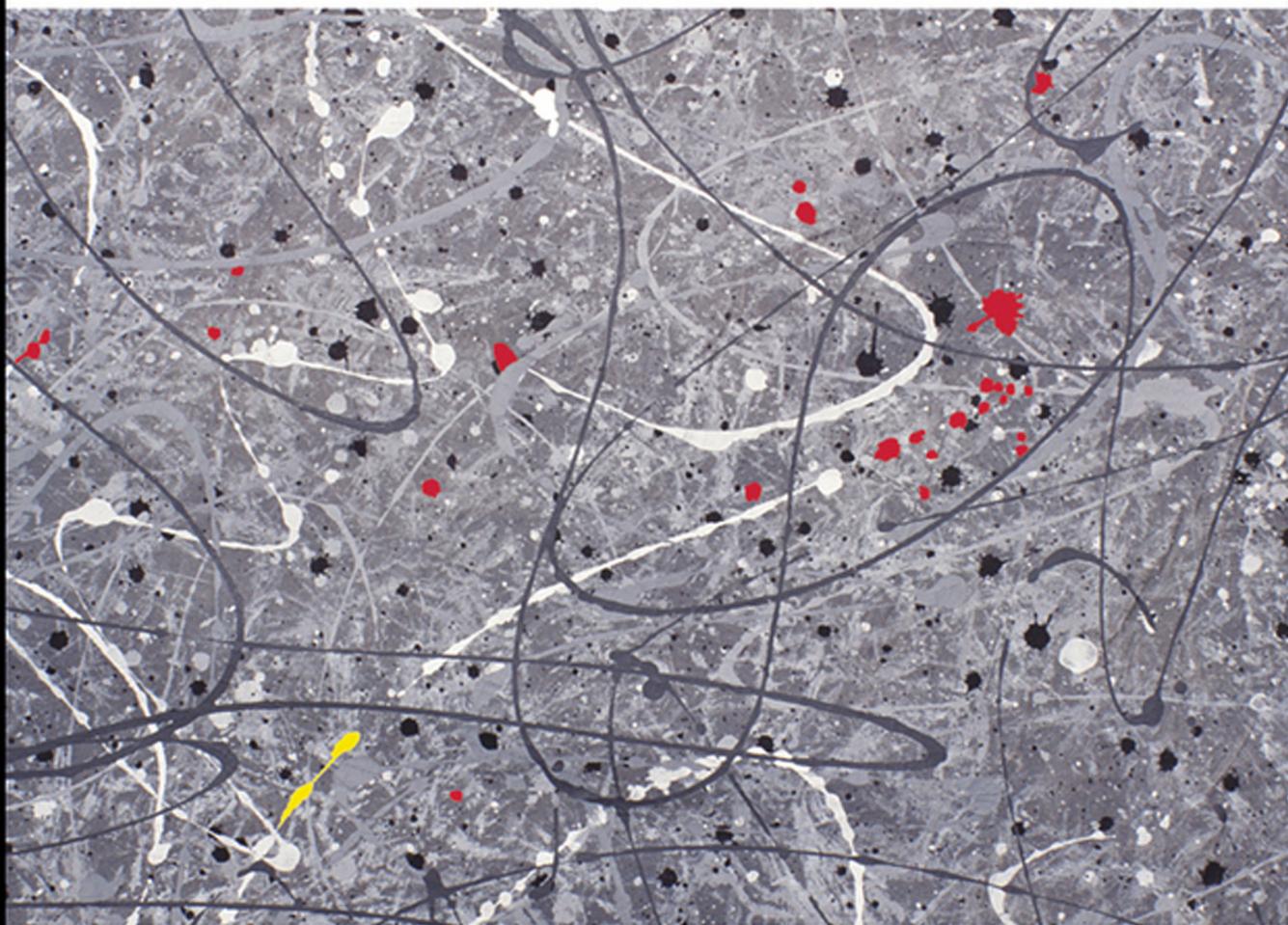


ENTERPRISE RISK MANAGEMENT

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



John Fraser and Betty J. Simkins, Editors

KOLB SERIES IN FINANCE

Essential Perspectives

ENTERPRISE RISK MANAGEMENT

The *Robert W. Kolb Series in Finance* provides a comprehensive view of the field of finance in all of its variety and complexity. The series is projected to include approximately 65 volumes covering all major topics and specializations in finance, ranging from investments, to corporate finance, to financial institutions. Each volume in the *Kolb Series in Finance* consists of new articles especially written for the volume.

