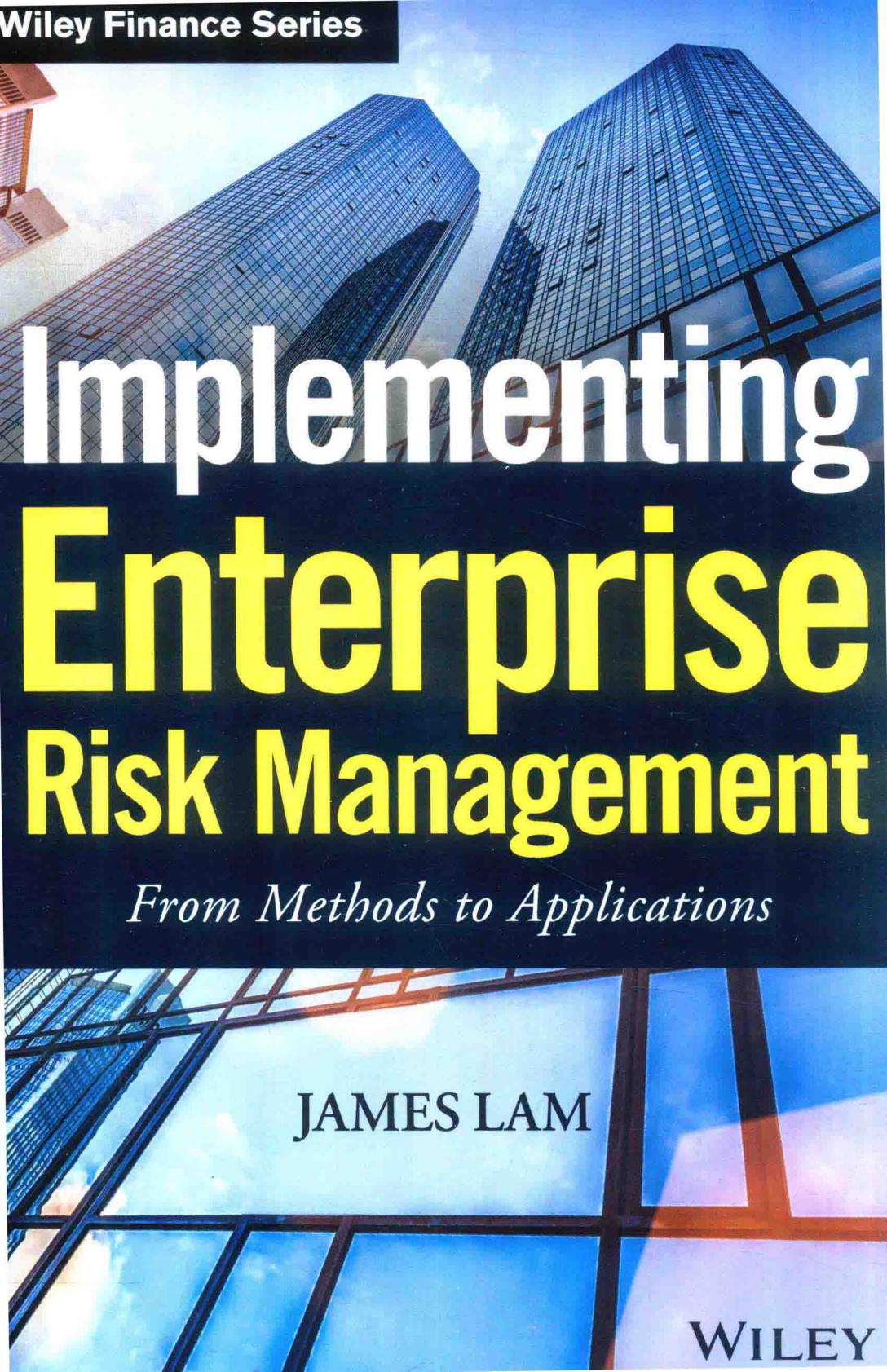


Wiley Finance Series



Implementing Enterprise Risk Management

From Methods to Applications

JAMES LAM

WILEY

Implementing Enterprise Risk Management

From Methods to Applications

JAMES LAM

WILEY

Copyright © 2017 by James Lam. 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) 646-8600, 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 publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data is Available:

ISBN 9780471745198 (Hardcover)

ISBN 9781118221563 (ePDF)

ISBN 9781118235362 (ePub)

Cover Image: © canadastock/Shutterstock

Cover Design: Wiley

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

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

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

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

For my father, and best friend, Kwan Lun Lam

Preface

Confucius said: “I hear and I forget. I see and I remember. I do and I understand.”

