

Internal Controls Toolkit

Christine H. Doxey

Table of Contents

Chapter 1 – Background on Internal Controls	1
Learning Objectives	1
The Goals and Challenges of Internal Controls	1
Risk-Based Internal Controls.....	1
Five Questions to Ask.....	2
Five Metrics to Consider	2
Application of Internal Controls.....	2
The Three Critical Corporate Controls.....	3
The Background and History of Internal Controls	4
Enterprise Risk Management (ERM) Integrated Framework—2004 And 2013	10
Example: Enterprise Risk Management (ERM) and the Application to the Procure to Pay (P2P) Cycle	10
An ERM Checklist.....	11
Internal Control over Financial Reporting—Guidance for Smaller Public Companies—2006	12
Guidance on Monitoring Internal Control Systems—2009.....	12
Definition and Objectives of Internal Controls.....	12
Types of Internal Controls and Control Mechanisms.....	13
Leveraging the Standards of Internal Control to Implement a Controls Self-Assessment (CSA) Program.....	14
Ethics and “Tone at the Top”.....	16
What is “tone at the top”?.....	16
What are the components of an effective ethics policy?.....	16
What are the components of a well-defined code of conduct?	17
What are examples of poor “tone at the top”?.....	17
Code of Conduct Considerations.....	17
Entity-Level Controls.....	18
Benefits for Entity-Level Controls	18
“Tone at the Top”	18
Roles and Responsibilities for Internal Control	19
Review Questions.....	23
Review Answers	25
Chapter 2 – The Order to Cash (O2C) Process	29
Learning Objectives	29
Introduction.....	29
Process Overview.....	29
Application of Internal Controls.....	29
Metrics.....	30
Sub-Processes	31
2.1 Order Entry/Edit	31
Introduction.....	31
Standard of Internal Control	31
Risk If Standard Is Not Implemented	32
2.2 Export Controls	33
Introduction.....	33
Application of Internal Controls.....	33
Standard of Internal Control	34
Risk If Standard Is Not Implemented	35
2.3 Sales Contracts	35
Introduction.....	35
Standard of Internal Control	36
Risk If Standard Is Not Implemented	36
2.4 Credit.....	36
Introduction.....	36

Table of Contents

Standard of Internal Control	37
Risk If Standard Is Not Implemented	37
2.5 Shipping	38
Introduction.....	38
Standard of Internal Control	38
Risk If Standard Is Not Implemented	39
2.6 Revenue Recognition/Billing.....	39
Introduction.....	39
Standard of Internal Control	40
Risk If Standard Is Not Implemented	42
2.7 Accounts Receivable (AR)	42
Introduction.....	42
Standard of Internal Control	43
2.8 Collection.....	44
Introduction.....	44
Standard of Internal Control	44
Risk If Standard Is Not Implemented	45
2.9 Cash Receipts and Application.....	45
Introduction.....	45
Standard of Internal Control	45
Risk If Standard Is Not Implemented	46
2.10 Price Establishment	46
Introduction.....	46
Standard of Internal Control	46
Risk If Standard Is Not Implemented	47
2.11 Promotional Activities.....	48
Introduction.....	48
Standard of Internal Control	48
Risk If Standard Is Not Implemented	49
Review Questions.....	50
Review Answers	51
Chapter 3 – Treasury Process.....	53
Learning Objectives	53
Introduction.....	53
Process Overview.....	53
Metrics.....	53
Application of Internal Controls.....	54
Sub-Processes	54
3.1 General Treasury Controls	54
Introduction.....	54
Standard of Internal Control	54
Risk If Standard Is Not Implemented	55
3.2 Financing Operations	56
Introduction.....	56
Standard of Internal Control	56
Risk If Standard Is Not Implemented	56
3.3 Investment of Available Funds	57
Introduction.....	57
Standard of Internal Control	57
Risk If Standard Is Not Implemented	57
3.4 Foreign Exchange.....	58
Introduction.....	58
Standard of Internal Control	58
Risk If Standard Is Not Implemented	58
Review Questions.....	59
Review Answers	60

