CHAPTER 1

Enterprise Risk Management

An Introduction and Overview

JOHN R.S. FRASER, FCPA, FCA
Former Chief Risk Officer, Hydro One Networks Inc.

ROB QUAIL, BASc
Principal, Robert Quail Consulting

BETTY J. SIMKINS, PhD
Department Head of Finance, Regents Professor of Finance, and Williams Companies Chair of Business, Spears School of Business at Oklahoma State University

COPYRIGHTED MATERIAL

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

—Often attributed to Charles Darwin, British naturalist

Prediction is very difficult, especially if it's about the future.

—Niels Bohr, 1922 Nobel Laureate in Physics

WHAT IS ENTERPRISE RISK MANAGEMENT?

We begin this chapter and the book with the above two quotes to highlight the importance of organizations being able to adapt to change and to being prepared for the uncertain future. We believe this book is crucial to organizations being ready for change, survival, and success and would like to see more organizations adopt enterprise risk management (ERM). ERM is about preparing the organization to survive and thrive in the future, as the Charles Darwin quote implies about living organisms, and we extend to our context. We believe that the organizations that are successful are the ones that are best able to adapt and adjust to the changing world they find themselves. History has shown this for both species and organizations. The Niels Bohr quote reminds us how difficult it is to predict the future. ERM prepares us for this!

In 2017, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) defined enterprise risk management as: "The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value." This 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*.

The purpose of ERM is not only to minimize risk exposure. It is to assist in finding the ideal level of risk for an organization to take in order to maximize opportunity. 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 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 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, academics, and students alike about this evolving discipline. 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. 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. Our companion volume, *Implementing Enterprise Risk Management: Case Studies and Best Practices* (2015), consists of numerous case study examples of how companies have actually implemented ERM in their organizations.

We believe that the implementation of ERM is not a one-size-fits-all exercise. Effective ERM implementations can include a broad range of activities, tools, and processes. Prudent practitioners will select and adapt common ERM practices to suit the culture, structure, and role of risk in value creation for their organization. *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 appetite, risk profiles, risk workshops, and the allocation of resources, while focusing on the principles that determine business success. This comprehensive resource also provides a thorough introduction to ERM as it relates to numerous specific risks such as credit, market, operational, climate change, cybersecurity, foreign exchange, and project management risks. As well, it offers a wealth of knowledge on the drivers, the techniques, the benefits, and the pitfalls to avoid in successfully implementing ERM.

DRIVERS OF ENTERPRISE RISK MANAGEMENT

There are theoretical and practical arguments for the use of ERM. As outlined in Chapter 2, "A Brief History of Risk Management," and Chapter 39, "A Review of Academic Research on Enterprise Risk Management," there has been an increasing consciousness in risk literature that a more holistic approach to managing risk makes good business sense.

External drivers for ERM's implementation have been studied, 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 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. 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.

For more information on the latest additions to regulatory requirements and recommendations for improved risk governance, please refer to Chapters 2 for highlights and to Chapter 6, "The Role of the Board in Risk Management Oversight," for more details on the changes.

Finally, it is important to note that ERM can increase firm value.[8] 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.

To summarize, the expected benefits to organizations from implementing ERM are that it:

- Ensures that the business objectives are clearly defined
- Reinforces the understanding of the business objectives throughout the layers of management
- May reduce the cost of capital
- May improve the credit rating
- Avoids surprises
- Helps ensure that resources are allocated to the most important areas of risks
- Improves team building among management and staff
- Improves the reporting of risks to all stakeholders

ABOUT THIS SECOND EDITION

In the decade since the first edition of this book was published, much has happened with regard to ERM practice. ISO and COSO released revised risk management framework documents, which provided more detailed guidance and placed increased emphasis on integration with strategy and the role of senior management. Significant progress was made in best practices in areas such as risk appetite, risk tolerance, and key risk indicators. And, perhaps most importantly, leading practitioners succeeded in integrating ERM into more business processes or applying ERM principles to business problems and processes.

