting systems that include key strategy and risk management metrics can help strengthen management's effectiveness at staying on top of key changes that may impact the entity's strategic goals.

Using a Framework to Build a Strategic Risk Management Mindset

Executive teams have used the Return Driven Strategy as a holistic framework to set, evaluate, refine, and execute strategy. It also has been integrated into strategic

planning processes and used as a way to evaluate the impact of events and scenarios, including merger-and-acquisition scenarios, on a strategy's performance. As directors and management have used the framework to evaluate the business strategy, they have been able to hone in on key risks that could destroy shareholder value while considering the upside of risk in terms of the opportunities, thereby using it as a strategic risk management framework.

CREATING A STRATEGIC RISK MINDSET AND CULTURE

How risky is our strategy? What events and risk scenarios could ruin our business? Do we have the right countermeasures and risk management strategies in place? These are just some of the questions on the minds of executives and board members today.

A Strategic Risk Management Mindset

A strategic risk management mindset focuses on examining how well a business strategy will perform under different scenarios and events. It encourages and supports thinking about scenarios where the strategy could perform so poorly that it could potentially result in significant losses, destruction of shareholder value, or a damaged corporate reputation. For example, management at Fidelity Investments knows that their strategy of providing investment services to an investor base all across the globe creates unbelievable demand for resiliency in its information technology functions. The tolerance for information systems outages or lack of access to pricing information approaches zero. They know that customers have little appetite for Fidelity to say their "systems are down." Thus, one of the key areas of focus of Fidelity's Risk Advisory Services Group is to oversee the business continuity planning processes at Fidelity.

A strategic risk mindset should also consider the "upside" of risk.[18] For example, the Target Corporation sidestepped the competitive threat from Wal-Mart by focusing on a customer segment different from Wal-Mart's and achieved profitable growth opportunities in the process. As another example, Samsung, confronted with serious brand erosion and commoditization risk, turned its attention to build on product innovation, speed to market, and a strong brand to turn a position of weakness into a position of market strength.

Risk can include loss of tangible assets, and it can also mean the potential loss of one of the company's most valuable assets—its reputation.[19] The H.J. Heinz Company has centered its enterprise risk management function on supporting an ultimate goal of protecting the Heinz reputation. In fact, its ERM program is formally known within as "Enterprise Reputation and Risk Management (or ER^2M)." Heinz's ER^2M helps the company meet two primary reputation related goals: (1) to further support doing the common thing uncommonly well, and (2) to help Heinz become the most trusted packaged food company. To help management see the importance of thinking about risk and reputation, Heinz defines risks as "anything that can prevent the company from achieving its objectives." They

recognize that any event that affects the Heinz reputation in the food industry will directly impact its ability to achieve its objectives.

Ultimately, strategic risk management and ERM need to be connected with the potential impact on shareholder value. Effective strategic risk management should provide a way for identifying and evaluating how a wide range of possible events and scenarios will impact a business's strategy execution, including the impact on the assets and shareholder value of the company. That's how risk management is positioned at the Dow Chemical Company. The objective of effective enterprise risk management at Dow is to improve management's ability to run its business with the view that if they can manage risks better, they can be more competitive. Management and the board realize they have the responsibility to pursue opportunities, which will require the assumption of risks. They seek to assume those risks in a well-managed, controlled manner that recognizes the reality that as new strategies are created, new risks arise that need to be managed.

The Return Driven Strategy framework provides a way to evaluate the strategic risks of a company from the perspectives of shareholder value risk, financial reporting risk, governance risk, customer and market risk, operations risk, innovation risk, brand risk, partnering risk, supply chain risk, employee engagement risk, R&D risk, and communications risk. It also provides a useful framework for understanding the cause-and-effect linkages in critical risk scenarios and explains how those scenarios would play out in the business strategy and impact profitability, growth, and shareholder value.[20]

The framework encourages thinking around these risk categories:

- *Shareholder value risk* provides a high-level overview of risk and is driven by future growth and return on investment as reflected in the plans of the company and the company's perceived ability to execute on them. Anything that will impede growth and returns, including the risk of unethical activities of the company, should be considered in assessing shareholder value risk using the first tenet of Return Driven Strategy, "Ethically Maximize Wealth."
- *Financial reporting risk* is driven by reporting irregularities in areas such as revenue recognition, which can result in restatements of financial reports and be devastating to shareholder value.
- *Governance risk* is driven by factors such as controls and governance capabilities, including the need for compliance with laws and regulations.
- *Customer and market risk* is driven fundamentally by the extent to which a company's offerings fulfill otherwise unmet needs, and this provides protection against competition.
- *Operations risk* can be driven by any part of the value chain and often surfaces with the inability to deliver offerings, which is at the heart of Return Driven Strategy.
- *Innovation risk* is driven by the inability to change or create offerings that fulfill customer needs better than your competitors do.
- *Brand risk* includes the risk of brand erosion and damage to a company's reputation.
- *Partnering risk* is driven by the activities of your partners, from vendors to joint ventures, to other associations, including counterparty risks.

