COSO Internal Controls

Robert R. Moeller

Table of Contents

Chapter 1 – Importance of the COSO Internal Control Framework 1
Learning Objectives 1
Introduction 1
The Importance of Enterprise Internal Controls 2
What Are Enterprise Internal Controls? 2
Understanding the COSO Internal Control Framework: How to Use This Book 3
Review Questions 4
Review Answers 5

Chapter 2 – How We Got Here: Internal Control Background 6
Learning Objectives 6
Introduction 6
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 10
The Original COSO Internal Control Framework 11
The Sarbanes-Oxley Act and Internal Accounting Controls 13
Title I: Public Company Accounting Oversight Board 14
Title II: Auditor Independence 16
Title III: Corporate Responsibility 17
Title IV: Enhanced Financial Disclosures 20
Title V: Analyst Conflicts of Interest 22
Titles VI through X: Fraud Accountability and White-Collar Crime 22
Title XI: Corporate Fraud Accountability 23
Review Questions 24
Review Answers 25

Chapter 3 – COSO Internal Controls: The New Revised Framework 27
Learning Objectives 27
Introduction 27
Understanding Internal Controls 27
Revised Framework Business and Operating Environment Changes 29
External Financial Reporting Objectives 30
Internal Control Operations Objectives 31
Internal Control Compliance Objectives 31
Overlapping Internal Control Objectives 31
The Revised COSO Internal Control Framework 32
COSO Internal Control Principles 33
COSO Objectives and Business Operations 34
Sources for More Information 36
Review Questions 37
Review Answers 38

Chapter 4 – COSO Internal Control Components: Control Environment 39
Learning Objectives 39
Introduction 39
Importance of the Control Environment 39
Control Environment Principle 1: Integrity and Ethical Values 40
Establishing an Enterprise Code of Conduct 41
Affirming Adherence to the Code of Conduct 43
Code Violations and Corrective Actions 43

Control Environment Principle 2: Role of the Board of Directors 44
Control Environment Principle 3: The Need for Authority and Responsibility 45
Control Environment Principle 4: Human Resource Strengths 47
Commitment to Competence 47
Attracting, Developing, and Retaining Individual Employees and Stakeholders 48
Planning and Preparing for Personnel Succession 48
Control Environment Principle 5: Individual Internal Control Responsibilities 49
Accounting for Internal Controls 49
Performance Measures, Incentives, and Rewards 49
COSO Control Environment in Perspective 50
Review Questions 52
Review Answers 53

Chapter 5 – COSO Internal Control Components: Risk Assessment 55
Learning Objectives 55
Introduction 55
Risk Assessment Component Principles 55
Risk Identification and Analysis 57
Risk Response Strategies 61
Fraud Risk Analysis 63
COSO Risk Assessment and the Revised Internal Control Framework 64
Review Questions 65
Review Answers 66

Chapter 6 – COSO Internal Control Components: Control Activities 67
Learning Objectives 67
Introduction 67
COSO Control Activity Principles 67
Control Activity Principles: Integration with Risk Assessment 68
Enterprise-Specific Control Activity Factors 68
Business Process Control Activities 69
Types of Transaction Control Activities 70
Control Activity Principles: Selection and Development of General IT Controls 71
Control Activity Technology General Controls 72
Security Management Processes 72
Technology Acquisition, Development, and Maintenance Processes 73
Control Activity Principles: Policies and Procedures 74
COSO Control Activities Today 76
Review Questions 77
Review Answers 78

Chapter 7 – COSO Internal Control Components: Information and Communication 80
Learning Objectives 80
Introduction 80
Information and Communications: What Has Changed? 80
Information and Communication Principle 1: Use of Relevant Information 82
Information from Relevant Sources 83
Processing Data through Information Systems 84
Importance of Information Quality 84
Information and Communication Principle 2: Internal Communications 87
Internal Control Communication 87
Communication beyond Normal Channels 88
Methods of Communication 89
Information and Communication Principle 3: External Communications 89
Inbound Communications 90
Communications beyond Normal Channels 91

The Importance of COSO Information and Communication ... 91
Review Questions ... 92
Review Answers ... 93

Chapter 8 – COSO Internal Control Components: Monitoring Activities ... 95
Learning Objectives ... 95
Introduction ... 95
Importance of COSO Monitoring Internal Control Activities ... 95
COSO Monitoring Principle 1: Conduct Ongoing and Separate Evaluations ... 97
Ongoing Evaluation Processes ... 98
Separate Monitoring Evaluations ... 99
COSO Monitoring Principle 2: Evaluate and Communicate Deficiencies ... 101
Communication of Monitoring Findings ... 101
Reporting to Senior Management and the Board of Directors ... 102
COSO Internal Control Monitoring in Perspective ... 102
Review Questions ... 104
Review Answers ... 105