For this reason, we chose to update, revise, or replace nearly all of the chapters from the first edition, and add many new ones; the book has grown from 28 to 43 chapters. Exhibit 1.1 lists the chapters in this second edition. Many of the new

Exhibit 1.1 Chapters in *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*

Chapter	Title
Part I: Overview and Drivers of Enterprise Risk Management	
1	Enterprise Risk Management: An Introduction and Overview
2	A Brief History of Risk Management
3	Strategic Risk Management: The Third Paradigm
4	The Role of the Board of Directors and Senior Management in Enterprise Risk Management
5	How to Teach Enterprise Risk Management: A Learner-Centered *Activities* Approach
6	The Role of the Board in Risk Management Oversight
Part II: Enterprise Risk Management, Culture, and Control	
7	ERM Frameworks
8	Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer
9	Creating a Risk-Aware Culture
10	Key Risk Indicators
11	Decision Risk Management
12	Increasing Adoption of Enterprise Risk Management in the U.S. Federal Government
13	Toolmaking in Risk Management: The Case of Core Values and the Formalization of "Risk Appetite"
14	Incorporating Risk Acumen and Enterprise Risk Management into Innovation Approaches
15	Scenario Planning as an Enrichment of Enterprise Risk Management
16	Unconscious Bias and Risk Management
17	Cognitive Bias: A Practical Approach
Part III: Enterprise Risk Tools and Techniques	
18	Risk Appetite and Tolerance in Competitive Strategy
19	How to Plan and Run a Risk Management Workshop
20	How to Prepare a Risk Profile
21	How to Allocate Resources Based on Risk
22	Quantitative Risk Assessment in ERM
23	Risk Appetite
24	Organizational Decision Making
25	The Challenges of and Solutions for Implementing Enterprise Risk Management
Part IV: Types of Risk	
26	Market Risk Management and Common Elements with Credit Risk Management
27	Credit Risk Management
28	Operational Risk Management
29	Managing Financial Risk and Its Interaction with Enterprise Risk Management

Exhibit 1.1 (*continued*)

Chapter	Title
30	Climate Change Risk
31	Cybersecurity: Risks and Governance
32	Foreign Exchange Risk Management
33	Risk Management and Outsourcing
34	Leveraging ERM for Growth
35	Commercial and D&O Insurance for Large Corporations
36	Managing Risk Associated with Project Delivery: A How-To Guide
Part V: Special Topics and Case Studies	
37	The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One
38	Enterprise Risk Management in the Public Sector: A First Look at the U.S. Department of Commerce
39	A Review of Academic Research on Enterprise Risk Management
40	Lessons from the Academy: ERM Implementation in the University Setting
41	Enterprise Risk Management: Lessons from the Field
42	Financial Reporting and Disclosure Risk Management
43	Directors and Risk: Whither the Best Practices: Evidence from Canada

chapters discuss the application of ERM to specific risks, such as foreign exchange risk, climate change, outsourcing, cybersecurity, and major projects. Others explore the relationship between ERM and other key business practices, such as corporate governance, strategic planning, scenario planning, insurance management, and business innovation. Several of the new or rewritten chapters go into depth on specific aspects of ERM, such as defining risk appetite and tolerance, managing cognitive bias, and risk-based decision making. We believe that the new content will greatly increase the value of this book, both as a reference and as an instructional resource.

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, educators, 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 and chapters as shown in Exhibit 1.1.

- Overview and Drivers of Enterprise Risk Management
- Enterprise Risk Management, Culture, and Control
- Enterprise Risk Management Tools and Techniques
- Types of Risks
- Special Topics and Case Studies

A brief description of the author(s) and the chapters is provided below. The author(s) bios are also included at the end of each chapter.

Overview and Drivers of Enterprise Risk Management

In Chapter 2, "A Brief History of Risk Management," Felix Kloman—retired risk management consultant, conceptual thinker, and lover of sailing—provides the background and history of risk management and the evolution of ERM from historical times up to 2008 (and for this second edition, John Fraser updates the narrative to 2019). 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. 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, spanning the millennia of human history and concluding 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 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.

Paul C. Godfrey (William and Roceil Low Professor of Business Strategy, Marriott School of Business, Brigham Young University), Kristina Narvaez (Director, Supply Chain Risk, Intermountain Health Care), Manny Lauria (Chief Executive Officer, KB Risk Solutions, LLC), and John Bugalla (ERM Insights) contributed Chapter 3, "Strategic Risk Management: The Third Paradigm." In it, they focus on the relationship between uncertainty and the strategic imperative to expand competitive advantage. They describe the need for modern "third paradigm" risk management practices to navigate a volatile, uncertain, complex, and ambiguous (VUCA) world. The authors explain that to successfully implement strategic risk management, executive leaders need to truly understand the foundations of strategy and strategic risk, and create organizational structures and cultures supportive of principles, processes, teams, and tools for managing strategic risks. By doing so, organizations will have a powerful tool to manage a VUCA future.

In Chapter 4, "The Role of the Board of Directors and Senior Management in Enterprise Risk Management," Bruce Branson (Professor of Accounting and Associate Director of the Enterprise Risk Management Initiative, North Carolina State College of Management) explains that the oversight of ERM 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 does lead to catastrophic results. Bruce explains the shared responsibility between the members of the board and the senior management team to nurture a risk-aware culture and embrace 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.

