

Contents

Preface	ix
Chapter 1: Importance of the COSO Internal Control Framework	1
The Importance of Enterprise Internal Controls	2
What Are Enterprise Internal Controls?	3
Understanding the COSO Internal Control Framework: How to Use This Book	4
Chapter 2: How We Got Here: Internal Control Background	5
Early Definitions of Internal Controls: Foreign Corrupt Practices Act of 1977	7
The FCPA and Internal Controls Today	8
Events Leading Up to the Treadway Commission	9
Earlier AICPA Auditing Standards: SAS Nos. 55 and 78	10
The Treadway Committee Report	11
The Original COSO Internal Control Framework	12
The Sarbanes-Oxley Act and Internal Accounting Controls	15
Notes	28
Chapter 3: COSO Internal Controls: The New Revised Framework	29
Understanding Internal Controls	30
Revised Framework Business and Operating Environment Changes	32
The Revised COSO Internal Control Framework	35
COSO Internal Control Principles	37
COSO Objectives and Business Operations	38
Sources for More Information	40
Chapter 4: COSO Internal Control Components: Control Environment	41
Importance of the Control Environment	41
Control Environment Principle 1: Integrity and Ethical Values	43
Control Environment Principle 2: Role of the Board of Directors	48
Control Environment Principle 3: The Need for Authority and Responsibility	49
Control Environment Principle 4: Human Resource Strengths	51
Control Environment Principle 5: Individual Internal Control Responsibilities	54
COSO Control Environment in Perspective	56

Chapter 5: COSO Internal Control Components: Risk Assessment	59
Risk Assessment Component Principles	60
Risk Identification and Analysis	62
Risk Response Strategies	66
Fraud Risk Analysis	69
COSO Risk Assessment and the Revised Internal Control Framework	70
Notes	71
Chapter 6: COSO Internal Control Components: Control Activities	73
COSO Control Activity Principles	74
COSO Control Activities Today	85
Chapter 7: COSO Internal Control Components: Information and Communication	87
Information and Communications: What Has Changed?	87
Information and Communication Principle 1: Use of Relevant Information	89
Information and Communication Principle 2: Internal Communications	96
Information and Communication Principle 3: External Communications	100
The Importance of COSO Information and Communication	102
Notes	103
Chapter 8: COSO Internal Control Components: Monitoring Activities	105
Importance of COSO Monitoring Internal Control Activities	106
COSO Monitoring Principle 1: Conduct Ongoing and Separate Evaluations	108
COSO Monitoring Principle 2: Evaluate and Communicate Deficiencies	112
COSO Internal Control Monitoring in Perspective	115
Note	115
Chapter 9: COSO Internal Control GRC Operations Controls	117
COSO Operations Objectives	117
Planning and Budgeting Operations Controls	119
IT Systems Operations Controls	123
Operations Procedure Controls and Service Catalogs	133
Importance of COSO Operations Controls	135
Note	135
Chapter 10: COSO Reporting Processes	137
COSO Reporting Objectives	137
COSO External Financial Reporting Controls	139
COSO Internal Financial Reporting Controls	141
COSO External Nonfinancial Reporting Controls	149
COSO Internal Nonfinancial Reporting Controls	149
Importance of COSO Reporting Controls	150
Note	151

Chapter 11: COSO Legal, Regulatory, and Compliance Objectives	153
Importance of Enterprise Compliance Controls	153
Regulatory Compliance Control Issues	155
Internal Controls and Legal Issues	157
Compliance with Professional and Other Standards	158
Chapter 12: Internal Control Entity and Organizational GRC Relationships	161
Internal Controls from an Organizational GRC Perspective	161
Enterprise Governance Overall Concepts	163
Business Entity–Level Internal Controls	167
Divisional and Functional Unit Internal Controls	175
Department- and Unit-Level Internal Controls	178
Organization and GRC Controls in Perspective	179
Note	179
Chapter 13: COSO, Service Management, and Effective IT Controls	181
Importance of IT General Controls	181
IT Governance General Controls	183
IT Management General Controls	184
Client-Server and Smaller Systems General IT Controls	188
ITIL Service Management Best Practices	191
Service Delivery Best Practices	200
Notes	201
Chapter 14: Cloud Computing, Virtualization, and Wireless Networks	203
Internal Controls for IT Wireless Networks	204
Cloud Computing and COSO Internal Controls	208
Storage Management Virtualization	214
COSO Internal Controls and Newer Technologies	215
Note	215
Chapter 15: Another Framework: COSO ERM	217
ERM Definitions and the ERM Portfolio View of Risk	218
The COSO ERM Framework Model	222
Other Dimensions of the ERM Framework	239
COSO ERM and the Revised Internal Control Framework	240
Notes	241
Chapter 16: Understanding and Using COBIT	243
An Executive’s Introduction to COBIT	244
Using COBIT to Assess Enterprise Internal Controls	252
Mapping COBIT to COSO Internal Controls	256
Notes	257

Chapter 17: ISO Internal Control and Risk Management Standards	259
Background and Importance of ISO Standards in a Global Commerce World	259
ISO Standards Overview	262
ISO Standards and the COSO Internal Control Framework	269
Notes	270
Chapter 18: COSO Internal Controls in the Board Room	271
Board Decisions and Internal Control Processes	272
Board Organization and Governance Rules	275
Corporate Charters and the Board Committee Structure	276
The Audit Committee and Managing Internal Controls	279
Board Member Internal Control Knowledge Requirements	281
COSO Internal Controls and Corporate Governance	282
Notes	283
Chapter 19: Service Organization Control Reports and COSO Internal Controls	285
Importance of Service Organization Internal Controls	286
Early Steps to Gain Assurance: SAS 70	287
Service Organization Control (SOC) Reports	288
Right-to-Audit Clauses	290
Internal Control Limitations	292
Chapter 20: Implementing the Revised COSO Internal Control Framework	293
Understanding What Is New in the 2013 Framework	293
Transitioning to the New COSO Guidance	295
Steps to Begin Implementing the New COSO Internal Control Framework	296
Index	297