Table of Contents

Chapter 4 – Procure to Pay (P2P) Process	61
Learning Objectives	61
Introduction.....	61
Consider Automation to Mitigate Risk in the P2P Process	61
Process Overview.....	63
Application of Internal Controls.....	64
Metrics.....	64
Sub-Processes	66
4.1 Supplier Selection and Management.....	66
Introduction.....	66
Standard of Internal Control	66
Risk If Standard Is Not Implemented.....	67
4.2 Purchasing/Ordering	67
Introduction.....	67
Standard of Internal Control	67
Risk If Standard Is Not Implemented	68
4.3 Import Controls	69
Introduction.....	69
Standard of Internal Control	69
Risk If Standard Is Not Implemented	70
4.4 Receiving.....	70
Introduction.....	70
Standard of Internal Control	70
Risk If Standard Is Not Implemented	71
4.5 Accounts Payable	72
Introduction.....	72
Standard of Internal Control	72
Risk If Standard Is Not Implemented	73
4.6 The Payment Process—General	74
Introduction.....	74
Standard of Internal Control	74
Risk If Standard Is Not Implemented	75
4.7 The Payment Process—Travel and Entertainment	76
Introduction.....	76
Standard of Internal Control	76
Risk If Standard Is Not Implemented	77
4.8 Research and Product Development.....	77
Introduction.....	77
Standard of Internal Control	77
Risk If Standard Is Not Implemented	78
4.9 Procurement Cards (P-Cards).....	78
Introduction.....	78
Standard of Internal Control	79
Risk If Standard Is Not Implemented	80
Review Questions.....	82
Review Answers	83
Chapter 5 – Hire to Retire (H2R) Process	85
Learning Objectives	85
Introduction.....	85
Process Overview.....	85
Metrics.....	85
Application of Internal Controls.....	86
The Health Insurance Portability and Accountability Act (HIPAA) Security Rule	87
Sub-Processes	87
5.1 Payroll Preparation and Security	87
Introduction.....	87

Table of Contents

Standard of Internal Control	87
Risk If Standard Is Not Implemented	88
5.2 Payroll Payment Controls.....	89
Introduction.....	89
Standard of Internal Control	89
Risk If Standard Is Not Implemented	90
5.3 Distribution of Payroll	90
Introduction.....	90
Standard of Internal Control	91
Risk If Standard Is Not Implemented	91
5.4 Compensation and Benefits	91
Introduction.....	91
Standard of Internal Control	91
Risk If Standard Is Not Implemented	92
5.5 Hiring and Termination.....	92
Introduction.....	92
Standard of Internal Control	92
Risk If Standard Is Not Implemented	93
5.6 Education, Training, and Development.....	93
Introduction.....	93
Standard of Internal Control	94
Risk If Standard Is Not Implemented	94
5.7 Contingent Workforce	94
Introduction.....	94
Standard of Internal Control	94
Risk If Standard Is Not Implemented	95
Review Questions.....	96
Review Answers	97
Chapter 6 – The Supply Chain Process	99
Learning Objectives	99
Introduction.....	99
Process Overview.....	99
Metrics.....	99
Application Of Internal Controls.....	100
Sub-Processes	100
6.1 Planning and Control.....	101
Introduction.....	101
Standard of Internal Control	101
Risk If Standard Is Not Implemented	101
6.2 Inventory Control.....	102
Introduction.....	102
Standard of Internal Control	102
Risk If Standard Is Not Implemented	103
6.3 Inventory Verification.....	104
Introduction.....	104
Standard of Internal Control	104
Risk If Standard Is Not Implemented	104
6.4 Inventory Valuation	104
Introduction.....	104
Standard of Internal Control	105
Risk If Standard Is Not Implemented	105
6.5 Product Cost Management.....	105
Introduction.....	105
Standard of Internal Control	105
Risk If Standard Is Not Implemented	106

Table of Contents

6.6 Original Equipment Manufacturers (OEMs)/Alliance Partners	107
Introduction.....	107
Standard of Internal Control	107
Risk If Standard Is Not Implemented	108
6.7 Supply Chain Security.....	108
Introduction.....	108
Standard of Internal Control	108
Risk If Standard Is Not Implemented	108
6.8 Transportation and Logistics	109
Introduction.....	109
Standard of Internal Control	109
Risk If Standard Is Not Implemented	110
Review Questions.....	111
Review Answers	112
Chapter 7 – Record to Report (R2R)	113
Learning Objectives	113
Introduction.....	113
Process Overview.....	113
Metrics.....	114
Differences Between IFRS And U.S. GAAP That Impact The R2R Process.....	114
Application of Internal Controls.....	115
Sub-Processes	115
7.1 International Transfer Pricing	115
Introduction.....	115
Standard of Internal Control	115
Risk If Standard Is Not Implemented	116
7.2 Intercompany Transactions	116
Introduction.....	116
Standard of Internal Control	116
Risk If Standard Is Not Implemented	116
Introduction.....	117
Standard of Internal Control	117
Risk If Standard Is Not Implemented	118
7.4 Processing and Reporting of Financial Information (The Final Mile).....	118
Introduction.....	118
Standard of Internal Control	118
Risk If Standard Is Not Implemented	120
7.5 Fixed Assets	120
Introduction.....	120
Standard of Internal Control	120
Risk If Standard Is Not Implemented	121
Review Questions.....	123
Review Answers	124
Chapter 8 – Government Contracts	125
Learning Objectives	125
Introduction.....	125
Application of Internal Controls.....	125
Process Overview.....	125
Metrics.....	125
Sub-Processes	126
8.1 U.S. Government Contracts—General.....	126
Introduction.....	126
Standard of Internal Control	126
Risk If Standard Is Not Implemented	129