Chapter 5, "How to Teach Enterprise Risk Management: A Learner-Centered *Activities* Approach," was written by David R. Lange (Adjunct Teaching Fellow, Trinity College, Dublin, and Emeritus Professor of Finance, Auburn University Montgomery) and Betty J. Simkins (Williams Companies Chair of Business, Regents Professor of Finance, Department Head of Finance, Oklahoma State University, and co-editor of this book). In it, the authors describe ways to teach ERM following a modern, learner-centered activities (LCA) approach. LCA emphasizes a holistic, discovery-based approach to learning to promote critical thinking and analysis. The chapter includes an appendix of LCAs that can be used to teach the contents of other chapters in this book. We are confident that this chapter will be an invaluable guide for ERM instructors and academics.

In Chapter 6, "The Role of the Board in Risk Management Oversight," John Fraser (Former Senior Vice President, Internal Audit and Chief Risk Officer, Hydro One Networks Inc., and co-editor of this book) explains the role of the board of directors in overseeing risk management. He provides the context of why this is important, and in many cases why risk oversight is now a governance requirement. John explains the challenges faced by boards of directors, as well as the various methodologies that boards may employ for approaching risk management. He provides concise approaches to assist boards in their oversight role. There are several ways that boards may organize to address ERM, often by using the audit committee, the full board, or increasingly by establishing a separate risk committee. This chapter compares these alternatives. Overall, this chapter provides a valuable resource to board members, management, assurance providers, and academics, who oversee, report on, provide independent assurance, or study this topic respectively. This chapter was previously published by Wiley in *The Handbook of Corporate Governance* in 2016.

Enterprise Risk Management, Culture, and Control

In Chapter 7, "ERM Frameworks," Frank Martens (Principal, Pacific Rim Risk Management Services Ltd) and Carmen Rossiter (Program Director, Centre in Governance, Risk Management and Control, Schulich Executive Education Centre, York University) explain why a framework is essential to the successful implementation of ERM. There are many frameworks available but the two most widely used are ISO 31000:2018, *Risk management—Guidelines,* and the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s *Enterprise Risk Management—Integrating with Strategy and Performance*. These frameworks provide useful guidance, and Frank and Carmen recommend using the best of both. Nevertheless, while generally accepted frameworks are a useful starting point, they are generic by their nature. As the chapter points out, the most successful organizations tailor their own framework to recognize their own unique culture and operating needs.

Chapter 8, "Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer," by Anette Mikes, is reprinted from our first edition. At the time of the writing, she was the Assistant Professor of Business Administration at Harvard Business School. She is now Associate Professor of Accounting, University of

Oxford. In this chapter, Anette provides insights into the types of roles that chief risk officers (CROs) play. Anette gained her PhD in ERM from the London School of Economics, and set up a program at Harvard Business School with Robert Kaplan to teach ERM. By drawing from the existing practitioner and academic literatures, including case studies and her own research, Anette describes the role of CROs and different types of ERM methodologies that she sees in practice. Anette describes the origins and rise of the CRO, and outlines four major roles that senior risk officers may fulfill. She demonstrates how CROs 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. This chapter will be of great interest to all CROs and those organizations thinking about how to implement ERM.

Risk culture, which refers to the way that the people in organizations view risk and risk management collectively or as individuals, has become an increasingly hot topic. Numerous failures of risk management in recent years have pointed to a lack of a culture that values and practices sound risk management. In Chapter 9, "Creating a Risk-Aware Culture," Brian Philbin, Wendy Saschenbreker-Tang, Heba Awad, and Golam Khan, all with the Canada Revenue Agency, describe their organization's culture and what is being done to promote a healthy risk culture. Their organization is considered a leader in the Canadian Federal Public Service for their progress with implementing ERM. The authors point out the necessity of having the right tools and risk information to help ensure that employees believe in the benefits of good risk management and are able to contribute to its success.

In Chapter 10, "Key Risk Indicators," Dmitriy Borovik, Matt Solomon, and Chris Kozler of Deloitte note that to adapt to changing times, an organization's risk management functions should be designed to integrate key risk indicators (KRIs) for risk management, risk mitigation, decision making, and strategic planning. Risk indicators, when designed correctly, are key for building organizational longevity. KRIs are metrics that can be used to help detect changes in an organization's risks. In this chapter, the authors provide examples of KRIs, and delve into the step-by-step process for developing them. Effective design and use of KRIs can provide forward-looking views on risk trends that can act as early warning signals in respect to a risk materializing. KRIs can also help indicate the present and future state of risk drivers and/or the effectiveness of risk mitigating strategies and controls.