- *Supply chain risk* focuses on the increasing risk in outsourcing and global supply chains.
- *Employee engagement risk* is driven by the employment practices of the company.
- *R&D risk* is driven by the processes and pipeline of options for new offerings for future growth.
- *Communications risk* is driven by how well your company communicates internally and externally.

Recognizing Value of Strategic Risk Management at High-Performance Companies

Research on high-performance companies can provide valuable insights about risk management. High-performance companies are vigilant to forces of change, and they manage risks and opportunities better than other companies. By better understanding how the success or failure of a business is driven by its plans and actions, we can improve how we value companies—and run our businesses.

Research about high-performance companies highlights that one of the challenges facing management teams is how to link business plans and enterprise risk management. There are three approaches for effective strategic risk management to consider: (1) a strategic risk assessment process, (2) a process to identify and protect Genuine Assets that are at risk, and (3) strategic risk monitoring and performance measurement.

BUILDING A STRATEGIC RISK ASSESSMENT PROCESS

A simple process for strategic risk assessment involves four steps:[21]

1. **Risk assessment of plans.** Strategic risk assessment can begin by conducting an overall risk assessment of strategic plans, including an understanding of how they drive value and the key assumptions those plans are based on. This assessment includes scenario analysis of various iterations of changing assumptions surrounding drivers of the strategy.
2. **Identify critical risk scenarios.** The next step is to identify and describe "critical risk scenarios" considering the severity and likelihood of the events and scenarios that might occur, especially those outside management's control, such as systemic risks. At this stage, management and the board need to define their overall appetite for these critical risk scenarios.
3. **Identify countermeasures.** Next, management would identify possible countermeasures for managing the critical risk scenarios and would consider the cost/benefit of the countermeasures.
4. **Establish a process for continuous monitoring.** Management would establish a process for continuous monitoring of the risk profile of the company, including the use of key risk indicators (KRIs) and best practices of performance measurement and performance management such as the Balanced Scorecard.[22]

Here are some questions to address during a strategic risk assessment process:

- What events or scenarios could create significant downside risk in your business strategy and plans?
- What key assumptions have been made about the viability of specific strategic initiatives and what ranges of possible scenarios exist surrounding the variability inherent in these assumptions?
- What is our appetite surrounding certain strategies and their associated ranges of key risk exposures? What is the worst case scenario surrounding each strategy and would the entity be able to survive certain risk events?
- What countermeasures have been developed to address these risk scenarios and events?
- Has the company considered the upside of risk and how it plans to realize the opportunities?
- What are the roles of the CFO, general counsel, chief risk officer (CRO), internal audit, and others in assessing and managing the threats and opportunities in your plans and business strategy?
- How is enterprise risk management incorporated and embedded in your plans and business strategy?
- What performance measures and key risk indicators are you monitoring to continuously assess and manage strategic business risk?

Strategic Risk Management Processes

There are several approaches to building a strategic risk management process. Several are described next.

Risk assessments. One approach is to regularly assess strategic risks from three perspectives: risks, opportunities, and capabilities (ROC). *Risks* are about risk of loss—the downside of risk, such as loss of revenue or loss of assets. *Opportunities* are about the upside of risk, such as opportunities for gains in revenue, profitability, and shareholder value. *Capabilities* are about distinctive strengths of an organization that can be used to manage the risks and opportunities.

Tools for risk assessment. There are many tools that can be useful in strategic risk assessment, including brainstorming, analysis of loss data, self-assessments, facilitated workshops, SWOT (strengths, weaknesses, opportunities, threats) analysis, risk questionnaires and surveys, scenario analysis, and other tools.