Each *Kolb Series* volume is edited by a specialist in a particular area of finance, who develops the volume outline and commissions articles by the world's experts in that particular field of finance. Each volume includes an editor's introduction and approximately thirty articles to fully describe the current state of financial research and practice in a particular area of finance.

The essays in each volume are intended for practicing finance professionals, graduate students, and advanced undergraduate students. The goal of each volume is to encapsulate the current state of knowledge in a particular area of finance so that the reader can quickly achieve a mastery of that special area of finance.

ENTERPRISE RISK MANAGEMENT

John Fraser
Betty J. Simkins

The Robert W. Kolb Series in Finance



WILEY

John Wiley & Sons, Inc.

Copyright © 2010 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/permissions>.

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 books. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Fraser, John, 1946–

Enterprise risk management : today's leading research and best practices for tomorrow's executives / John Fraser, Betty J. Simkins
p. cm. – (The Robert W. Kolb series in finance)

Includes index.

ISBN 978-0-470-49908-5 (cloth)

1. Risk management. I. Simkins, Betty J., 1957– II. Title.

HD61.F74 2010

658.15–dc22

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Foreword by Robert S. Kaplan	xix
PART I Overview	1
1 Enterprise Risk Management: An Introduction and Overview	3
What Is Enterprise Risk Management?	3
Drivers of Enterprise Risk Management	4
Summary of the Book Chapters	5
<i>Overview</i>	5
<i>ERM Management, Culture, and Control</i>	6
<i>ERM Tools and Techniques</i>	8
<i>Types of Risks</i>	10
<i>Survey Evidence and Academic Research</i>	12
<i>Special Topics and Case Studies</i>	13
Future of ERM and Unresolved Issues	15
Notes	16
About the Editors	16
2 A Brief History of Risk Management	19
Introduction	19
Risk Management in Antiquity	19
After the Middle Ages	20
The Past 100 Years	21
Notes	28
About the Author	29
3 ERM and Its Role in Strategic Planning and Strategy Execution	31
Rising Expectations for Strategic Risk Management	32
<i>ERM Positioned as Value-Adding</i>	33
<i>Board Demands for More Strategic Risk Management</i>	34
Integrating Risk into Strategic Planning	34
<i>Recognizing Strategic Business Risk</i>	35
<i>Evaluating Strategic Business Risk</i>	36

<i>11 Tenets of the Return Driven Framework</i>	37
<i>Using a Framework to Build a Strategic Risk Management Mindset</i>	39
Creating a Strategic Risk Mindset and Culture	40
<i>A Strategic Risk Management Mindset</i>	40
<i>Recognizing Value of Strategic Risk Management at High-Performance Companies</i>	42
Building a Strategic Risk Assessment Process	42
<i>Strategic Risk Management Processes</i>	43
<i>Focus on Genuine Assets at Risk</i>	44
<i>Strategic Risk Management and Performance Measurement</i>	45
<i>Critical Steps for Value-Added Strategic Risk Management</i>	47
Conclusion	48
Notes	48
About the Authors	50
4 The Role of the Board of Directors and Senior Management in Enterprise Risk Management	51
Introduction	51
Governance Expectations for Board Oversight of Risk Management	52
Delegation of Risk Oversight to Board Committees	58
Formalizing Risk Management Processes	58
Senior Executive Leadership in Risk Management	60
The Role of the Internal Audit Function in ERM	61
External Audit as an Independent Source of Key Risk Identification	61
ERM Implementation Strategies	62
<i>Role of the Audit Committee</i>	62
<i>Role of the Board</i>	63
<i>Training</i>	64
<i>Board Composition</i>	64
<i>Reporting</i>	65
<i>Compliance</i>	66
<i>Culture</i>	66
Conclusion	66
Notes	67
PART II ERM Management, Culture, and Control	69
5 Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer	71
The Origins of the CRO	72
The CRO as Compliance Champion	75
The CRO as Modeling Expert	76
The CRO as Strategic Controller	77
The CRO as Strategic Advisor	78
Which CRO Role to Play?	79
Conclusion	81
Notes	82