Chapter 11, "Decision Risk Management," concerns the relationship between ERM and decision making. Hans Læssøe has 35 years of industry experience with the LEGO Group, covering a range of positions. Starting in 2007, he established the LEGO Group's strategic risk management function, which, over the years, was expanded to cover strategic scenario planning, project risk, and opportunity management, as well as ERM. In 2017, Mr. Læssøe founded AKTUS, a Danish consulting firm. In this chapter, he points out that the need for risk management to be used in decision making is laid out clearly in the COSO standard, and even more strongly in the ISO 31000 standard, where this is repeated, on average, more than once per page. Yet neither the standards nor most textbooks on risk management provide tangible guidance on *how* to do this. This chapter is aimed to remedy at least some of this void in the risk management literature, and is focused on providing practical guidance, process, and tools for how to implement effective decision risk management.

Thomas H. Stanton is a former president of the Association for Federal Enterprise Risk Management (AFERM), a former member of the federal Senior Executive Service, and among, many other things, teaches at the Center for Advanced Governmental Studies at Johns Hopkins University. With his experience in both federal government and ERM theory and practice, in Chapter 12, "Increasing Adoption of Enterprise Risk Management in the U.S. Federal Government," he charts the history of ERM in the U.S. federal government and compares the challenges of implementing ERM in the government with those of a private company. He also recommends some of the steps that should be taken to further spread ERM within the government. Mr. Stanton has published several books on risk management, including: *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis* (2014) and *Managing Risk and Performance: A Guide for Government Decision Makers* (Wiley, 2016).

In Chapter 13, "Toolmaking in Risk Management: The Case of Core Values and the Formalization of 'Risk Appetite,'" Anette Mikes (Associate Professor of Accounting, University of Oxford) notes the current confusion about how to measure and monitor risk appetite —let alone act upon it—despite a sizable consulting industry that has grown up around the concept. Based on her study of the emergence and formalization of a new risk-management tool—the "risk appetite radar" (RAR)—in two Canadian high-reliability organizations, she describes two risk managers' journeys toward operationalizing and formalizing risk appetite and making multiple values at risk count in decision making. The two cases of risk-appetite object formation and stabilization suggest alternative ways to cast core values as management objects: one assumes the fixation of corporate values, while the other allows for the dynamic, collaborative nature of value prioritization in corporate life.

In Chapter 14, "Incorporating Risk Acumen and Enterprise Risk Management into Innovation Approaches," Dr. Paul L. Walker (James J. Schiro and Zurich Chair of Enterprise Risk Management, Executive Director, Center for Excellence in Enterprise Risk Management, St. John's University, Tobin College of Business) notes that companies need to start considering risk as part of the innovation process. Innovation is really a risk management response to strategic irrelevance risk (or bankruptcy) so risk and innovation are a natural fit. He points out that some risks seen in the ERM process can even be used to identify new innovation possibilities when fully understood via strategic disruption or opportunity workshops. Risk management can be part of the brainstorming (about business models, products, platforms, etc.) once innovation is under way. Also, he explains why risks should be analyzed in portfolios, as few companies today rely on just one product or idea and even those channels can expire. A portfolio of current products and revenue offerings and a portfolio of things in the innovation pipeline are valuable ways to manage the larger set of risks and opportunities facing the company.

Chapter 15, "Scenario Planning as an Enrichment of Enterprise Risk Management," is written by Henk Krijnen, who is Distinguished Lecturer for the Society of Petroleum Engineers on scenario planning and the founder of NavIncerta, providing training and consultancy in the areas of decision and risk analysis and scenario planning. He worked at Shell for 35 years, and during his last five years in Shell's corporate strategy department he played a pivotal role in establishing new approaches for risk and scenario analysis within the company.

This chapter describes the opportunities for scenario planning to strengthen ERM. He explains how the activity of establishing what is uncertain and what is not, and the assessment of possible outcomes of the uncertain political, economic, regulatory, technological, societal, and other developments and how these are all related, provides the key benefit of a scenario planning exercise: a much better understanding of the contextual environment.

Chapter 16, "Unconscious Bias and Risk Management," is written by Toby Groves, PhD, a researcher and speaker on social cognitive psychology. In this chapter, Toby describes decision making in the risk management realm as "far from black and white," and points out that the subjectivity that is a part of risk management makes it vulnerable to bias. Toby describes a range of relevant conscious and unconscious biases that may affect decision makers at all levels of an organization. The chapter describes the causes and effects of evidentiary and decision-making biases that the risk manager or ERM practitioner might encounter, and their implications for ERM.

