

# Contents

<b>Introduction to the Internal Controls Toolkit</b>	<b>1</b>
Introduction	1
General Standards of Internal Control	7
How This Toolkit Is Organized	8
<b>Chapter 1: Background on Internal Controls</b>	<b>11</b>
The Goals and Challenges of Internal Controls	11
Enterprise Risk Management (ERM) Integrated Framework—2004 and 2013	27
Leveraging the Standards of Internal Control to Implement a Controls Self-Assessment (CSA) Program	36
Ethics and “Tone at the Top”	38
Code of Conduct Considerations	41
Entity-Level Controls	41
Roles and Responsibilities for Internal Control	44
<b>Chapter 2: The Order to Cash (O2C) Process</b>	<b>49</b>
Introduction	49
Process Overview	49
Application of Internal Controls	51
Metrics	51
Sub-Processes	53
2.1 Order Entry/Edit	53
2.2 Export Controls	56
2.3 Sales Contracts	60
2.4 Credit	62
2.5 Shipping	64
2.6 Revenue Recognition/Billing	67
2.7 Accounts Receivable (AR)	72

2.8	Collection	75
2.9	Cash Receipts and Application	77
2.10	Price Establishment	79
2.11	Promotional Activities	81
<b>Chapter 3: Treasury Process</b>		<b>85</b>
	Introduction	85
	Process Overview	87
	Metrics	87
	Application of Internal Controls	87
	Sub-Processes	88
3.1	General Treasury Controls	88
3.2	Financing Operations	91
3.3	Investment of Available Funds	92
3.4	Foreign Exchange	94
<b>Chapter 4: Procure to Pay (P2P) Process</b>		<b>97</b>
	Introduction	97
	Consider Automation to Mitigate Risk in the P2P Process	97
	Process Overview	103
	Application of Internal Controls	103
	Metrics	103
	Sub-Processes	106
4.1	Supplier Selection and Management	106
4.2	Purchasing/Ordering	108
4.3	Import Controls	111
4.4	Receiving	113
4.5	Accounts Payable	116
4.6	The Payment Process—General	119
4.7	The Payment Process—Travel and Entertainment	123
4.8	Research and Product Development	125
4.9	Procurement Cards (P-Cards)	127
<b>Chapter 5: Hire to Retire (H2R) Process</b>		<b>133</b>
	Introduction	133
	Process Overview	135
	Metrics	135
	Application of Internal Controls	136
	The Health Insurance Portability and Accountability Act (HIPAA) Security Rule	137
	Sub-Processes	137

5.1 Payroll Preparation and Security	138
5.2 Payroll Payment Controls	141
5.3 Distribution of Payroll	144
5.4 Compensation and Benefits	145
5.5 Hiring and Termination	147
5.6 Education, Training, and Development	149
5.7 Contingent Workforce	149

## **Chapter 6: The Supply Chain Process** **153**

Introduction	153
Process Overview	155
Metrics	155
Application of Internal Controls	156
Sub-Processes	156
6.1 Planning and Control	157
6.2 Inventory Control	159
6.3 Inventory Verification	162
6.4 Inventory Valuation	163
6.5 Product Cost Management	164
6.6 Original Equipment Manufacturers (OEMs)/Alliance Partners	167
6.7 Supply Chain Security	169
6.8 Transportation and Logistics	170

## **Chapter 7: Record to Report (R2R)** **173**

Introduction	173
Process Overview	175
Metrics	175
Differences Between IFRS and U.S. GAAP That Impact the R2R Process	176
Application of Internal Controls	177
Sub-Processes	177
7.1 International Transfer Pricing	177
7.2 Intercompany Transactions	178
7.3 Accumulation of Financial Information	180
7.4 Processing and Reporting of Financial Information (the Final Mile)	182
7.5 Fixed Assets	186

## **Chapter 8: Government Contracts** **189**

Introduction	189
Application of Internal Controls	189
Process Overview	189

Metrics	191
Sub-Processes	191
8.1 U.S. Government Contracts—General	191
8.2 U.S. Government Contracts—Non-Commercial Products	197
8.3 U.S. Government Contracts—Commercial Products	199
8.4 Contracts with State and Local Governments and Educational Institutions Within the United States	202
8.5 Contracts with Governments Outside the United States	203

## **Chapter 9: Records and Information Management** **207**

Introduction	207
Process Overview	207
Metrics	209
Application of Internal Control and Definitions	209
General Data Protection Regulation (GDPR)	210
The Health Insurance Portability and Accountability Act (HIPAA)	211
Sub-Processes	211
9.1 Standards of Internal Control Responsibilities	211
9.2 Standards of Internal Record-Keeping Requirements	214

## **Chapter 10: Computer, Telecommunications, and Systems Controls** **219**

Introduction	219
Process Overview	221
Metrics	221
Application of Internal Controls	223
SAE 18	223
Sub-Processes	224
10.1 Owners, Users, and Service Providers	224
10.2 Physical Security and Environmental Controls	229
10.3 Computer Access Control	232
10.4 Network Operations and Security Controls	242
10.5 Systems Development Methodology	245
10.6 Change Management	248
10.7 Computer and Telecommunications Backup for Production Restart/Recovery	251
10.8 Disaster Recovery and Business Contingency Planning	252
10.9 Input Controls	259
10.10 Output Controls	260
10.11 Paperless Transactions, Electronic Commerce, and EDI	261
10.12 Non-Company Networks and Bulletin Boards	264

<b>Chapter 11: Protection of Assets: Human, Physical, and Intellectual</b>	<b>271</b>
Introduction	271
Process Overview	271
Metrics	273
Application of Internal Control	273
Sub-Processes	274
11.1 Security Framework	274
11.2 Perimeter Security	276
11.3 Interior Security	279
11.4 Protecting Intellectual Property	281
<b>Chapter 12: The Insurance Process</b>	<b>285</b>
Introduction	285
Process Overview	285
Metrics	285
Application of Internal Controls	287
Sub-processes	287
12.1 Protection Against Physical Damage and Other Accidents	287
12.2 Insurance (Property and Casualty Risks)	288
12.3 Business Continuity	290
<b>Chapter 13: Environmental, Health, and Safety (EH&amp;S)</b>	<b>291</b>
Introduction	291
Process Overview	291
Metrics	293
Application of Internal Control	293
Sub-Processes	293
13.1 General Controls	294
<b>Chapter 14: Customer Services</b>	<b>297</b>
Introduction	297
Process Overview	297
Metrics	297
Application of Internal Control	299
Sub-Processes	299
14.1 Policy	300
14.2 Call Center Management	302
14.3 Warranty	304
14.4 Support Sales	307

<b>Chapter 15: Professional Services (PS)</b>	<b>309</b>
Introduction	309
Process Overview	309
Metrics	311
Application of Internal Controls	311
Sub-Processes	312
15.1 General Controls	312
15.2 Opportunity-Bid Process	313
15.3 Program Management	316
15.4 Customer Order Management	321
<b>Chapter 16: Entity-Level Controls</b>	<b>325</b>
Introduction	325
Process Overview	325
Metrics	327
Application of Internal Controls	327
Sub-Processes	328
16.1 Compliance and Compliance Screening	328
16.2 Internal Controls Roles and Responsibilities	331
16.3 Entity Management Controls	334
16.4 Audit Committee Controls	335
<b>Glossary</b>	<b>341</b>
<b>Addendum—Additional Tools</b>	<b>353</b>
<b>Index</b>	<b>385</b>