

ENTERPRISE RISK MANAGEMENT

Today's Leading Research and Best
Practices for Tomorrow's Executives

Second Edition



John R.S. Fraser, Rob Quail, and Betty Simkins

*Foreword by Robert S. Kaplan, Senior Fellow
and Marvin Bower Professor of Leadership
Development, Harvard Business School*

Praise for *Enterprise Risk Management*

“The 2010 version of this book was a masterpiece on the topic of risk management; the first of its kind to brilliantly cover the risk management landscape and summarize it in a highly readable, understandable and enlightening format style. This latest version represents how the authors have taken their masterpiece and turned it into an even better one. The management of enterprise risk is one of the most vexatious problems confronting boards and executives worldwide. Accordingly, this ‘update’ by Fraser, Quail, and Simkins represents the ultimate ‘how to’ book written with the ‘risk management problem solver’ in mind. As with the first edition, it continues to provide the essential link that has been missing for effectively teaching ERM at the university and executive education levels and it is an exceptional achievement by true risk management gurus.”

—Dr. Chris Bart, FCPA, founder and Lead Faculty, The Directors College of Canada; Executive Chairman, Caribbean Governance Training Institute

“The comprehensive application of risk management principles and practice is a necessary aspect of the business management of any organization, whether public, private, or not-for-profit. This book, edited by Fraser, Quail, and Simkins, provides a thorough review of the aspects of risk management from cultural to quantitative, as well as from the practical to the theoretical. Just as risk management cannot sit still, this edition reflects developments in risk theory and understanding that must be reflected in an organization’s overall management of risk.”

—Doug Brooks, retired CEO and Vice-Chair, ivari (formerly Transamerica Life Insurance Company of Canada)

“Consider an amalgam of risk disciplines that, aggregated correctly, shines spotlights on pitfalls and points out attainable opportunities. Financial regulators call this tonic of survival enterprise risk management (ERM). The effectiveness of ERM programs meaningfully predicted how well financial institutions weathered the Great Recession. Of course, ERM applies to nonfinancial organizations as well. ERM is measurement, monitoring, and escalation. It is culture, governance, and strategy. ERM is for poets and for gearheads and needs both to be effective. Perhaps above all, ERM is dynamic. An effective ERM framework for a given company at a given time might not be effective for another company or even that same company at another time. How does one confine ERM to a single volume? Identify and flesh out the components; recognize what has changed in the past 10 years; compile a meaningful, relevant set of chapters from which users can glean what they seek; and open up the collection with a succinct introduction that pulls the components together and guides the reader on how to use the book. Messrs Fraser, Quail, and Dr. Simkins have done just that in *Enterprise Risk Management: Today’s Leading Research and Best Practices for Tomorrow’s Executives*, Second Edition. With almost a complete overhaul of the work they did in their first edition, Messrs. Fraser, Quail, and Dr. Simkins hit the latest hot ERM topics. They added a timely discussion of cybersecurity risks and guidance for managing it. Further, this edition adds chapters on the burgeoning ESG topic though environmental issues like climate change and societal concepts like bias to supplement no less than three repeated and amended chapters on governance matters. This volume will be a valuable resource for me and my ERM team at BOK Financial, and I’m glad they compiled it.”

—Tally Ferguson, CFA, CERP | SVP Director of Enterprise-Wide Risk Management, Bank of Oklahoma, a division of BOKF NA

“The effective management of enterprise risk is essential for boards and executives worldwide. *Enterprise Risk Management: Today’s Leading Research and Best Practices for Tomorrow’s Executives* includes insightful, highly readable, and practical contributions from leading practitioners and academics. I believe that this unique and definitive collection will serve as a valuable reference for executives, risk managers, and students.”

—Laura Formusa, LLB, ICD.D, Corporate Director; former President and CEO, Hydro One Inc.

“Throughout many years of serving risk professionals and executives within our corporate clients, I have seen numerous attempts to design and execute integrated risk management strategies within their businesses and disciplines. A recurring problem has been a lack of common points-of-reference and language to focus stakeholders toward that result. This book is by far the most comprehensive study I have seen, logically layered to enable a summary read or deep treatment of all risk categories, written by both experienced practitioners and top academics. . . . Enthusiastically recommended!”