In Chapter 17, "Cognitive Bias: A Practical Approach," Rob Quail (Principal, Robert Quail Consulting, and former Director–Enterprise Risk, and Vice President–Customer Service at Hydro One Networks Inc.) provides the companion piece for Chapter 16. In it, Rob describes the broad implications of cognitive bias for an effective ERM program, and discusses at some length the strategies that can be employed by the risk manager to help reduce the impact of cognitive bias. These include techniques to slow down and formalize thinking, inject broad, unweighted factual information and expert perspectives into risk assessments, make prudent use of probability estimates, and structure risk discussions to manage the impact of social bias on risk assessments.

Enterprise Risk Tools and Techniques

In Chapter 18, "Risk Appetite and Tolerance in Competitive Strategy," James Darroch (CIT Chair in Financial Services, Schulich School of Business, York University) and David Finnie (Founder and President, Marshall, Griffith & Woods Ltd.) explain that the articulation of the corporation's ability and willingness to take risk is captured in its risk appetite and risk tolerance documentation. They discuss definitions to ensure that what is meant by risk appetite and risk tolerance is clear and they put these terms in the context of the remainder of the chapter. The authors outline the concepts of risk capacity and/or capability, which are key considerations in what determines an organization's ability to take risk. They conclude the chapter with a description of the key elements in the articulation of the risk appetite and tolerance. This includes the necessary links to strategy and authorities as well as the statement of risk limits and related requirements.

In Chapter 19, "How to Plan and Run a Risk Management Workshop," Rob Quail provides practical advice on how to design and run a risk workshop. There is little 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 that each workshop has to be designed carefully depending on the circumstances and desired outcomes. Rob has also added two appendices specifically addressing aspects of ERM that are now becoming more critical. Appendix 19.A explains how to run a workshop virtually when the participants cannot be in the same room and Appendix 19.B covers how to design and run workshops to address the high-impact but low-probability risks known as black swans.

In Chapter 20, "How to Prepare a Risk Profile," John Fraser and Rob Quail provide practical advice on how to prepare a risk profile for executive management and the board of directors. John and Rob wanted to have a chapter on risk profiles, and while there is a lot written about risk maps, heat maps, and risk identification, they could not find anything specific about how to actually conduct structured interviews and prepare a risk profile. As a result, they decided to document the Hydro One model that has been used since 1999, 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 and environmental scans. Ideally the results of workshops and interviews (or surveys) are to be consolidated and reconciled. It is their hope that these step-by-step instructions will give confidence to risk managers implementing ERM on how best to conduct these interviews effectively.

In Chapter 21, "How to Allocate Resources Based on Risk," Joe Toneguzzo (former 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 the implementation of ERM began at Hydro One, Joe, who was responsible for obtaining funding and allocating resources for asset management, collaborated with the risk management group to develop a leading-edge, risk-based resource allocation technique. 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 prioritized 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.

John Hargreaves (Managing Director, Hargreaves Risk & Strategy, London, England) explores and provides guidance on the popular topic of quantifying risks in Chapter 22, "Quantitative Risk Assessment in ERM." John 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. For 17 years he ran a course on Strategic Management for an MSc program at the London School of Economics. In this chapter, 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. Of special interest is his introduction to the topic of Monte Carlo simulation techniques.

In Chapter 23, "Risk Appetite," Rob Quail explains how few concepts from ERM have stimulated more discussion, debate, and confusion than risk appetite. This chapter provides a practical method for developing a meaningful expression of risk appetite that aligns with the strategic ambitions of an organization. Further, it provides an approach for assessing the appetite for risk that is exhibited day to day by decision makers throughout the organization. This can be used as a diagnostic tool to improve organizational alignment with regard to risk and performance. Risk appetite brings greater color and context to the role of risk taking in creating value, and provides a means for board concurrence on the desired risk appetite for the organization. Finally, because it uses a consistent scale for measuring risk appetite, it can be used to monitor changes in risk appetite over time, which can be useful in making adjustments and improvements to other aspects of an ERM program, such as risk tolerances and KRIs.

In Chapter 24, "Organizational Decision Making," Mohamed Ismail (Senior Project Manager, Toronto Transit Commission) builds on Rob Quail's Chapter 23 on risk appetite and provides a model with great examples of how to construct a structured approach to support objective decision making related to risks and resource allocation in times of shifting values. This structured approach applies the principles of ERM and integrates the risk appetite into the decision making. The process and model described in this chapter provides a valuable tool to the decision makers that provides them at a glance with an objective, qualified, ranked list of initiatives that takes into account the benefits (or the potential negative impacts) to the organization based on what the organization values most as expressed in the risk appetite. Therefore, it translates the ERM and the risk appetite into a practical and objective tool to inform the decision making.