Indeed, the value of knowledge is not in its acquisition but in its application. I am grateful that I have had opportunities to apply risk management in a wide range of roles throughout my 30-year career in risk management. As a consultant, I’ve worked with clients with different requirements based on their size, complexity, and industry. As a risk manager, I’ve implemented enterprise risk management (ERM) programs while overcoming data, technical, and cultural challenges. As a founder of a technology start-up, I’ve worked with customers to leverage advanced analytics to improve their risk quantification and reporting. In the past four years, as a board member and risk committee chair, I’ve worked with my board colleagues to provide independent risk oversight while respecting the operating role of management.

These experiences have taught me that knowledge of ERM best practices is insufficient. Value can be created only if these practices are integrated into the decision-making processes of an organization. The purpose of this book is to help my fellow risk practitioners to bridge the gap between knowledge and practical applications.

In my first book, *Enterprise Risk Management—From Incentives to Controls* (Wiley, 1st edition 2003, 2nd edition 2014), the focus was on the *what* questions related to ERM:

- What is enterprise risk management?
- What are the key components of an ERM framework?
- What are best practices and useful case studies?
- What are the functional requirements for credit, market, and operational risks?
- What are the industry requirements for financial institutions, energy firms, and non-financial corporations?

In this companion book, the focus is on the *how* questions:

- How to implement an ERM program?
- How to overcome common implementation issues and cultural barriers?

- How to leverage ERM in all three lines of defense: business and operational units, risk and compliance, and the board and internal audit?
- How to develop and implement specific ERM processes and tools?
- How to enhance business decisions and create value with ERM?

The publication of my first ERM book was one of the most gratifying professional experiences of my career. The book has been translated into Chinese, Japanese, Korean, and Indonesian. It has been adopted by leading professional associations and university programs around the world. On Amazon.com, it has ranked #1 best-selling among 25,000 risk management titles. In a 2007 survey of ERM practitioners in the United States and Canada conducted by the Conference Board of Canada, the book was ranked among the top-10 in ERM books and research papers. In addition, the book has brought me countless consulting and speaking opportunities internationally.

In my travels, risk professionals most often request practical approaches and case studies, as well as best-practice templates and examples that can assist them in their ERM programs. Based on this feedback, I have structured this book to focus on effective implementation of ERM.

OVERVIEW OF THE BOOK

This book is organized into seven parts. Part One provides the overall context for the current state and future vision of ERM:

- Chapter 1 introduces the notion that *risk is a bell curve*. It also lays out the fundamental concepts and definitions for enterprise risk management. We also discuss the business case for, and current state of, the practice of ERM.
- Chapter 2 reviews the key trends and developments in ERM since the 2008 financial crisis, including lessons learned and major changes since that time.
- In Chapter 3, a new performance-based continuous model for ERM is introduced. This new model is more fitting for global risks that are changing at an ever faster speed (e.g. cybersecurity, emerging technologies). As part of this discussion, seven specific attributes for this new ERM model are provided.
- In addition to the board and management, other stakeholders such as regulators, institutional investors, and rating agencies are increasingly focused on ERM. Chapter 4 discusses their requirements and expectations.

ERM is a multi-year effort that requires significant attention and resources. As such, Part Two focuses on ERM program implementation:

- Chapter 5 lays out the scope and objectives of an ERM project, including the need to set a clear vision, obtain buy-in, and develop a roadmap. This chapter also provides an ERM Maturity Model and an illustrative 24-month implementation plan.
- One of the key success factors in ERM is addressing change management and risk culture. Chapter 6 describes risk culture success factors and the cognitive biases and behavior obstacles that risk professionals must overcome.
- Given the wide range and complexity of risks, having a structured and organizing ERM framework is essential. Chapter 7 provides an overview of several published frameworks and an ERM framework that I've developed to support performance-based continuous ERM.

The next four parts provide deep dives into the key components of the ERM framework. Part Three focuses on risk governance and policies:

- Chapter 8 discusses two versions of the “three lines of defense” model—the conventional model and a modified model that I've developed to reflect better the role of the board.
- Chapter 9 goes further into the important role of the board in ERM, including regulatory requirements and expectations, current board practices, and three key levers for effective risk oversight.
- Chapter 10 describes my first-hand experience as an independent director and risk committee chair at E*TRADE Financial. This case study discusses our turnaround journey, the implementation of ERM best practices, and the tangible benefits that we've realized to date.
- As expected, the rise of the chief risk officer (CRO) is correlated to the adoption of ERM. Chapter 11 discusses the evolution in the role of the CRO, including key responsibilities, required skills, and desired attributes. The chapter also provides professional profiles of six prominent current or former CROs.
- Chapter 12 focuses on one of the most important risk policies: risk appetite statement. This chapter provides practical steps and key requirements for developing an effective risk appetite statement.