—Alan Garner, president and CEO (retired), Marsh Canada

“Enterprise Risk Management provides a comprehensive overview of how and why companies ought to approach risk management. For more than 25 years, companies have struggled to understand the value of ERM and, in particular, how sound risk management practices enhance resilience. This book offers insights from leading consultants and academics on the basics of risk management, covering key stakeholders’ roles as well as ‘how to’ frameworks that support effective risk management. Most importantly, practitioners who have developed and refined ERM programs at their companies offer a frank view of what works and what doesn’t. *Enterprise Risk Management* translates ERM foundations and frameworks into effective risk practices and will help every organization that is embarking on or re-booting ERM.”

—Ellen Hexter, principal, Hexter & Co.; Senior Advisor, Enterprise Risk Management, The Conference Board

“Not only has ERM continued to generate more attention in academic literature, I can confirm from my service as the chair of a corporate audit committee that managing risk on an enterprise-wide basis is drawing more and more attention from boards too. Recent surveys suggest that the COVID-19 pandemic has increased the scrutiny and visibility of risk management. However, questions about optimizing and gaining the most benefit from ERM activities remain. In many organizations, how they assess progress, measure maturity, and evaluate success of their risk management programs are key issues. In this environment, the second edition of *Enterprise Risk Management: Today’s Leading Research and Best Practices for Tomorrow’s Executives*, offers insights into what practitioners are doing and what the future holds. With insights from top ERM thought leaders in industry and academe and with added chapters on hot topics such as climate change, cyber security, outsourcing, and risk appetite, this book is a much-needed resource for scholars, practitioners, board members, and educators alike.”

—Rob Hoyt, PhD, Moore Chair and Professor of Risk Management and Insurance, Terry College of Business, University of Georgia; ERM scholar; insurance company Audit Committee Chair

“In the aftermath of the Covid-19 pandemic, all organizations should examine the effectiveness of their ERM program and make necessary improvements. In this second edition, the co-editors—Fraser, Quail, and Simkins—have put together a comprehensive and updated compilation of ERM research and best practices. The blend of academic and industry insights, along with new content on disruptive risks such as cyber security and climate change, provide a useful guide to ERM implementation.”

—James Lam, President, James Lam & Associates; independent director and audit committee chairman, RiskLens, Inc.; author, *Implementing Enterprise Risk Management—From Methods to Applications*

“Simkins and Fraser have already published two successful risk publications, which I hold in high regard, and that have received great feedback from anyone I have spoken to about the books. Their eagerness to update their content is therefore greatly welcomed. It is refreshing and encouraging to see a book that seeks to capture what I believe to be the true essence of risk management the way *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives* does. Specifically, that risk management is not just about surviving, but about thriving in a constant changing world. The book covers a wide variety of topics that range from risk culture to quantitative risk analysis, both of which are hot topics in the field of risk management at the moment, and special attention has been given to emerging risk subjects such as climate change, cyber risk, and outsourcing, ensuring that this is one of the most up-to-date books on the market.

What makes this book so compelling, is that rather than relying on only a couple of authors, Simkins, Fraser, and Quail have invited leading global experts in the field of risk management to contribute. The book is also complemented with real case studies and examples. This, along with their understanding that risk management is not a one size fits all, ensures that this is a book that will add huge value to anyone seeking to learn about ERM or implement it within their organization.”

—Alexander Larsen, BHRM, CFIRM, President, Baldwin Global Risk Services Ltd.

“This set of readings will be an invaluable resource for academic and practitioner alike, and provides a thorough, accessible, but rigorous overview of enterprise risk management.”

—Brian Lucey, Professor of International Finance and Commodities, Trinity Business School, Trinity College Dublin, Ireland

“I highly recommend the work of John Fraser, a successful risk practitioner who has received significant and deserved recognition for his program, and his co-editors Quail and Professor Simkins. This book has contributions from some of the leading thought leaders and practitioners in risk management around the world. They challenge your thinking, even if you are an experienced practitioner yourself. Their insights merit careful consideration and I expect all readers will learn a great deal and be able to apply a number of the suggestions in the book to upgrade their own risk programs.”