In Chapter 25, "The Challenges of and Solutions for Implementing Enterprise Risk Management," John Fraser and Betty Simkins use Hydro One's enterprise risk management practices from 2000 to 2013 as a case study. This chapter draws on the company's experiences in achieving ERM maturity, and illustrates the process using various aspects of ISO 31000. This chapter explores the struggles organizations face in implementing ERM and offers some solutions. The authors then provide highlights of proven solutions and suggestions, referencing additional guidance materials to assist implementers of ERM.

Types of Risk

In Chapter 26, "Market Risk Management and Common Elements with Credit Risk Management," Rick Nason (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. Rick points out that market risk management requires an understanding not only of the tools and techniques, but also of the underlying business, in order to successfully implement the market risk function within the ERM framework of an 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 27, "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.

In Chapter 28, "Operational Risk Management," 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. Diana has taught risk management since 1992 and has a background in decision science. 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 ERM? 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.

Daniel A. Rogers (Associate Professor of Finance, School of Business Administration, Portland State University) provides in Chapter 29, "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. 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 affect company performance.

In Chapter 30, "Climate Change Risk," John Fraser, Rob Quail, and Betty Simkins seek to explain what are considered to be some of the major causes and implications of climate change, some of the possible global solutions, and how

risk managers should be involved. Climate change presents unique challenges to risk managers: the scope of its potential impact on many industries is broad; there are layers of uncertainty concerning its impact on many facets of the strategic environment; and its impacts stretch out many years into the future, well beyond the typical scope of strategic planning and conventional enterprise risk assessments. The authors discuss some of these challenges and the implications for risk managers.

Cybersecurity has become a very hot topic and a major focus for senior management and boards due to the sensational incidents that have been perpetrated. In Chapter 31, "Cybersecurity: Risks and Governance," two experienced cybersecurity experts, Andrew Krupowicz and Phil Young, describe the types of cybersecurity debacles that have happened and can happen to major organizations and individuals. The authors fill their chapter with interesting examples of the types of problems that have occurred and explain why these were allowed to happen. The causes, as they point out, can be both of a highly technical nature as well as due to simple human manipulation and error. Most importantly, they explain how to protect computer systems and cyber assets from hackers, and lay out the various role of key personnel in any large organization, including the chief information security officer, the chief information officer, the security department, and internal audit.

In Chapter 32, "Foreign Exchange Risk Management," Lars Oxelheim (Professor of International Business and Finance at the School of Business and Law, University of Agder, Norway, and Professor Emeritus at Lund University, Sweden), Alf Alviniussen (Former Senior Vice President in Corporate Finance, Norsk Hydro ASA, Oslo), and Håkan Jankensgård (Associate Professor in Corporate Finance, Lund University) note that one of the main ambitions of ERM is to reduce the impact of silos on risk management decisions. In the context of foreign exchange risk management (FXRM), there is a clear potential for silo effects because many business units prefer to manage their own FX risk; doing so allows them to protect their operating margins and performance targets according to their own preferences. Recognizing that this can lead to poor coordination, and a suboptimal outcome for the firm as a whole, many firms centralize FXRM. The authors recommend and discuss the benefits of centralization and integration of exposure management as an integral part of an enterprise-wide risk management.

In Chapter 33, "Risk Management and Outsourcing," Rob Quail explains that outsourcing of business processes is a common activity in public and private sectors. The dependence on another party to deliver business processes traditionally done by the enterprise carries a variety of unique risks. Fortunately, there exists a range of approaches to manage these risks and provide reasonable assurance that the objectives of the outsourcing will be achieved. This chapter explores the reasons why organizations choose to outsource, some of the risk management implications of this activity, and common approaches applied by the organizations to treat these risks.

In Chapter 34, "Leveraging ERM for Growth," Diana Del Bel Belluz describes the role that ERM can play in helping organizations grow and build value. She describes the relationship between ERM and the stages of what she terms the "growth cycles": strategic visioning, transitioning, and ongoing business. She goes

on to describe potential ways that ERM can be integrated into strategic planning, scenario planning, investment analysis, decision analysis and decision quality, and other essential aspects of the strategic visioning stage. She further describes ways that ERM can strengthen ongoing business operations by revisioning the role of risk management, clearly describing the organization's risk appetite, supporting leaders in their risk management roles, and debiasing and improving risk-based decision making.