Competitive intelligence. The area of competitive intelligence (CI) can be a valuable part of strategic risk management. CI is an integral component of fact-based strategic planning processes. It should definitely be part of strategic risk management and ERM. "The ethical collection and analysis of CI can reduce the risk associated with strategic decision making," says Gary Plaster of the Landmark Group and a founding member of the Society of Competitive Intelligence Professionals. Around 400 BC, Sun-tzu in *The Art of War* wrote "Keep your friends close and your enemies closer," which is one way of thinking about CI. For example, pharmaceutical

companies are vigilant about being at trade shows and scientific meetings, and they monitor clinical trials in the industry. "War games" are used at pharmaceutical companies like Wyeth to develop plans to counter potential market moves by competitors.[23] Competitive intelligence is an asset that can be used to manage customer and market risks.

Corporate sustainability risk. One of the areas often overlooked in risk management is related to corporate sustainability and corporate social responsibility (CSR). Connecting strategy and CSR is a challenge for executive teams, as Debby Bielak, Sheila Bonini, and Jeremy Oppenheim wrote in their October 2007 article, "CEOs on Strategy and Social Issues," in the *McKinsey Quarterly.* The risks and opportunities facing companies in the area of corporate sustainability are more complex and have greater potential impact than ever before, and senior executives, board members, and managers are seeking better ways to manage these challenges and opportunities. In his book *Making Sustainability Work*, Marc Epstein presents a definition for corporate sustainability that's useful in strategic risk management. He focuses on nine principles of sustainability: (1) ethics, (2) governance, (3) transparency, (4) business relationships, (5) financial return, (6) community involvement/economic development, (7) value of products and services, (8) employment practices, and (9) protection of the environment. Each of these areas can be assessed as part of strategic risk management. For example, changes in environmental regulations and expectation of environmental standards for companies in a global business environment should be considered in risk assessment and risk management strategies.

Risk transfer and retention strategies. One of the basic countermeasures for managing and mitigating risk involves risk transfer and retention strategies. After identifying critical risk scenarios, which include the potential effect on company assets and shareholder value, management must determine how much should be retained or transferred. The risk management strategy should consider whether to protect corporate assets by purchasing insurance, self-insuring, or creating a captive. This assessment requires a deep understanding of the types and limits of insurance and consideration of emerging legal, regulatory, and political trends; damage awards; geographic locations; available insurance products; and options as well as coverage law.

Focus on Genuine Assets at Risk

Some of the most valuable assets of an organization aren't on the balance sheet. Genuine assets include the most valuable tangible and intangible resources and capabilities of an organization and must be protected because some of them may be at risk.[24] Companies routinely insure tangible assets on the balance sheet to protect against loss. But what about protecting the genuine assets?

Genuine assets are the tangible and intangible resources, capabilities, and traits that make an organization and its offerings unique, such as employee expertise, brand, reputation, and so on. As mentioned, some genuine assets appear on the balance sheet, but many don't. As the "building blocks" of strategy, genuine assets form the basis for creating sustainable competitive advantages. And only through

these advantages can you plan and execute business strategy that leads to higher returns, higher growth, and, ultimately, increased market value.

When identifying these assets, management should be very specific as to what the genuine asset is. They should think specifically about how it allows the company to accomplish its strategy in ways other firms couldn't, thereby leading to higher performance. How difficult would it be for another firm to develop a similar genuine asset, allowing it to copy the activity that led to high performance? How long would it take? How much money would it cost?

To help identify and manage the risks to genuine assets, management should ask three questions:

1. What are the *most valuable* and *unique* capabilities and resources (genuine assets) of the company?
2. What scenarios and events could put the most valuable genuine assets at risk?
3. What countermeasures can be developed to protect these assets?

Examples of genuine assets to consider in a risk assessment would include corporate reputation, customer information, competitor intelligence, vendor intelligence, specialized processes and capabilities, existing patents and trademarks, and intellectual property that should be protected with patents, trademarks, and other means.

Customer information is an example of a genuine asset that must be protected. Information security is a big issue at most companies, yet breaches occur, sometimes with significant potential impact. For example, the British government recently announced that government workers lost two computer disks containing names, addresses, dates of birth, national insurance numbers, and banking information for approximately 25 million residents of the United Kingdom, almost half its population. Effective risk management in the area of data security requires the right mindset and attitude toward information security among employees. It requires an understanding and awareness that the information on a $20 storage device or a $1,000 laptop, if not protected, could result in potential loss of customers, corporate reputation, and shareholder value.

Some genuine assets can support and be part of an effective risk management strategy and can help protect a company against risks. For example, having a "Plan B" in place for potential disruptions in critical parts of the supply chain is an example of a genuine asset for effective strategic risk management. Another example is employees having a risk mindset and risk attitude that support the organization's strategy and risk appetite.