References	82
Acknowledgments	85
About the Author	85
6 Creating a Risk-Aware Culture	87
The Importance of Culture	87
<i>Defining Culture</i>	87
<i>The Goals of Culture</i>	87
<i>The Importance of Culture</i>	88
<i>When the Chips Are Down</i>	88
<i>Culture Can Discourage Good Risk Taking</i>	90
Elements of a Risk-Aware Culture	91
<i>Behavioral Elements</i>	91
<i>Process Elements</i>	91
How to Create a Risk-Aware Culture	91
<i>Defining the Elements</i>	91
<i>Measuring and Monitoring</i>	92
<i>Involvement and Buy-In</i>	93
<i>Openness</i>	93
<i>Tone from the Top</i>	93
<i>Alignment of Incentives and Rewards—Walking the Talk</i>	93
What Does Risk Management Have to Do?	94
Conclusion	95
References	95
About the Author	95
7 ERM Frameworks	97
Introduction	97
<i>Introduction to the ISO Risk Management Framework</i>	97
<i>Principles of Risk Management and Excellence in Risk Management</i>	99
Elements of an ERM Framework	100
<i>ERM Framework: Concept and Elements</i>	100
Risk Management Process (RMP)	102
<i>Risk Management Process: Context</i>	105
<i>Risk Management Process: Risk Assessment</i>	106
<i>Risk Management Process: Risk Treatment</i>	109
<i>Risk Management Process: Monitoring and Review</i>	109
<i>Risk Management Process: Communication and Consultation</i>	109
<i>Risk Management Process: Recording the Risk Management Process</i>	110
Mandate and Commitment to the ERM Framework	110
<i>Rationale for Commitment to ERM</i>	111
<i>Gap Analysis for ERM</i>	111
<i>Context for ERM Framework</i>	112
<i>Design, Decision, and Implementation of the ERM Framework</i>	112
Risk Management Policy	113
<i>Policies for the ERM Framework</i>	113
<i>Policies for Risk Management Decisions</i>	113
<i>Review of Policies</i>	117

Integration of Risk Management and Resources for ERM	118
Communications, Consultation, and Reporting	119
Accountability	120
Continuous Improvement	121
Conclusion	122
References	122
About the Author	123
8 Identifying and Communicating Key Risk Indicators	125
Introduction	125
What Is a Key Risk Indicator?	126
<i>Definition</i>	126
<i>Examples of KRIs</i>	126
<i>Differentiation from Key Performance Indicators</i>	128
Practical Applications	129
<i>Validate Organizational Planning and Monitor Performance</i>	129
<i>Enhance Operational Efficiency and Effectiveness</i>	130
<i>Clarify Risk-Taking Expectations</i>	131
<i>Monitor Risk Exposures</i>	132
<i>Measure Risk</i>	133
Value of KRIs to Risk Management	134
Design Principles	135
<i>Keep the Stakeholders and Objectives in Mind</i>	135
<i>Leverage Management Insight and Existing Metrics</i>	135
<i>Have a Good Basic Understanding of the Risks</i>	135
<i>Limit Indicators to Those That Are Most Representative</i>	136
<i>Ensure Clarity in What Is Being Measured</i>	136
<i>Focus More on Objective Measures</i>	136
<i>Consider the Wider Set of KRIs</i>	136
<i>Consider the Relative Importance of KRIs</i>	136
<i>Monitor for Continual Usefulness</i>	137
<i>Think Longer Term</i>	137
Implementation Considerations	137
<i>Obtaining Buy-In</i>	138
<i>Lack of Resources and Skills</i>	138
<i>Data and Technology Challenges</i>	138
<i>Integration with Business Activities</i>	139
<i>Sustainability of the KRI Framework</i>	139
Conclusion	139
Note	139
Acknowledgment	140
About the Author	140
PART III ERM Tools and Techniques	141
9 How to Create and Use Corporate Risk Tolerance	143
Introduction	143
What Is Risk Tolerance?	144