Risk management started out as the term used by many organizations to describe their insurance-buying activities. While ERM has evolved to include much more than insurance, insurance remains a critical mitigant for any organization. In Chapter 35, "Commercial and D&O Insurance for Large Corporations," Stephen J. Mallory (President, CEO, and founder of Directors Global Risk Consulting Inc.) covers both commercial and directors' and officers' insurance. This is an ideal reference source for risk managers, senior management, and boards as it not only explains the risk-related issues but provides a valuable checklist to use as a tool in any organization. Steve has a wealth of experience not only in insurance, but also in ERM, and has board of director experience where he was the chair of a risk committee. This chapter was previously published in *The Handbook of Board Governance* (Wiley, 2016).

In Chapter 36, "Managing Risk Associated with Project Delivery: A How-To Guide," Mike Winters, EVP and Chief Information Officer, Modern Niagara Group Inc., notes that even in large and complex projects, risk management often does not receive sufficient focus as part of project management—that is, until the risks materialize as issues. Potential risks identified by risk analysis in early stages are typically filed away and not actively checked and monitored. In later phases of the project, when potential risks emerge, mitigation and remediation strategies are used to counter these risks, but their impact on the project as a whole is often not comprehensively considered. The guidance that follows is anchored in theory, leading practices, and the author's own battle scars. It has been written through the lens of a project sponsor, by someone who has held progressive roles of systems developer, solution architect, project manager, project director, and then executive project sponsor. No matter whether you are at the beginning or fairly advanced through your project management career journey, this information is highly valuable.

Special Topics and Case Studies

In Chapter 37, "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 Fraser, and Betty Simkins describe the successful implementation of ERM at Hydro One Networks Inc. over a five-year period. 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. The company 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). This chapter was first published in the *Journal of Applied Corporate Finance*.

Chapter 38 is entitled "Enterprise Risk Management in the Public Sector: A First Look at the U.S. Department of Commerce." In it, Karen Hardy (Former Deputy Chief Risk Officer and Director of Risk Management at the U.S. Department of Commerce) describes the journey of implementing ERM at an executive-level government agency. In this chapter, she gives context on the mission and role of the Department of Commerce and its constituent bureaus. She then describes the implementation approach of the department in introducing ERM, and the challenges faced, given the breadth, complexity, and diversity of the roles of the various bureaus. She describes the adoption of SMART (specific, measurable, attainable, relevant, and time-based) goals for implementation as crucial for the rollout's success. The chapter touches on aspects of leadership buy-in, culture, maturity, governance, and clarity of the role as key aspects of the successful implementation of ERM in this highly complex government organization. This chapter provides valuable lessons learned for ERM implementation in multifaceted organizations.

In Chapter 39, "A Review of Academic Research on Enterprise Risk Management," Donald Pagach (Professor of Accounting, NC State University) and Heather Pascanik (Consultant at Guidehouse) examine the progression of ERM academic and case research since 2005. Their review covers four specific areas. First, they review academic papers focused on identifying firms adopting ERM processes. Second, they review research that examined firm characteristics associated with the implementation of ERM. Next, they review one of the more difficult areas of ERM research, which is determining if ERM creates value for organizations. Finally, they review academic business cases addressing ERM.

In Chapter 40, "Lessons from the Academy: ERM Implementation in the University Setting," Anne E. Lundquist (Assistant Vice President for Campus Strategy at Anthology Inc.) explores the unique aspects of the University of Washington's risk environment, including how leadership, goal setting, planning, and decision making differ from those in the for-profit sector. The lack of risk management regulatory requirements, combined with cultural and environmental differences, help explain why there are a limited number of fully evolved ERM programs at colleges and universities. The second half of the chapter explores the decision to adopt and implement ERM at the University of Washington (UW), including a description of their early decisions, a timeline of how the program evolved, a discussion of their ERM framework, and examples of some of the tools used in their risk management process. It traces the evolution of the UW program as well as demonstrating the decisions that administrators made to tailor ERM to fit the "decentralized" culture of a university.

In Chapter 41, "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 (the late Kathryn and Richard Kip Professor of Accounting, University of North Florida), and Paul L. Walker (James J. Schiro and Zurich Chair of Enterprise Risk Management Executive Director, Center for Excellence in Enterprise Risk Management St. John's University, Tobin College of Business). The authors of this chapter have been involved in the area of ERM since 1996. 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 ERM is like in real life.

"Financial Reporting and Disclosure Risk Management" is discussed extensively by Susan Hume (Associate Professor of Finance and International Business, School of Business, the College of New Jersey) in Chapter 42. The author boils down the key requirements of the extensive regulations for financial reporting and disclosure into an easy-to-understand chapter. Susan discusses key topics such as reporting on internal controls under Sarbanes-Oxley, accounting for derivatives, and fair value accounting. Susan explains how ERM reporting and disclosure provides the forum to discuss the key vulnerabilities and risks of the firm and thereby strengthens management accountability. The board and senior management must 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 to add helpful insights for the more experienced reader.