Chapter 9 – COSO Internal Control GRC Operations Controls ... 107
Learning Objectives ... 107
Introduction ... 107
COSO Operations Objectives ... 107
Planning and Budgeting Operations Controls ... 108
Operations Goals ... 109
Budgeting and Budget Performance Monitoring ... 110
IT Systems Operations Controls ... 111
IT Policy and Governance Controls ... 112
IT Standards ... 113
IT Management and Organization Controls ... 114
IT Physical and Environmental Controls ... 115
IT Systems Software Controls ... 116
IT System Development and Application Controls ... 117
Operations Procedure Controls and Service Catalogs ... 119
Importance of COSO Operations Controls ... 120
Review Questions ... 121
Review Answers ... 122

Chapter 10 – COSO Reporting Processes ... 123
Learning Objectives ... 123
Introduction ... 123
COSO Reporting Objectives ... 123
COSO External Financial Reporting Controls ... 124
COSO Internal Financial Reporting Controls ... 126
Document Imaging ... 127
Document and Report Library Services ... 128
Reporting Control Workflow Technologies ... 129
Document Forms Processing Internal Controls ... 129
Application Records Management Reporting Controls ... 131
COSO External Nonfinancial Reporting Controls ... 131
COSO Internal Nonfinancial Reporting Controls ... 132
Importance of COSO Reporting Controls ... 133
Review Questions ... 134
Review Answers ... 135

Chapter 11 – COSO Legal, Regulatory, and Compliance Objectives ... 136
Learning Objectives ... 136

Introduction ... 136
Importance of Enterprise Compliance Controls ... 136
Regulatory Compliance Control Issues ... 137
Internal Controls and Legal Issues ... 139
Compliance with Professional and Other Standards ... 139
Review Questions ... 141
Review Answers ... 142

Chapter 12 – Internal Control Entity and Organizational GRC Relationships ... 143
Learning Objectives ... 143
Introduction ... 143
Internal Controls from an Organizational GRC Perspective ... 143
Enterprise Governance Overall Concepts ... 144
Enterprise Governance and Internal Controls ... 146
GRC Risk Management Components ... 146
Business Entity–Level Internal Controls ... 148
The Importance of the Tone at the Top ... 148
Mission Statements ... 149
Enterprise-Wide Codes of Conduct ... 151
Divisional and Functional Unit Internal Controls ... 153
Department- and Unit-Level Internal Controls ... 155
Organization and GRC Controls In Perspective ... 156
Review Questions ... 158
Review Answers ... 159

Chapter 13 – COSO, Service Management, and Effective IT Controls ... 161
Learning Objectives ... 161
Introduction ... 161
Importance of IT General Controls ... 161
IT Governance General Controls ... 163
IT Management General Controls ... 163
IT Standards ... 163
IT Organization and Management ... 164
IT Physical and Environmental System General Controls ... 165
Client-Server and Smaller Systems General IT Controls ... 166
ITIL Service Management Best Practices ... 169
Financial Management for IT Services ... 171
Service Delivery Service Level Management ... 172
Service Delivery Capacity Management ... 173
Service Delivery Availability Management ... 174
Service Delivery Best Practices ... 175
Review Questions ... 177
Review Answers ... 178

Chapter 14 – Cloud Computing, Virtualization, and Wireless Networks ... 179
Learning Objectives ... 179
Introduction ... 179
Internal Controls for IT Wireless Networks ... 180
Key Components of an IT Wireless System ... 181
Wireless Network Security Concerns ... 182
Cloud Computing and COSO Internal Controls ... 183
Reviewing Cloud Computing Application Controls ... 184
Cloud Computing Security and Privacy Challenges ... 186
Storage Management Virtualization ... 187
COSO Internal Controls And Newer Technologies ... 188
Review Questions ... 189

Review Answers ... 190

Chapter 15 – Another Framework: COSO ERM ... 191
Learning Objectives ... 191
Introduction ... 191
ERM Definitions and the ERM Portfolio View of Risk ... 191
The COSO ERM Framework Model ... 194
COSO ERM Components: Internal Environment ... 195
COSO ERM Components: Objective Setting ... 197
COSO ERM Components: Event Identification ... 198
COSO ERM: Risk Assessment Components ... 199
COSO ERM Components: Risk Response ... 200
COSO ERM Components: Control Activities ... 203
COSO ERM Components: Information and Communication ... 205
COSO ERM Components: Monitoring ... 207
Other Dimensions of the ERM Framework ... 208
COSO ERM and the Revised Internal Control Framework ... 208
Review Questions ... 210
Review Answers ... 211

