

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

Implementing ERM Dashboards	351
Avoid Common Mistakes	357
Best Practices	358
Notes	361

CHAPTER 19

Feedback Loops 362

Introduction	362
What Is a Feedback Loop?	363
Examples of Feedback Loops	364
ERM Performance Feedback Loop	366
Measuring Success with the ERM Scorecard	368
Notes	371

PART SEVEN

Other ERM Resources

CHAPTER 20

Additional ERM Templates and Outlines 375

Introduction	375
Strategic Risk Assessment	375
CRO Report to the Risk Committee	376
Cybersecurity Risk Appetite and Metrics	378
Model Risk Policy	380
Risk Escalation Policy	382
Notes	385

About the Author 386

Index 387