Table of Contents

8.2 U.S. Government Contracts— Non-Commercial Products	129
Introduction.....	129
Standard of Internal Control	129
Risk If Standard Is Not Implemented	130
8.3 U.S. Government Contracts— Commercial Products.....	130
Introduction.....	130
Standard of Internal Control.....	130
Risk If Standard Is Not Implemented.....	131
8.4 Contracts with State and Local Governments and Educational Institutions Within the United States	132
Introduction.....	132
Standard of Internal Control	132
Risk If Standard Is Not Implemented.....	132
8.5 Contracts with Governments Outside the United States.....	132
Introduction.....	132
Standard of Internal Control	133
Risk If Standard Is Not Implemented	133
Review Questions.....	135
Review Answers	136
Chapter 9 – Records and Information Management	137
Learning Objectives	137
Introduction.....	137
Process Overview.....	137
Metrics.....	137
Application of Internal Control and Definitions	138
General Data Protection Regulation (GDPR).....	138
The Health Insurance Portability and Accountability Act (HIPAA).....	139
Sub-Processes	139
9.1 Standards of Internal Control Responsibilities.....	139
Standard of Internal Control	139
Risk If Standard Is Not Implemented	140
9.2 Standards of Internal Record-Keeping Requirements	140
Introduction.....	140
Standard of Internal Control	140
Risk If Standard Is Not Implemented	141
Review Questions.....	144
Review Answers	145
Chapter 10 – Computer, Telecommunications, and Systems Controls	147
Learning Objectives	147
Introduction.....	147
Process Overview.....	147
Metrics.....	148
Application of Internal Controls.....	149
SAE 18.....	149
Sub-Processes	149
10.1 Owners, Users, and Service Providers	150
Introduction.....	150
Definitions.....	150
Standard of Internal Control	150
Risk If Standard Is Not Implemented	152
10.2 Physical Security and Environmental Controls.....	153
Introduction.....	153
Standard of Internal Control	153
Risk If Standard Is Not Implemented	154

Table of Contents

10.3 Computer Access Control.....	154
Introduction.....	154
Definitions.....	155
Standard of Internal Control	155
Risk If Standard Is Not Implemented	159
10.4 Network Operations and Security Controls	160
Introduction.....	160
Definitions.....	160
Standard of Internal Control	160
Risk If Standard Is Not Implemented	162
10.5 Systems Development Methodology	162
Introduction.....	162
Standard of Internal Control	162
Risk If Standard Is Not Implemented	163
10.6 Change Management.....	164
Introduction.....	164
Definitions.....	164
Standard of Internal Control	164
Risk If Standard Is Not Implemented	165
10.7 Computer and Telecommunications Backup for Production Restart/Recovery	165
Introduction.....	165
Standard of Internal Control	166
Risk If Standard Is Not Implemented	166
10.8 Disaster Recovery and Business Contingency Planning	166
Introduction.....	166
Definitions.....	167
Standard of Internal Control	169
Risk If Standard Is Not Implemented	170
10.9 Input Controls	170
Introduction.....	170
Standard of Internal Control	170
Risk If Standard Is Not Implemented	171
10.10 Output Controls.....	171
Introduction.....	171
Standard of Internal Control	171
Risk If Standard Is Not Implemented	171
10.11 Paperless Transactions, Electronic Commerce, and EDI	172
Introduction.....	172
Definitions.....	172
Standard of Internal Control	172
Risk If Standard Is Not Implemented	173
10.12 Non-Company Networks and Bulletin Boards	173
Introduction.....	173
Vulnerability and Threat Management.....	174
Definitions.....	174
Standard of Internal Control	174
Risk If Standard Is Not Implemented	176
Review Questions.....	177
Review Answers	178
Chapter 11 – Protection of Assets: Human, Physical, and Intellectual.....	181
Learning Objectives	181
Introduction.....	181
Process overview.....	181
Metrics.....	181
Application of Internal Control	182
Sub-Processes	182