—Norman D. Marks, CPA, CRMA, author; speaker; thought leader; OCEG Fellow; Honorary Fellow of the Institute of Risk Management

“This new edition of *Enterprise Risk Management: Today’s Leading Research and Best Practices for Tomorrow’s Executives* could not have come at a better moment when managing risk at the firm and industry levels demands a portfolio management perspective. It crystallizes the holistic approach to risk management, which is even more important in these times of growing emerging enterprise risks including cybersecurity risk, climate change risk, innovation risk, and outsourcing risk. Drawing on their vast experiences, the authors address key ERM dimensions and tools, including risk appetite, scenario planning, and how they relate to strategy execution. *Enterprise Risk Management* is rigorous, clear, and provides a comprehensive resource filled with practical guides on how to identify enterprise-scale risks, prioritize risks, and implement ERM. Highly recommended reading for all risk management professionals, business executives, and students in the field of risk management.”

—Dr. Richard Ottoo, CFA, FRM, Vice President, Global Association of Risk Professionals (GARP)

“*Risk in business.*’ The spectrum of the understanding and interpretation of the concept varies as widely as the extent to which boards consider its management their responsibility. As boards appreciate that risk management, along with strategic planning and executive talent management, is their key responsibility, the need for enhanced understanding and frameworks to manage and monitor an enterprise’s risk becomes critical. This book is intended to provide a practical reference that weaves together the academic and the practical: a timely and valuable resource to any director or executive looking for guidance in managing enterprise-wide risk. In particular, the excellent chapter on board oversight of ERM offers a practical framework and extremely helpful checklists.”

—Lewis Rose, FCPA, FCA, ICD.D, board chair; strategic advisor; investor; former CEO, President, and CFO of private and publicly listed corporations in Canada, the United Kingdom, and the United States

“The Second Edition of *Enterprise Risk Management: Today’s Leading Research and Best Practices for Tomorrow’s Executives* is the most comprehensive review of the history, applications, and implications of ERM in the marketplace. The cross-section of industries and scholars represented is impressive and I highly recommend this book for anyone in the discipline—or in a leadership position.”

—Norean R. Sharpe, PhD, Dean and Joseph H. and Maria C. Schwartz Distinguished Chair, The Peter J. Tobin College of Business, St. John’s University

“This book provides a comprehensive, up-to-date, and insightfully integrated overview of ERM theory and practice. As such, it should be an important resource for ERM instructors, students, researchers, and practitioners for many years to come.”

—Mike Stramaglia, President and founder, Matrisc Advisory Group; Executive-in-Residence, Global Risk Institute; Program Director, Centre of Excellence in Governance, Risk Management and Control, Schulich Executive Education Centre

ENTERPRISE RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT

Today's Leading Research and Best
Practices for Tomorrow's Executives

Second Edition

**John R.S. Fraser
Rob Quail
Betty J. Simkins**

WILEY

Copyright © 2021 by John Wiley & Sons, Inc. All rights reserved.

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

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Names: Fraser, John R. S., 1946- editor. | Quail, Rob, editor. | Simkins, Betty J., 1957- editor.

Title: Enterprise risk management : today's leading research and best practices for tomorrow's executives / [edited by] John R.S. Fraser, Rob Quail, and Betty J. Simkins.

Description: Second edition. | Hoboken, New Jersey : John Wiley & Sons, Inc., [2021] | Includes index.

Identifiers: LCCN 2021013946 (print) | LCCN 2021013947 (ebook) | ISBN 9781119741480 (cloth) | ISBN 9781119741435 (adobe pdf) | ISBN 9781119741459 (epub)

Subjects: LCSH: Risk management.

Classification: LCC HD61 .E5354 2021 (print) | LCC HD61 (ebook) | DDC 658.15/5—dc23

LC record available at <https://lcn.loc.gov/2021013946>

LC ebook record available at <https://lcn.loc.gov/2021013947>

Cover Design: Wiley

Cover Image: © CARACOLLA/iStock/Getty Images

10 9 8 7 6 5 4 3 2 1

Contents

Foreword to the Second Edition	xiii
Foreword to the First Edition	xv
Part I Overview and Drivers of Enterprise Risk Management	1
1 Enterprise Risk Management: An Introduction and Overview	3
<i>John R.S. Fraser, Rob Quail, and Betty J. Simkins</i>	
2 A Brief History of Risk Management	23
<i>H. Felix Kloman and John R.S. Fraser</i>	
3 Strategic Risk Management: The Third Paradigm	37
<i>Paul C. Godfrey, Kristina Narvaez, Emmanuel Lauria, and John Bugalla</i>	
4 The Role of the Board of Directors and Senior Management in Enterprise Risk Management	55
<i>Bruce C. Branson</i>	
5 How to Teach Enterprise Risk Management: A Learner-Centered Activities Approach	75
<i>David R. Lange and Betty J. Simkins</i>	
6 The Role of the Board in Risk Management Oversight	103
<i>John R.S. Fraser</i>	
Part II Enterprise Risk Management, Culture, and Control	131
7 ERM Frameworks	133
<i>Frank Martens and Carmen Rossiter</i>	