Risk analytics provide useful input to business and risk leaders. Risk assessment and quantification is the focus of Part Four:

- Chapter 13 discusses the implementation requirements, common pitfalls, and practical solutions for developing a risk-control self-assessment process.

- What gets measured gets managed, so it is not enough only to identify and assess risks. Chapter 14 provides a high-level review of risk quantification models, including those designed to measure market risk, credit risk, and operational risk.

ERM can create significant value only if it supports management strategies, decisions, and actions. Part Five focuses on risk management strategies that will optimize an organization's risk profile:

- The integration of strategy and ERM, also known as strategic risk management, is covered in Chapter 15. The chapter outlines the processes and tools to measure and manage strategic risk, including M&A analysis and risk-based pricing. Case studies and examples of strategic risk models are also provided.
- Chapter 16 goes further into risk-based performance management and discusses other strategies to add value through ERM, such as capital management and risk transfer.

Board members and business leaders need good metrics, reports, and feedback loops to monitor risks and ERM effectiveness. Part Six focuses on risk monitoring and reporting:

- Chapter 17 discusses the integration of key performance and risk indicators, including the sources and characteristics of effective metrics.
- Once these metrics are developed, they must be delivered to the right people, at the right time, and in the right way. Chapter 18 provides the key questions, best-practice standards, and implementation requirements of ERM dashboard reporting.
- Once an ERM program is up and running, how do we know if it is working effectively? Chapter 19 answers this critical question by establishing a quantifiable performance objective and feedback loop for the overall ERM program. An example of a feedback loop based on earnings-at-risk analysis is also discussed.

Chapter 20 in Part Seven provides additional ERM templates and outlines to help readers accelerate their ERM initiatives.

Throughout this book, specific step-by-step implementation guidance, examples, and outlines are provided to support risk practitioners in implementing ERM. They are highlighted below:

- Example of a reputational risk policy (Chapter 4, Appendix A)
- ERM Maturity Model and benchmarks (Chapter 5, Appendix A)

- Practical 24-month plan for ERM program implementation (Chapter 5, Appendix B)
- 10-step process for developing a risk appetite statement, including examples of risk metrics and tolerance levels (Chapter 12)
- Implementation of the RCSA process, including common pitfalls and best practices (Chapter 13)
- Example of a strategic risk assessment (Chapter 20)
- Structure and outline of a CRO report to the risk committee (Chapter 20)
- Example of a cybersecurity risk appetite statement and metrics (Chapter 20)
- Example of a model risk policy (Chapter 20)
- Example of a risk escalation policy (Chapter 20)

SUGGESTED CHAPTERS BY AUDIENCE

Given its focus on ERM implementation, this book does not necessarily need to be read in its entirety or in sequence. Readers should select the relevant chapters based on the implementation phase and ERM maturity at their organizations. In general, I would suggest the following chapters by the seniority of the reader:

- Board members and senior corporate executives should read Chapters 1, 3, 6, 9, 10, 12, 15, and 19.
- Mid- to senior-level risk professionals, up to a CRO, should read the above chapters plus Chapters 4, 5, 7, 8, 11, and 16.
- Students and junior-level risk professionals should read the entire book.

Acknowledgments

I would like to thank the Enterprise Risk Management team at Workiva for contributing to this book through excellent research and editorial support. In particular, I would like to thank Joe Boeser, Melissa Chen, Adam Gianforte, Garrett Lam, Jay Miller, Diva Sharma, Rachel Stern, and Zach Wisner. I want to especially thank Mark Ganem and Neil O'Hara for their outstanding editorial support. This book was the result of a collaborative team effort and it was truly my pleasure to work with such a great team.

I would also like to extend my appreciation to Paymon Aliabadi, Matt Feldman, Susan Hooker, Merri Beth Lavagnino, Bob Mark, and Jim Vinci for sharing their stories and experiences as chief risk officers across different industry sectors. Their experiences in ERM implementation provide useful and practical insights. They also offer good advice to risk professionals who aspire to become a CRO. Their compelling stories are featured in Chapter 11. I am confident that risk professionals, regardless of where they are in their careers, will be inspired by their stories and benefit from their advice. I know I have.

Finally, I would like to thank Bill Fallon and Judy Howarth from John Wiley & Sons for their patience and assistance throughout the book production process.