Chapter 16 – Understanding and Using COBIT ... 212
Learning Objectives ... 212
Introduction ... 212
An Executive's Introduction to COBIT ... 213
COBIT Principle 1: Meeting Stakeholder Needs ... 213
COBIT Principle 2: Covering the Enterprise End to End ... 214
COBIT Principle 3: Applying a Single Integrated Architecture Framework ... 215
COBIT Principle 4: Enabling a Holistic Approach ... 217
COBIT Principle 5: Separating Governance from Management ... 219
Using COBIT to Assess Enterprise Internal Controls ... 219
Mapping COBIT to COSO Internal Controls ... 222
Review Questions ... 223
Review Answers ... 224

Chapter 17 – ISO Internal Control and Risk Management Standards ... 225
Learning Objectives ... 225
Introduction ... 225
Background and Importance of ISO Standards in a Global Commerce World ... 225
ISO Standards Overview ... 227
ISO 9001 Quality Management Systems ... 227
ISO IT Security Standards: ISO 27002 ... 230
IT Security Technique Requirements: ISO 27001 ... 231
Service Quality Management: ISO 2000 ... 232
ISO Standards and the COSO Internal Control Framework ... 233
Review Questions ... 234
Review Answers ... 235

Chapter 18 – COSO Internal Controls in the Board Room ... 236
Learning Objectives ... 236
Introduction ... 236
Board Decisions and Internal Control Processes ... 237
Board Organization and Governance Rules ... 238
Corporate Charters and the Board Committee Structure ... 239
The Audit Committee and Managing Internal Controls ... 242
Board Member Internal Control Knowledge Requirements ... 243
COSO Internal Controls and Corporate Governance ... 244

Review Answers 190

Chapter 15 – Another Framework: COSO ERM 191
Learning Objectives 191
Introduction........ 191
ERM Definitions and the ERM Portfolio View of Risk 191
The COSO ERM Framework Model 194
COSO ERM Components: Internal Environment 195
COSO ERM Components: Objective Setting 197
COSO ERM Components: Event Identification 198
COSO ERM: Risk Assessment Components 199
COSO ERM Components: Risk Response 200
COSO ERM Components: Control Activities........ 203
COSO ERM Components: Information and Communication 205
COSO ERM Components: Monitoring 207
Other Dimensions of the ERM Framework 208
COSO ERM and the Revised Internal Control Framework........ 208
Review Questions........ 210
Review Answers 211

Chapter 16 – Understanding and Using COBIT........ 212
Learning Objectives 212
Introduction........ 212
An Executive's Introduction to COBIT 213
COBIT Principle 1: Meeting Stakeholder Needs 213
COBIT Principle 2: Covering the Enterprise End to End........ 214
COBIT Principle 3: Applying a Single Integrated Architecture Framework 215
COBIT Principle 4: Enabling a Holistic Approach........ 217
COBIT Principle 5: Separating Governance from Management 219
Using COBIT to Assess Enterprise Internal Controls 219
Mapping COBIT to COSO Internal Controls 222
Review Questions........ 223
Review Answers 224

Chapter 17 – ISO Internal Control and Risk Management Standards 225
Learning Objectives 225
Introduction........ 225
Background and Importance of ISO Standards in a Global Commerce World 225
ISO Standards Overview........ 227
ISO 9001 Quality Management Systems 227
ISO IT Security Standards: ISO 27002 230
IT Security Technique Requirements: ISO 27001 231
Service Quality Management: ISO 2000........ 232
ISO Standards and the COSO Internal Control Framework 233
Review Questions........ 234
Review Answers 235

Chapter 18 – COSO Internal Controls in the Board Room........ 236
Learning Objectives 236
Introduction........ 236
Board Decisions and Internal Control Processes........ 237
Board Organization and Governance Rules 238
Corporate Charters and the Board Committee Structure 239
The Audit Committee and Managing Internal Controls........ 242
Board Member Internal Control Knowledge Requirements 243
COSO Internal Controls and Corporate Governance 244

Review Questions 245
Review Answers 246

Chapter 19 – Service Organization Control Reports and COSO Internal Controls 247
Learning Objectives 247
Introduction 247
Importance of Service Organization Internal Controls 248
Early Steps to Gain Assurance: SAS 70 248
Service Organization Control (SOC) Reports 249
Right-To-Audit Clauses 250
Internal Control Limitations 252
Review Questions 254
Review Answers 255

Chapter 20 – Implementing the Revised COSO Internal Control Framework 256
Learning Objectives 256
Introduction 256
Understanding What Is New in the 2013 Framework 256
Transitioning to the New COSO Guidance 257
Steps To Begin Implementing the New COSO Internal Control Framework 258
Review Questions 259
Review Answers 260

Glossary 261
Index 265