Why Is Setting Risk Tolerance Important?	144
What Are the Factors to Consider in Setting Risk Tolerance?	145
<i>Attitude About Risk</i>	146
<i>Goals</i>	146
<i>Capability to Manage Risk</i>	147
<i>Capacity to Take Risk</i>	149
<i>Cost/Benefit of Managing Risk</i>	150
How Can Your Organization Make Risk Tolerance Useful in Managing Risk?	150
Conclusion	152
Notes	153
About the Authors	154
10 How to Plan and Run a Risk Management Workshop	155
Introduction	155
What Is a Risk Workshop?	155
Why Use Workshops?	156
How to Conduct a Risk Workshop	156
Preparation	156
<i>Identify the Sponsor</i>	157
<i>Set the Objectives of the Workshop</i>	158
<i>Set the Scope</i>	159
<i>Assemble Reference Materials</i>	160
<i>Set the Agenda</i>	162
<i>Decide on Attendees</i>	164
<i>Arrange Venue</i>	164
Execution	165
<i>Facilitate the Workshop</i>	165
<i>Record the Results</i>	167
<i>Prepare the Final Report</i>	167
Techniques for Planning and Facilitating Effective Risk Workshops	168
<i>"Anonymous" Voting</i>	168
<i>Useful Facilitation Tips</i>	169
<i>Tough Spots</i>	169
Conclusion	170
About the Author	170
11 How to Prepare a Risk Profile	171
Introduction	171
Definition and Uses of a Corporate Risk Profile	171
Common Types of Corporate Risk Profiles	173
<i>The "Top 10" List</i>	173
<i>The Risk Map</i>	173
<i>The Heat Map</i>	174
Advantages and Disadvantages of Information-Gathering Methodologies	176

How to Prepare a “Top 10” Risk Profile—Hydro One’s Experience	176
<i>Step 1: Schedule Interviews and Gather Background Information</i>	177
<i>Step 2: Prepare the Interview Tools</i>	178
<i>Step 3: Summarize the Interview Findings</i>	181
<i>Step 4: Summarize the Risk Ratings and Trends</i>	182
<i>Step 5: Draft the Top 10 Risk Profile</i>	182
<i>Step 6: Review the Draft Risk Profile</i>	184
<i>Step 7: Communicate the Risk Profile with the Board or Board Committee</i>	185
<i>Step 8: Track the Results</i>	186
Conclusion	186
Notes	186
References	187
About the Author	188
12 How to Allocate Resources Based on Risk	189
Introduction	189
Risk Policy and a Center of Excellence for Risk Management	191
<i>Key Policy Elements</i>	191
<i>Center of Excellence</i>	192
<i>Translating Strategic Objectives into Risk-Based Concepts</i>	192
The Consequence Domain	193
<i>The Probability Domain</i>	197
<i>The Integration of Business Objectives/Risk Events/Risk Concepts</i>	198
Risk-Based Business Processes and Organizational Considerations	200
<i>Risk-Based Business Processes</i>	200
<i>Organizational Considerations</i>	204
Concepts, Methods, and Models Enabling Risk Identification, Evaluation, Mitigation, Prioritization, and Management	206
<i>The Concept of Evaluation Time Frames</i>	206
<i>Methods and Models to Quantify the Impact of Risk Events</i>	207
<i>Prioritization of Investment Proposals</i>	209
<i>Management of the Portfolio of Preferred Investment Proposals</i>	211
Information Requirements and Challenges	211
<i>Operational Risk Assessment Information</i>	212
<i>Strategic Risk Assessments</i>	212
Measures of Effectiveness for Continuous Improvement	213
Conclusion	213
Notes	214
About the Author	216
Appendix 12.A	216
13 Quantitative Risk Assessment in ERM	219
Introduction	219
Risk Assessment: Four Alternative Approaches	222
<i>Method 1: Active Management of the Largest Risks</i>	222
<i>Method 2: “High/Medium/Low” Classification of Risks: The Two-Dimensional Risk Map</i>	224