Table of Contents

11.1 Security Framework	182
Introduction.....	182
Standard of Internal Control	182
Risk If Standard Is Not Implemented	183
11.2 Perimeter Security.....	184
Introduction.....	184
Standard of Internal Control	184
Risk If Standard Is Not Implemented	185
11.3 Interior Security.....	185
Introduction.....	185
Standard of Internal Control	185
Risk If Standard Is Not Implemented	186
11.4 Protecting Intellectual Property.....	186
Introduction.....	186
Standard of Internal Control	187
Risk If Standard Is Not Implemented	187
Review Questions.....	188
Review Answers	189
Chapter 12 – The Insurance Process.....	191
Learning Objectives	191
Introduction.....	191
Process Overview.....	191
Metrics.....	191
Application of Internal Controls.....	192
Sub-Processes	192
12.1 Protection Against Physical Damage and Other Accidents	192
Introduction.....	192
Standard of Internal Control	192
Risk If Standard Is Not Implemented	192
12.2 Insurance (Property and Casualty Risks).....	192
Introduction.....	192
Standard of Internal Control	193
Risk If Standard Is Not Implemented	193
12.3 Business Continuity.....	193
Standard of Internal Control	193
Risk If Standard Is Not Implemented	194
Review Questions.....	195
Review Answers	196
Chapter 13 – Environmental, Health, and Safety (EH&S).....	197
Learning Objectives	197
Introduction.....	197
Process Overview.....	197
Metrics.....	197
Application of Internal Control	198
Sub-Processes	198
13.1 General Controls.....	198
Standard of Internal Control	198
Risk If Standard Is Not Implemented	199
Review Questions.....	200
Review Answers	201
Chapter 14 – Customer Services	203
Learning Objectives	203
Introduction.....	203
Process Overview.....	203

Table of Contents

Metrics.....	203
Application of Internal Control	204
Sub-Processes	204
14.1 Policy.....	204
Introduction.....	204
Standard of Internal Control	204
Risk If Standard Is Not Implemented	205
14.2 Call Center Management	205
Introduction.....	205
Standard of Internal Control	206
Risk If Standard Is Not Implemented	206
14.3 Warranty.....	207
Introduction.....	207
Standard of Internal Control	207
Risk If Standard Is Not Implemented	208
14.4 Support Sales	209
Introduction.....	209
Standard of Internal Control	209
Risk If Standard Is Not Implemented	209
Review Questions.....	210
Review Answers	211
Chapter 15 – Professional Services (PS).....	213
Learning Objectives	213
Introduction.....	213
Process Overview.....	213
Metrics.....	213
Application of Internal Controls.....	214
Sub-Processes	214
15.1 General Controls.....	214
Introduction.....	214
Standard of Internal Control	214
Risk If Standard Is Not Implemented	215
15.2 Opportunity-Bid Process	215
Introduction.....	215
Standard of Internal Control	215
Risk If Standard Is Not Implemented	216
15.3 Program Management.....	216
Introduction.....	216
Standard of Internal Control	216
Risk If Standard Is Not Implemented	219
15.4 Customer Order Management.....	219
Introduction.....	219
Standard of Internal Control	219
Risk If Standard Is Not Implemented	221
Review Questions.....	222
Review Answers	223
Chapter 16 – Entity-Level Controls.....	225
Learning Objectives	225
Introduction.....	225
Process Overview.....	225
Metrics.....	225
Application of Internal Controls.....	226
Sub-Processes	226
16.1 Compliance and Compliance Screening.....	226
Introduction.....	226

Table of Contents

Standard of Internal Control	227
Risk If Standard Is Not Implemented	228
16.2 Internal Controls Roles and Responsibilities	228
Introduction.....	228
Standard of Internal Control	228
Risk If Standard Is Not Implemented	229
16.3 Entity Management Controls	230
Introduction.....	230
Standard of Internal Control	230
Risk If Standard Is Not Implemented	230
16.4 Audit Committee Controls.....	231
Introduction.....	231
Standards of Internal Control	231
Risk If Standard Is Not Implemented	232
Review Questions	234
Review Answers	235
Addendum – Additional Tools	237
Glossary.....	259
Index	267