8	Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer	151
	<i>Anette Mikes</i>	
9	Creating a Risk-Aware Culture	167
	<i>Brian Philbin, Wendy Saschenbreker-Tang, Heba Awad, and Golam Khan</i>	
10	Key Risk Indicators	193
	<i>Dmitriy Borovik, Matt Solomon, and Chris Kozler</i>	
11	Decision Risk Management	213
	<i>Hans Læssøe</i>	
12	Increasing Adoption of Enterprise Risk Management in the U.S. Federal Government	235
	<i>Thomas H. Stanton</i>	
13	Toolmaking in Risk Management: The Case of Core Values and the Formalization of “Risk Appetite”	255
	<i>Anette Mikes</i>	
14	Incorporating Risk Acumen and Enterprise Risk Management into Innovation Approaches	281
	<i>Paul L. Walker</i>	
15	Scenario Planning as an Enrichment of Enterprise Risk Management	297
	<i>Henk Krijnen</i>	
16	Unconscious Bias and Risk Management	323
	<i>Toby Groves</i>	
17	Cognitive Bias: A Practical Approach	335
	<i>Rob Quail</i>	
	Part III ERM Tools and Techniques	345
18	Risk Appetite and Tolerance in Competitive Strategy	347
	<i>James Darroch and David Finnie</i>	
19	How to Plan and Run a Risk Management Workshop	369
	<i>Rob Quail</i>	

20	How to Prepare a Risk Profile	391
	<i>John R.S. Fraser and Rob Quail</i>	
21	How to Allocate Resources Based on Risk	411
	<i>Joseph P. Toneguzzo</i>	
22	Quantitative Risk Assessment in ERM	441
	<i>John Hargreaves</i>	
23	Risk Appetite	459
	<i>Rob Quail</i>	
24	Organizational Decision Making	473
	<i>Mohamed Ismail</i>	
25	The Challenges of and Solutions for Implementing Enterprise Risk Management	491
	<i>John R.S. Fraser and Betty J. Simkins</i>	
	Part IV Types of Risk	507
26	Market Risk Management and Common Elements with Credit Risk Management	509
	<i>Rick Nason</i>	
27	Credit Risk Management	531
	<i>Rick Nason</i>	
28	Operational Risk Management	549
	<i>Diana Del Bel Belluz</i>	
29	Managing Financial Risk and Its Interaction with Enterprise Risk Management	573
	<i>Daniel A. Rogers</i>	
30	Climate Change Risk	589
	<i>John R.S. Fraser, Rob Quail, and Betty J. Simkins</i>	
31	Cybersecurity: Risks and Governance	603
	<i>Andrew Krupowicz and Phil Young</i>	
32	Foreign Exchange Risk Management	631
	<i>Lars Oxelheim, Alf Alviniussen, and Håkan Jankensgård</i>	

33	Risk Management and Outsourcing	657
	<i>Rob Quail</i>	
34	Leveraging ERM for Growth	671
	<i>Diana Del Bel Belluz</i>	
35	Commercial and D&O Insurance for Large Corporations: Best Practices in Protecting the Assets and Liabilities of Directors and Officers and Their Organizations	691
	<i>Stephen J. Mallory</i>	
36	Managing Risk Associated with Project Delivery: A How-To Guide	717
	<i>Mike Winters</i>	
Part V	Special Topics and Case Studies	737
37	The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One	739
	<i>Tom Aabo, John R.S. Fraser, and Betty J. Simkins</i>	
38	Enterprise Risk Management in the Public Sector: A First Look at the U.S. Department of Commerce	765
	<i>Karen Hardy</i>	
39	A Review of Academic Research on Enterprise Risk Management	785
	<i>Donald Pagach and Heather Pascanik</i>	
40	Lessons from the Academy: ERM Implementation in the University Setting	807
	<i>Anne E. Lundquist</i>	
41	Enterprise Risk Management: Lessons from the Field	841
	<i>William G. Shenkir, Thomas L. Barton, and Paul L. Walker</i>	
42	Financial Reporting and Disclosure Risk Management	865
	<i>Susan Hume</i>	
43	Directors and Risk: Whither the Best Practices—Evidence from Canada	883
	<i>David W. Kunsch and Chris Bart</i>	
	Index	905

