# Contents

COPYRIGHTED MATERIAL

http://www.pbookshop.com

**Preface** **xi**

**Chapter 1: Introduction: Enterprise Risk Management Today** **1**

The COSO Internal Controls Framework: How Did We Get Here? 2
The COSO Internal Controls Framework 3
COSO Internal Controls: The Principal Recognized Internal Controls Standard 14
An Introduction to COSO ERM 14
Governance, Risk, and Compliance 15
Global Computer Products: Our Example Company 16

**Chapter 2: Importance of Governance, Risk, and Compliance Principles** **21**

Road to Effective GRC Principles 22
Importance of GRC Governance 23
Risk Management Component of GRC 25
GRC and Enterprise Compliance 26
Importance of Effective GRC Practices and Principles 28

**Chapter 3: Risk Management Fundamentals** **31**

Fundamentals: Risk Management Phases 32
Other Risk Assessment Techniques 45

**Chapter 4: COSO ERM Framework** **51**

ERM Definitions and Objectives: A Portfolio View of Risk 51
COSO ERM Framework Model 55
Other Dimensions of the ERM Framework 86

**Chapter 5: Implementing ERM in the Enterprise** **89**

Roles and Responsibilities of an Enterprise Risk Management Function 90
Risk Management Policies, Standards, and Strategies 100
Business, IT, and Risk Transfer Processes 105
Risk Management Reviews and Corrective Action Practices 108
ERM Communications Approaches 112
CRO and an Effective Enterprise Risk Management Function 113

**Chapter 6: Importance of Strong Enterprise Governance Practices** **115**

History and Background of Enterprise Governance: A U.S. Perspective 116
Enterprise Integrity and Ethical Behavior 119
Disclosure and Transparency 125
Rights and Equitable Treatment of Shareholders and Key Stakeholders 126
Governance Role and Responsibilities of the Board 128
Governance as a Key Element of GRC 128

**Chapter 7: Enterprise Compliance Issues Today** **131**

Compliance Issues Today 132
Establish a Compliance Assessment Team 133
Compliance Risk Assessments and Compliance Program Reviews 136
Work Unit–Level Compliance Tracking and Review Processes 138
Compliance-Related Procedures and Staff Education Programs 141
Enterprise Hotline Compliance and Whistleblower Support 142
Assessing the Overall Enterprise Compliance Program 144

**Chapter 8: Integrating ERM with COSO Internal Controls** **147**

COSO Internal Controls Background and Earlier Legislation 147
Efforts Leading to the Treadway Commission 151
COSO Internal Controls Framework 156
COSO Internal Controls and COSO ERM: Compared 174

**Chapter 9: Sarbanes-Oxley and Enterprise Risk Management Concerns** **177**

Sarbanes-Oxley Act Background 177
SOx Legislation Overview 179
Enterprise Risk Management and SOx Section 404 Reviews 193
Internal Controls Reporting and Materiality 198
PCAOB Risk-Based Auditing Standards 199
Sarbanes-Oxley: The Other Sections 200
SOx and COSO ERM 201

**Chapter 10: Corporate Culture and Risk Portfolio Management** **203**

Whistleblower and Hotline Functions 204
Risk Portfolio Management 208
Integrated Enterprise-Wide Risk Management 211

**Chapter 11: OCEG Capability Model GRC Standards** **215**

GRC Capability Model ''Red Book'' 215
Other OCEG Materials: The ''Burgundy Book'' 223
Level and Scope of the OCEG Standards-Setting Authority 224

http://www.pbookshop.com

**Chapter 12: Importance of GRC Principles in the Board Room 225**

Board Decisions and Risk Management 226
Board Organization and Governance Rules 230
Corporate Charters and the Board Committee Structure 231
Audit Committees and Managing Risks 235
Establishing a Board-Level Risk Committee 238
Audit and Risk Committee Coordination 244
COSO ERM and Corporate Governance 245

**Chapter 13: Role of Internal Audit in Enterprise Risk Management 247**

Internal Audit Standards for Evaluating Risk 248
COSO ERM for More Effective Internal Audit Planning 251
Risk-Based Internal Audit Findings and Recommendations 264
COSO ERM and Internal Audit 265

**Chapter 14: Understanding Project Management Risks 267**

Project Management Process 268
*PMBOK® Guide*: *A Guide to the Project Management Book of Knowledge* 269
*PMBOK® Guide*'s Project Manager Risk Management Approach 272
Project-Related Risks: What Can Go Wrong 282
Implementing ERM for Project Managers 285

**Chapter 15: Information Technology and Enterprise Risk Management 291**

IT and the COSO ERM Framework 292
IT Application Systems Risks 294
Effective IT Continuity Planning 302
Worms, Viruses, and System Network Risks 307
IT and Effective ERM Processes 309

**Chapter 16: Establishing an Effective GRC Culture throughout the Enterprise 311**

First Steps to Establishing a GRC Culture: An Example 312
Promoting the Concept of Enterprise Risk 314
Establishing of Enterprise-Wide Governance Awareness 319
Enterprise Codes of Conduct 323
Building a GRC Culture: Risk, Governance, and Compliance Education Programs 326
Keeping the GRC Culture Current 327

**Chapter 17: ISO 31000 and 38500 Risk Management Worldwide Standards 331**

ISO Standards-Setting Process 332
Understanding ISO 31000 334

http://www.pbookshop.com

ISO 38500: The Corporate Governance of IT 337
Implementing an ISO Standard 340

**Chapter 18: ERM and GRC Principles Going Forward 343**

ERM and GRC for the Internal Controls Professional 344
COSO's Ongoing Support Role 347
COSO ERM and GRC Future Prospects 348

**About the Author 351**

**Index 353**

http://www.pbookshop.com