<i>Method 3: Risk Assessment Using Refined Classifications:</i>	
<i>Refining the Classification</i>	225
<i>Method 4: Statistical Analysis</i>	229
Aggregating Probabilities and Impacts	230
Total Corporate Risk: An Illustration	232
Incorporating Risk Quantification in the Business Planning Process	233
Sensitivities and Scenarios	233
Conclusion	234
Notes	235
References	235
About the Author	235
PART IV Types of Risk	237
14 Market Risk Management and Common Elements with Credit Risk Management	239
Introduction to Credit Risk and Market Risk	239
<i>A Taxonomy of Market and Credit Risk</i>	240
<i>Credit and Market Risk in an ERM Framework</i>	241
Responding to Credit and Market Risk	242
<i>The Case for Actively Managing Market Risk</i>	243
<i>The Case for Not Actively Managing Market Risk</i>	244
<i>Natural Market Risk Management</i>	245
Measuring Market Risk	246
<i>The Markets as Risk Indicators</i>	247
<i>Measuring Potential Impact</i>	248
<i>Earnings at Risk</i>	249
Market Risk Management with Forward-Type Products	250
<i>Market Risk Management with Option-Type Products</i>	253
<i>Trade-Offs Between Option Strategies and Forward Strategies</i>	255
<i>Operational Issues of Using Derivatives</i>	256
<i>Governance and Oversight of Market Risk Management</i>	257
Conclusion	259
Notes	259
References	260
About the Author	260
15 Credit Risk Management	261
Credit Risk Analysis	261
<i>Fundamental Analysis of Credit Default Risk (Probability of Default)</i>	263
<i>Market-Based Analysis of Credit Default Probability</i>	266
<i>Statistical-Based Models of Credit Risk</i>	268
<i>Credit Risk Mitigation</i>	269
An Analysis of the Credit Crisis	272
Conclusion	277
Notes	277

References	277
About the Author	278
16 Operational Risk Management	279
Introduction	279
What Is Operational Risk and Why Should You Care About It?	280
Is Risk All Bad?	283
How Do You Assess Operational Risks, Particularly in a Dynamic Business Environment?	284
Why You Need to Define Risk Tolerance for Aligned Decision Making	287
What Can You Do to Effectively Manage Operational Risk?	289
How Do You Encourage a Culture of Risk Management at the Operational Level?	296
How Do You Align Operational Risk Management with Enterprise Risk Management?	297
Conclusion	300
Notes	301
About the Author	301
17 Risk Management: Techniques in Search of a Strategy	303
Introduction	303
Current Situation	304
Risk Strategy Framework	307
Governance	312
New Directions	314
<i>Enterprise Risk Management (ERM): The First Step</i>	314
<i>Enterprise Resilience (ER): The Next Step?</i>	315
Conclusion	316
Notes	316
References	318
About the Author	320
18 Managing Financial Risk and Its Interaction with Enterprise Risk Management	321
Introduction	321
What Is Financial Risk and How Is It Managed?	322
<i>Case 1: Currency Price Risk: The Multinational Corporation</i>	323
<i>Case 2: Interest Rate Risk: The "Heavy-Debt" Firm</i>	324
<i>Case 3: Commodity Price Risk: The Firm with a Highly Volatile Input Cost</i>	324
Theoretical Underpinnings of Financial Hedging and Empirical Findings	325
<i>Hedging Reduces Expected Costs of Financial Distress and Underinvestment</i>	325
<i>Hedging Creates More Debt Capacity</i>	326
<i>Hedging Reflects the Incentives of the Firm's Management and Board</i>	326
<i>Does Hedging Affect Firm Value?</i>	327