In Chapter 43, "Directors and Risk: Whither the Best Practices—Evidence from Canada," Dr. David W. Kunsch (Associate Professor, St. John Fisher College) and Dr. Chris Bart (Founder, The Directors College of Canada, and Executive Chairman, Caribbean Governance Training Institute) describe the results and conclusions from a survey of 63 Canadian board directors concerning their risk management oversight practices. In this chapter, the authors conclude that when directors sit on a board that has adopted a formal risk oversight framework, there is evidence of better risk management practices, and that not adopting such a framework appears associated with poorer risk management practices.

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?
- How are universities continuing to evolve approaches for teaching ERM?
- What unresolved issues do we see?

These issues all merit study and more attention than they have received to date. An entire 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 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.

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 gold mine 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 ERM that provides practical information. This publication covered the establishment and implementation of the ERM process. It has since been superseded by AS/NZS ISO 31000:2009, *Risk Management—Principles and Guidelines* and then by AS ISO 31000:2018.
2. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (September 1992 for internal control, and September 2004 and 2017 for enterprise risk management).
3. Group of Thirty, "Derivatives: Practices and Principles" (Washington, DC: Global Derivatives Study Group, July 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 (The Toronto Report)," (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; Conference Board, "Emerging Governance Practices in Enterprise Risk Management" Conference Board Research Report No. R-1398-07-WG (February 15, 2007); and *NYSE: Corporate Governance Guide*, 2014, https://www.nyse.com/publicdocs/nyse/listing/NYSE_Corporate_Governance_Guide.pdf.
8. Risk management in general has been shown to increase firm value. See Charles W. Smithson and Betty J. Simkins, "Does Risk Management Add Value? A Survey of the Evidence," *Journal of Applied Corporate Finance* 17, no. 3 (2005): 8–17.

ABOUT THE EDITORS

John R.S. Fraser, FCPA, FCA, is the former Senior Vice President, Internal Audit & Chief Risk Officer of Hydro One Networks Inc., one of Canada's largest electricity transmission and distribution companies. He is a Fellow of the Ontario Institute of Chartered Professional Accountants and a Certified Internal Auditor. He has more

than 30 years' experience in the governance, risk, and control fields, including areas such as: finance, fraud, derivatives, safety, environmental, computers, and operations. He is past Chair of the Advisory Committee of the Conference Board of Canada's Strategic Risk Council, an ex-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 Professional Accountants. He is a recognized authority on enterprise risk management and has co-authored numerous academic papers on the subject. He is also co-editor of *Implementing Enterprise Risk Management: Case Studies and Best Practices*, published by Wiley in 2015.

Rob Quail, BASc (Industrial Engineering, University of Toronto) was part of the team that established the enterprise risk management processes, tools, and methodologies at Hydro One Networks Inc. that are widely regarded as best practice. He has successfully applied ERM methodologies to a broad range of business problems and challenges, including acquisitions, outsourcing, downsizing, large-scale IT projects, labor disruption, regulatory compliance management, major construction project management, strategic planning, and capital investment.

Rob has lectured on ERM techniques at the York University Schulich School of Business since 2010. In addition to his ERM roles, Rob has held key executive leadership roles in the areas of business technology, outsourcing, and customer service. Today, Rob provides independent consulting services in enterprise risk management, business process and technology outsourcing, and customer care to clients in a variety of industry sectors, including energy, health care, technology, financial services, and government agencies.

Betty J. Simkins, PhD, is the Department Head of Finance, Regents Professor of Finance, and Williams Companies Chair of Business in the Spears School of Business at Oklahoma State University. Betty received her PhD from Case Western Reserve University. She has more than 60 publications in academic finance journals. She has won awards for her teaching, research, and outreach, including the top awards at OSU: Regents Distinguished Research Award, Regents Distinguished Research Award, and Outreach Excellence Award. Her primary areas of research are risk management, energy finance, and corporate governance. Betty currently serves on the Commodity Futures Trading Commission Market Risk Advisory Committee and she is co-editor of the *Journal of Commodity Markets*. She also serves on the editorial boards of 12 other academic journals, is Vice President of Financial Education for the Financial Management Association International, and is past president of the Eastern Finance Association, among other leadership positions. In addition to the first edition of this book, she has published two other Wiley books: *Energy Finance and Economics: Analysis and Valuation, Risk Management and the Future of Energy* and *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Prior to entering academia, she worked in the corporate world for ConocoPhillips and Williams Companies. She conducts executive education courses for companies globally.