Foreword to the Second Edition

Since the 2010 publication of the first edition of Fraser and Simkins, *Enterprise Risk Management*, the world has not become a less risky place. Business now must operate in a volatile, uncertain, complex, and ambiguous (VUCA) environment. John Fraser, Betty Simkins, and Rob Quail have done an invaluable service for all businesses, nonprofits, and government agencies by producing the new and improved second edition of this book. They have updated the excellent collection of case studies in the first edition of innovative risk management practices. Even more important, they have advanced the science of enterprise risk management by adding 30 new chapters. The new content includes the emerging risk areas of cyber, climate, and foreign exchange; new industry applications in government, higher education, and insurance; new frameworks for ethics, decision making, and risk appetite; and new applications for innovation, ERM, outsourcing, project management, and scenario planning. The book's lessons are not presented as deductive, top-down, preachy lectures. Rather, all content is grounded in the real-world practices and experiences of a wonderfully diverse set of innovating organizations from around the globe. The book's extensive and rich set of observations will educate scholars in the field and enable them to share leading-edge frameworks and examples with their students. The book offers an abundance of practical advice for practitioners to improve the enterprise risk management processes and practices in their organizations. I personally feel grateful to the three editors and the many chapter authors for bringing us this expanded body of risk management knowledge. Risk management professionals, and their organizations, should feel similarly.

ROBERT S. KAPLAN
Senior Fellow and Marvin Bower Professor of Leadership Development
Harvard Business School

Foreword to the First Edition

I am pleased to welcome this important collection of authoritative papers on enterprise risk management. This subject has, unfortunately, operated below the visibility screen of most CEOs for many years. In the financial institutions, where regulations require a risk management process, most bank CEOs viewed it as a compliance process, much like internal audit and internal controls. They did not view risk management as a strategic process nor one that demanded much of their time and attention. As a consequence, most businesses have limited ability to assess its risk from rapid growth, increased complexity in financing and securitization, and globalization. Company executives have not been the only ones failing to pay sufficient attention to the topic. Few MBA, accounting, or finance programs departments featured courses and training in enterprise risk management.

The events of 2007–2009 have made the gaps in knowledge, training, and attention to risk management abundantly clear, albeit in a highly costly and tragic manner. Businesses, business schools, regulators, and the public are now scrambling to catch up with the emerging field of enterprise risk management. This subject must become a priority for students to study, executives to practice, and regulators to verify. Fraser and Simkins have produced an impressive contribution to the field, one that I believe will help to educate many. I hope this book, beyond its educational and attention-directing mission, will also stimulate the production of other articles and books so that a common body of knowledge can be developed for this vital profession. We are indebted to John Fraser and Betty Simkins for organizing the impressive author team and the editing of this book.

ROBERT S. KAPLAN
Baker Foundation Professor
Harvard University

To Wendy, my wife, and my family, who are my inspiration, and to my parents who instilled in me a lifelong thirst for learning. Also, to Betty and Rob, with whom it has been a wonderful experience to update this book because of their knowledge, experience and enthusiasm for risk management.

—John Fraser

I'd like to thank my wife Amber for her love, support and encouragement. I'd also like to thank co-editor John Fraser for his support, friendship, and mentorship throughout my career and beyond. Finally, I'd like to thank Carmen Rossiter for lighting this particular fire; encouraging us to put this second edition together.

—Rob Quail

To my husband (Russell) and our family: sons and daughters-in-law (Luke & Stephanie and Walt & Lauren), daughter and fiancé (Susan & Fletcher), our youngest daughter (April), and our grandchildren (Izzy and Russell, and one about to be born who will be named Riordan). I also want to thank co-editor John Fraser who is a guru on enterprise risk management and a thought leader in this area. It is a true honor to work with him!

—Betty Simkins

PART I

Overview and Drivers of Enterprise Risk Management

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

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 <i>Activities</i> 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.