Interaction of Financial Hedging with Other Types of Risk Management	328
<i>Credit Risk Management</i>	328
<i>Operational Risk Management</i>	329
<i>Strategic Risk Management</i>	330
<i>Reputation and Legal Risk Management</i>	330
<i>Financial Reporting and Disclosure Risk Management</i>	331
What Can We Learn About ERM Given Our Knowledge of Financial Hedging?	332
Notes	333
References	333
About the Author	334
19 Bank Capital Regulation and Enterprise Risk Management	337
Introduction	337
The Evolution of Bank Capital Requirements	337
<i>Overview of U.S. Capital Ratios</i>	338
<i>Basel I</i>	339
<i>Basel II</i>	341
<i>Enterprise Risk Management (ERM) and Economic Capital</i>	343
Conclusion	345
Notes	346
References	347
About the Author	349
20 Legal Risk Post-SOX and the Subprime Fiasco: Back to the Drawing Board	351
Introduction	351
The Legal Framework of Legal and Reputational Risk Management	352
<i>The Federal Rules of Professional Responsibility for Attorneys</i>	355
<i>Whistle-Blower Protection Under Sox</i>	357
<i>Audit Reform</i>	358
<i>Codes of Conduct</i>	358
An Assessment of the SOX Framework on Legal and Reputational Risk	359
<i>The Subprime Fiasco</i>	360
<i>The SOX Shortcomings</i>	362
Toward Optimal Reputational and Legal Risk Management	363
Conclusion	365
Note	365
References	365
About the Author	367
21 Financial Reporting and Disclosure Risk Management	369
The Importance of Disclosure Management and ERM Foundations in the United States	369
	370

Disclosure and Sarbanes-Oxley	371
<i>New Group for Reporting: Public Company Accounting Oversight Board</i>	371
Important SOX Sections	372
<i>Section 404: Internal Controls and Compliance Management</i>	372
<i>Section 302: Who Is Responsible for Financial Reporting?</i>	372
Other Financial Reporting	375
<i>Accounting for Derivatives—FASB 133</i>	375
<i>Firm Choice for FASB 133 and Disclosure Risk Management</i>	375
Risk Identification, Monitoring, and Reporting	377
Financial Reporting Challenges Today	379
<i>Paring Down Internal Control: Auditing Standard 5 (AS5)</i>	379
<i>Global Financial Crisis and ERM</i>	379
<i>Reexamining Fair Value Accounting: FASB 157</i>	380
<i>Conflicts with International Standards: Rules versus Principles</i>	381
<i>Adding ERM to Company Credit Ratings</i>	383
Conclusion	383
Notes	383
References	384
About the Author	384

PART V Survey Evidence and Academic Research 385

22 Who Reads What Most Often?: A Survey of Enterprise Risk Management Literature Read by Risk Executives 387

Introduction	387
Survey Methodology	389
Survey Results	390
<i>Survey Respondent Profile</i>	390
<i>ERM Tools and Techniques Used by Respondents</i>	392
<i>Most Frequently Read Literature on ERM</i>	396
<i>Critical Areas of Need</i>	399
<i>Key Findings of Our Survey</i>	400
Conclusion	402
Appendix 22.A: Publications Included in the Survey	403
Appendix 22.B: Survey Respondents Who Gave Permission to Be Identified	410
Notes	410
References	412
About the Authors	416

23 Academic Research on Enterprise Risk Management 419

Introduction	419
Academic Research on Enterprise Risk Management	420
<i>Colquitt, Hoyt, and Lee (1999)</i>	425
<i>Kleffner, Lee, and McGannon (2003)</i>	426
<i>Liebenberg and Hoyt (2003)</i>	426