Implementing Enterprise Risk Management

Contents

Preface	xiii
Acknowledgments	xix
PART ONE	
ERM in Context	
CHAPTER 1	
Fundamental Concepts and Current State	3
Introduction	3
What Is Risk?	4
What Does Risk Look Like?	8
Enterprise Risk Management (ERM)	11
The Case for ERM	13
Where ERM Is Now	18
Where ERM Is Headed	19
Notes	20
CHAPTER 2	
Key Trends and Developments	21
Introduction	21
Lessons Learned from the Financial Crisis	21
The Wheel of Misfortune Revisited	26
Global Adoption	34
Notes	37
CHAPTER 3	
Performance-Based Continuous ERM	41
Introduction	41
Phase Three: Creating Shareholder Value	43
Performance-Based Continuous ERM	44
Case Study: Legacy Technology	56
Notes	59

CHAPTER 4

Stakeholder Requirements	61
Introduction	61
Stakeholders Defined	62
Managing Stakeholder Value with ERM	79
Implementing a Stakeholder Management Program	80
Appendix A: Reputational Risk Policy	83
Notes	87

PART TWO**Implementing an ERM Program****CHAPTER 5**

The ERM Project	93
Introduction	93
Barriers to Change	93
Establish the Vision	95
Obtain Buy-In from Internal Stakeholders	97
Assess Current Capabilities against Best Practices	100
Develop a Roadmap	104
Appendix A: ERM Maturity Model	108
Appendix B: Practical Plan for ERM Program	
Implementation	111

CHAPTER 6

Risk Culture	115
Introduction	115
Risk Culture Success Factors	117
Best Practice: Risk Escalation	130
Conclusion	130
Notes	131

CHAPTER 7

The ERM Framework	132
Introduction	132
The Need for an ERM Framework	132
ERM Framework Criteria	136
Current ERM Frameworks	138
An Update: The Continuous ERM Model	145
Developing a Framework	150
Conclusion	153
Notes	153

PART THREE

Governance Structure and Policies

CHAPTER 8

The Three Lines of Defense	157
Introduction	157
COSO's Three Lines of Defense	158
Problems with This Structure	160
The Three Lines of Defense Revisited	164
Bringing It All Together: How the Three Lines Work in Concert	172
Conclusion	173
Notes	173

CHAPTER 9

Role of the Board	175
Introduction	175
Regulatory Requirements	176
Current Board Practices	179
Case Study: Satyam	180
Three Levers for ERM Oversight	181
Conclusion	189
Notes	189

CHAPTER 10

The View from the Risk Chair	191
Introduction	191
Turnaround Story	191
The GPA Model in Action	192
Top Priorities for the Risk Oversight Committee	192
Conclusion	196
Notes	197

CHAPTER 11

Rise of the CRO	198
Introduction	198
History and Rise of the CRO	199
A CRO's Career Path	201
The CRO's Role	202
Hiring a CRO	206
A CRO's Progress	208
Chief Risk Officer Profiles	212
Notes	225

CHAPTER 12

Risk Appetite Statement	227
Introduction	227
Requirements of a Risk Appetite Statement	228
Developing a Risk Appetite Statement	233
Roles and Responsibilities	239
Monitoring and Reporting	242
Examples of Risk Appetite Statements and Metrics	246
Notes	250

PART FOUR**Risk Assessment and Quantification****CHAPTER 13**

Risk Control Self-Assessments	255
Introduction	255
Risk Assessment: An Overview	255
RCSA Methodology	256
Phase 1: Setting the Foundation	259
Phase 2: Risk Identification, Assessment, and Prioritization	262
Phase 3: Deep Dives, Risk Quantification, and Management	267
Phase 4: Business and ERM Integration	270
ERM and Internal Audit Collaboration	272
Notes	273

CHAPTER 14

Risk Quantification Models	274
Introduction	274
Market Risk Models	275
Credit Risk Models	278
Operational Risk Models	281
Model Risk Management	283
The Loss/Event Database	288
Early Warning Indicators	289
Model Risk Case Study: AIG	289
Notes	290

PART FIVE**Risk Management****CHAPTER 15**

Strategic Risk Management	295
Introduction	295
The Importance of Strategic Risk	296
Measuring Strategic Risk	299
Managing Strategic Risk	301
Appendix A: Strategic Risk Models	310
Notes	312

CHAPTER 16

Risk-Based Performance Management	314
Introduction	314
Performance Management and Risk	316
Performance Management and Capital	317
Performance Management and Value Creation	319
Summary	323
Notes	324

PART SIX**Risk Monitoring and Reporting****CHAPTER 17**

Integration of KPIs and KRIs	327
Introduction	327
What Is an Indicator?	327
Using Key Performance Indicators	329
Building Key Risk Indicators	330
KPI and KRI Program Implementation	335
Best Practices	337
Conclusion	338
Notes	339

CHAPTER 18

ERM Dashboard Reporting	340
Introduction	340
Traditional Risk Reporting vs. ERM Dashboard Reporting	344
General Dashboard Requirements	348