Strategic Risk Management and Performance Measurement

Many people believe that the recent financial crisis is largely attributable to the failure to link performance incentives with the risk management activities within the enterprise. Many of the executive compensation packages provide numerous unintended incentives for management to assume excessive amounts of risk exposures to achieve specific performance compensation targets.

Compensation incentives are typically designed to encourage executives to achieve strategic goals and initiatives and boards have typically evaluated those executives on whether they successfully achieve specific targets. Unfortunately, for many, risks associated with those compensation packages are overlooked. Boards are sometimes unaware of the nature of all risk exposures to the organization created by the executives. As long as the expected returns are achieved, few questions about the amount and types of risks being assumed are voiced.

The recent crisis is now placing greater light on the risks inherent in these executive compensation packages, and regulations are now being established to shed more insight into the risks associated with performance incentives. For example, the U.S. Treasury Department announced in January 2009 a new requirement for the chief executive officer (CEO) of financial institutions that receive federal funding under the Troubled Asset Relief Program's (TARP) Capital Purchase Program. For those entities, the CEO must certify within 120 days of receiving the funding that the entity's compensation committee has reviewed the senior executive's incentive compensation arrangements with the senior risk officers to ensure that these arrangements do not encourage senior executives to "take unnecessary and excessive risks that could threaten the value of the financial institution."

Effective strategic risk management should be a continual process that includes metrics for continuous monitoring of risk. An organization's key risk indicators and metrics should link to the potential impact of risk on shareholder value. Holistic performance management systems such as the Balanced Scorecard give organizations an unprecedented opportunity to align strategy and performance measures with risk management—and to achieve integrated, strategic risk management.

The Balanced Scorecard focuses on strategy and accountability and fosters a continuous process for risk assessment and risk management. The Balanced Scorecard framework can help management develop and use these risk metrics. With its focus on strategy and accountability, the Balanced Scorecard can foster a continuous process for risk assessment and risk management.

Strategy maps also can provide a useful way to understand the cause-and-effect relationships in critical risk scenarios and can suggest risk metrics that would be valuable in effective risk management. Risk dashboards can also provide a way to monitor key metrics and trends.

Kaplan and Norton's closed-loop management system (the Execution Premium model) provides another useful platform for a systematic approach to strategic risk management that integrates with overall management.[25] The Strategic Risk Management Lab at DePaul University has been working with management teams to help them embed strategic risk management into each stage of the management system.

- In Stage 1, "Develop the Strategy" involves defining mission, vision and values; conducting strategic analysis and formulating strategy. This stage is where companies can conduct strategic risk assessments and formulate strategic risk management plans as part of their strategy. This can be done using a variety of tools and frameworks including the Return Driven Strategy framework.
- In Stage 2, "Translate the Strategy" involves defining strategic objectives and themes; selecting measures, targets and strategic initiatives. In this stage,

management can identify strategic risk management objectives and measures that could be included in Balanced Scorecards. Risk management objectives can be incorporated in the financial perspective and internal process perspective of Balanced Scorecards and Strategy Maps. They can also use strategy maps to identify the cause-and-effect linkages and root causes of key strategic risks.

- In Stage 4, "Monitor and Learn" involves holding strategy reviews and operational reviews. In this stage management teams can hold strategic risk management reviews.
- And in Stage 5, "Test and Adapt" management conducts strategic risk analysis.

These are just a few examples of using the closed-loop management system to drive better strategic risk management.

Critical Steps for Value-Added Strategic Risk Management

Strategic risk management is increasingly being viewed as a core competency at both the management and board levels. In fact, board members are increasingly focused on strategic risk management, asking executives such questions as "Of the top five strategic business risks the company faces, which ones are you looking at, and what countermeasures are you devising?" The Strategic Risk Management Lab in the Center for Strategy, Execution, and Valuation at DePaul University is sharing with management teams and boards emerging best practices gleaned from its research. Consider the following list of 10 practices worth striving toward.[26]

1. Communicate and share information across business and risk functions—and externally. This is considered by some to be the ultimate risk management "best practice."
2. Break down risk management silos. Establish interdisciplinary risk management teams, so that each functional area can understand where it fits into the entire company strategy and how it affects other areas.
3. Identify and, where possible, quantify strategic risks in terms of their impact on revenue, earnings, reputation, and shareholder value.
4. Make strategic risk assessments part of the process of developing strategy, strategic plans, and strategic objectives. Again, this requires a combination of skills that can be achieved by creating interdisciplinary teams.
5. Monitor and manage risk through the organization's performance measurement and management system, including its Balanced Scorecard.
6. Account for strategic risk and embed it within the strategic plan and strategic plan management process. Wherever scenario planning is included in developing the strategic plan, there should also be a discussion of countermeasures in the event that a risk event occurs.
7. Use a common language of risk throughout your organization. Everyone must understand the organization's particular drivers of risk, its risk appetite, and what management considers acceptable risk levels.
8. Make strategic risk management, like strategy management itself, a continual process. Risk is inherently dynamic, so risk management and

assessment must evolve from being an event to being a process—and must include regular analysis and critical risk information refreshes. Strategic risk management reviews should be conducted as part of regular strategy reviews.