<i>Beasley, Clune, and Hermanson (2005a)</i>	427
<i>Beasley, Clune, and Hermanson (2005b)</i>	428
<i>Desender (2007)</i>	429
<i>Beasley, Pagach, Warr (2008)</i>	429
<i>Pagach and Warr (2008a)</i>	430
<i>Pagach and Warr (2008b)</i>	431
<i>Gates, Nicolas, and Walker (2009)</i>	431
Case Studies on ERM	432
<i>Harrington, Niehaus, and Risko (2002)</i>	432
<i>Aabo, Fraser, and Simkins (2005)</i>	434
<i>Stroh (2005)</i>	434
<i>Acharyya and Johnson (2006)</i>	435
<i>Nocco and Stulz (2006)</i>	436
Conclusion	436
Notes	437
References	438
About the Authors	439
24 Enterprise Risk Management: Lessons from the Field	441
Introduction	441
Lessons from the ERM Process	442
<i>Clarifying Strategies and Objectives</i>	442
<i>Identifying Risks</i>	443
<i>Assessing Risk</i>	444
<i>Acting on the Risks</i>	448
<i>Monitoring Risks</i>	449
Lessons from Integrating ERM with Ongoing Management Initiatives	449
<i>Strategic Planning and ERM</i>	449
<i>The Balanced Scorecard and ERM</i>	452
<i>Budgeting and ERM</i>	454
<i>Internal Auditing and ERM</i>	454
<i>Business Continuity Planning, Crisis Preparedness, and ERM</i>	455
<i>Corporate Governance and ERM</i>	456
Some Key Value Lessons from ERM	457
Conclusion	459
Notes	459
References	460
Further Reading	461
About the Authors	462
PART VI Special Topics and Case Studies	465
25 Rating Agencies' Impact on Enterprise Risk Management	467
Introduction	467
Banking: General	468

Insurance: S&P	468
Insurance: Moody's	470
Insurance: Fitch	471
Insurance: A.M. Best	472
U.S. Energy Companies: S&P	473
Nonfinancial Companies: S&P	473
A Fly in the Ointment	476
Conclusion	476
Notes	477
Further Reading	478
About the Author	478
26 Enterprise Risk Management: Current Initiatives and Issues	479
Question 1	482
Question 2	483
Question 3	489
Question 4	491
Question 5	493
Question 6	495
Question 7	497
Question 8	499
Notes	502
27 Establishing ERM Systems in Emerging Countries	505
Introduction	505
Enterprise Risk Management and Its Benefits in Emerging Markets	506
<i>Evolution of Risk Management in Emerging Markets</i>	509
<i>The Rationale for Effective Risk Management in Emerging Markets</i>	515
<i>The Responsibility of the Board in Risk Management and Extensions to Emerging Markets</i>	516
<i>Risk, Reward, and Risk Appetite in Emerging Markets</i>	523
Observations of ERM Practices in Emerging Countries	524
Conclusion	524
Appendix: COSO Approach to Enterprise Risk Management	525
Notes	527
References	528
About the Author	528
28 The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One	531
Hydro One	533
Getting Started with ERM	533
<i>Corporate Risk Management Group</i>	534
<i>Pilot Study</i>	534
<i>Final Approval</i>	538

Processes and Tools	538
<i>The Business Context</i>	538
<i>Identification and Assessment of Risks and Controls</i>	540
<i>Tolerability of Risk—and Risk Mitigation</i>	542
<i>Monitor and Review</i>	543
Corporate Risk Profile	543
<i>Description of Risk Sources</i>	543
Quantifying the Unquantifiable	548
Benefits of ERM and Outcomes at Hydro One	550
<i>Current Status</i>	552
Conclusion	553
Notes	553
About the Authors	556
Index	557

Foreword

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

ENTERPRISE RISK MANAGEMENT

PART I

Overview

CHAPTER 1

Enterprise Risk Management

An Introduction and Overview

JOHN R.S. FRASER

Vice President, Internal Audit & Chief Risk Officer, Hydro One Networks Inc.

BETTY J. SIMKINS

Williams Companies Professor of Business and Professor of Finance, Oklahoma State University

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

—Charles Darwin

WHAT IS ENTERPRISE RISK MANAGEMENT?

Enterprise risk management (ERM) can be viewed as a natural evolution of the process of risk management. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines enterprise risk management as: “. . . a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” The COSO definition is intentionally broad and deals with risks and opportunities affecting value creation or preservation. Similarly, in this book, we take a broad view of ERM, or what we call—a *holistic approach to ERM*.

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

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

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

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

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

DRIVERS OF ENTERPRISE RISK MANAGEMENT

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

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

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

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

SUMMARY OF THE BOOK CHAPTERS

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

Overview

ERM Management, Culture, and Control

ERM Tools and Techniques

Types of Risks

Survey Evidence and Academic Research

Special Topics and Case Studies

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

Overview

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

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

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

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

ERM Management, Culture, and Control

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

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