9. Develop key risk indicators (KRIs) to continuously monitor the company's risk profile. Like the Balanced Scorecard with its measures, targets, and initiatives, the risk management system should include KRIs, thresholds and trigger points, and countermeasures to mitigate or manage the risk.
10. Integrate ERM into Strategy Execution Systems. This means integrating ERM into the entire management system. This will require strategic risk management as a core competency in organizations and a commitment to continuously monitor and manage risk in the strategy and its execution.

CONCLUSION

The need to connect strategy and enterprise risk management couldn't be more relevant than it is in the current economic climate. Effective strategic risk management is likely to make the difference between survivability and demise for many. Designed effectively, the connection of ERM and strategy should be value-adding, allowing the enterprise to be more proactive and flexible in managing uncertainties tied to strategies as they unfold.

The key to successful strategic risk management is the ability to identify those risks embedded in the organization's business strategy that are potentially the most consequential. Focusing on strategic risks serves as a filter for management and boards of directors to reduce the breadth of the risk-playing field and ensure that they are focused on the right risks.

NOTES

1. For example, see Standard & Poor's "Enterprise Risk Management: Standard & Poor's To Apply Enterprise Risk Analysis to Corporate Ratings," (May 2008) New York. www.standardandpoors.com.
2. For example, see the *New York Times* magazine "Risk MisManagement" January 4, 2009, feature story that was highly critical of the short comings of risk oversight processes at many of the failed financial services institutions.
3. Federal Reserve Governor Randall S. Kroszner's speech, "Strategic Risk Management in an Interconnected World," October 20, 2008, Baltimore, Maryland. www.federalreserve.gov.
4. Ernst & Young 2006 report, "Board Members on Risk." www.ey.com.
5. IBM Global Business Survey's "Balancing Risk and Performance with an Integrated Finance Organization: The 2008 Global CFO Study" (2008).
6. The Conference Board's 2007 research study, "Emerging Governance Practices in Enterprise Risk Management."
7. "The 2008 Financial Crisis: A Wake-Up Call for Enterprise Risk Management," by the Risk and Insurance Management Society (RIMS).
8. The Conference Board's "Overseeing Risk Management and Executive Compensation" report (December 2008).

9. See the article by Mark Beasley, Bruce Branson, and Bonnie Hancock, titled "Rising Expectations: Audit Committee Oversight of Enterprise Risk Management," *Journal of Accountancy* (April 2008) 44–51.
10. See the article by Mark L. Frigo and Richard J. Anderson, "A Strategic Framework for Governance, Risk and Compliance" *Strategic Finance* (February 2009).
11. For more about this example, see "Trial by Fire: A Blaze in Albuquerque Sets Off Major Crisis for Cell-Phone Giants" in the January 29, 2001, issue of the *Wall Street Journal*.
12. See article by Mark L. Frigo, "Strategic Risk Management: The New Core Competency" *Balanced Scorecard Report* (January–February 2009).
13. Porter, Michael E. *Competitive Advantage* (New York: Free Press, 1985), 476.
14. Frigo, Mark L., and Joel Litman, *Driven: Business Strategy, Human Actions and the Creation of Wealth* (Chicago, IL: Strategy and Execution, 2008).
15. For more, see Mark L. Frigo and Joel Litman, *Driven: Business Strategy, Human Actions and the Creation of Wealth* (Chicago, IL: Strategy and Execution, 2008); "What Is Return Driven Strategy?" by Mark Frigo and Joel Litman in the February 2002 issue of *Strategic Finance*; and "Performance Measures That Drive the First Tenet of Business Strategy" by Mark Frigo in the September 2003 issue of *Strategic Finance*.
16. For more about this, see "When Strategy and Valuation Meet: Five Lessons from Return Driven Strategy" by Joel Litman and Mark Frigo in the August 2004 issue of *Strategic Finance*.
17. For more discussion of Harley-Davidson and strategic risk management, see Chapter 14, "Co-Creating Risk Management, Governance, and Transformational Change," in *Co-Creating the Future: Engaging Customers, Employees and All Stakeholders to Co-Create Mutual Value* by Venkat Ramaswamy and Francis Gouillart (2009); Frigo, Mark L. and Venkat Ramaswamy, *Co-Creating Wealth: A New Risk-Return Paradigm of Value Co-Creation* (2009); and Frigo, Mark L. and Venkat Ramaswamy, "Co-Creating Risk-Return" Working Paper (2009).
18. See Slywotzky, Adrian, "The Upside of Risk: The 7 Strategies for Turning Big Threats Into Growth Breakthroughs," *Crown Business* (2007).
19. For a discussion on the importance of reputation risk management, see the article by Robert Eccles, Scott Newquist, and Roland Schatz titled "Reputation and Its Risks," *Harvard Business Review* (February 2007).
20. For more about Return Driven Strategy, see Mark L. Frigo and Joel Litman, *Driven: Business Strategy, Human Actions and the Creation of Wealth* (Chicago, IL: Strategy and Execution, 2008).
21. See article by Mark L. Frigo, "When Strategy and ERM Meet," *Strategic Finance* (January 2008).
22. See Robert S. Kaplan and David P. Norton, "The Balanced Scorecard: Measures That Drive Strategic Performance," *Harvard Business Review* (January–February 1992) 71–79.
23. See "Corporate Covertness: More Firms Use 'CI' Analysts to Gather Data on Rivals, But It's Mostly Hugh-Hush" *Chicago Tribune*, December 10, 2007; and "The Intelligence Diaries: Here's Your Study Guide To What the Industry Once Knew—And Lost," *Pharmaceutical Executive*, November 2007.
24. For a discussion on genuine assets, see Chapter 12 "Genuine Assets" in Mark L. Frigo and Joel Litman, *Driven: Business Strategy, Human Actions and the Creation of Wealth* (Chicago, IL: Strategy and Execution, 2008).

25. Kaplan, Robert S., and David P. Norton, "Mastering the Management System," *Harvard Business Review* (January 2008), and Kaplan, Robert S., and David P. Norton, *Execution Premium: Linking Strategy to Operations for Competitive Advantage* (Boston, MA: Harvard Business School Press, 2008).
26. See article by Mark L. Frigo "Strategic Risk Management: The New Core Competency," *Balanced Scorecard Report* (January–February 2009).

ABOUT THE AUTHORS

Mark S. Beasley, PhD, CPA, is Deloitte Professor of Enterprise Risk Management and Professor of Accounting in the College of Management at North Carolina State University. He is the Director of NC State's Enterprise Risk Management (ERM) Initiative (www.erm.ncsu.edu), which provides leadership about ERM practices and their integration with strategy and corporate governance. Mark currently is serving on the board for the Committee of Sponsoring Organizations of the Treadway Commission (widely known at COSO). He has previously served on several national task forces and working groups, including the Auditing Standards Board SAS No. 99 Fraud Task Force and the advisory board for the Conference Board's research about board of director responsibility for ERM. He is the author of textbooks, casebooks, and continuing education materials and has published extensively in business and academic journals. Mark is also a frequent speaker at national and international conferences on ERM, internal controls, and corporate governance, including audit committee practices. He received a BS in accounting from Auburn University and a PhD from Michigan State University.

Mark L. Frigo, PhD, CPA, CMA is Director of the Center for Strategy, Execution, and Valuation and the Strategic Risk Management Lab in the Kellstadt Graduate School of Business at DePaul, and Ledger & Quill Alumni Foundation Distinguished Professor of Strategy and Leadership in the School of Accountancy at DePaul University. He is a leading expert in Strategic Risk Management. The author of 6 books and more than 80 articles, his work is published in leading business journals including *Harvard Business Review*. He is the editor of the Strategic Management section of *Strategy Finance* and lectures frequently at universities and conferences in Europe. He is the co-author with Joel Litman of the book *Driven: Business Strategy, Human Actions and the Creation of Wealth* (www.returndriven.com). He received his BS in Accountancy from the University of Illinois, an MBA from Northern Illinois University and completed postgraduate studies in the Kellogg Graduate School of Management at Northwestern University. He is a CPA in the State of Illinois and a Certified Management Accountant. Dr. Frigo received his PhD in Economics and Econometrics. Dr. Frigo serves as an advisor to executive teams and boards of directors in the area of Strategic Risk Management.