Contents

Preface xi
Acknowledgments xv

Chapter 1: What We All Share 1
   Need for Control Criteria 1
   Overview of the COSO Internal Control Integrated Framework 2
   Holistic, Integrated View 3
   Revised COSO Internal Controls Framework 6
   What We Must Do 8
   Basic Scoping and Strategies for Maintenance 11
   Where We Depart 12
   Triangle of Efficiency 13
   Controls versus Processes 14
   The Debate Continues 18
   Organization of This Book 18

Appendix 1A: COSO 17 Principles 20

Chapter 2: Setting the Scope of Your Documentation Project: Identifying the Core 21
   Start with Business Objectives 21
   After the Initial Year 24
   Mapping the Entity to the Financial Statements: Ins and Outs 25
   Consider Risks, Not Just Quantitative Measures 27
   Inherent and Control Risk 28
   Overstatement and Understatement 28
   Does “In Scope” Imply Extensive Testing? 37
   A Consolation 39
   Be Careful Out There! 40

Appendix 2A: Summary of Scoping Inquiries 42
### Chapter 3: The Risk Assessment Component

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment Principles in COSO</td>
<td>46</td>
</tr>
<tr>
<td>Cost Control</td>
<td>46</td>
</tr>
<tr>
<td>Basics</td>
<td>47</td>
</tr>
<tr>
<td>Likelihood, Magnitude, Velocity, and Persistence</td>
<td>48</td>
</tr>
<tr>
<td>Separate Assessments of Inherent and Control Risks</td>
<td>50</td>
</tr>
<tr>
<td>Role of Assertions</td>
<td>51</td>
</tr>
<tr>
<td>Assertions</td>
<td>52</td>
</tr>
<tr>
<td>Principles 6 and 7: Specify Suitable Objectives; Identify and Analyze</td>
<td>56</td>
</tr>
<tr>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Identifying Risks</td>
<td>59</td>
</tr>
<tr>
<td>External Sources of Risk Information</td>
<td>60</td>
</tr>
<tr>
<td>Internal and External Reporting Risks</td>
<td>61</td>
</tr>
<tr>
<td>Compliance Risks</td>
<td>61</td>
</tr>
<tr>
<td>Disclosed Material Weaknesses in Risk Assessment</td>
<td>62</td>
</tr>
<tr>
<td>Principle 8: Assess Fraud Risk</td>
<td>62</td>
</tr>
<tr>
<td>Auditor Responsibility to Detect Fraud</td>
<td>65</td>
</tr>
<tr>
<td>Antifraud Controls for Management to Consider</td>
<td>66</td>
</tr>
<tr>
<td>Ties to Other Principles and Components</td>
<td>66</td>
</tr>
<tr>
<td>Principle 9: Identify and Assess Significant Change</td>
<td>66</td>
</tr>
<tr>
<td>Gathering Information to Support the Risk Assessment and Consider Change</td>
<td>68</td>
</tr>
</tbody>
</table>

### Appendix 3A: SAS No. 99 Exhibit: Management Antifraud Programs and Controls

<table>
<thead>
<tr>
<th>Attachment</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA “CPA’s Handbook of Fraud and Commercial Crime Prevention” Code of Conduct</td>
<td>87</td>
</tr>
<tr>
<td>Financial Executives International Code of Ethics Statement</td>
<td>91</td>
</tr>
</tbody>
</table>

### Appendix 3B: Understanding Fraud Risk Assessment

<table>
<thead>
<tr>
<th>Chapter 4: Control Environment</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1: Commitment to Integrity and Ethical Values</td>
<td>100</td>
</tr>
<tr>
<td>Principle 2: Board of Directors (Governance) Demonstrates Independence</td>
<td>104</td>
</tr>
<tr>
<td>from Management and Exercises of the Development and Performance of the</td>
<td></td>
</tr>
<tr>
<td>Internal Control</td>
<td></td>
</tr>
<tr>
<td>Principle 3: Management Establishes, with Board Oversight, Structures,</td>
<td>109</td>
</tr>
<tr>
<td>Reporting Lines, and Appropriate Authorities and Responsibilities in the</td>
<td></td>
</tr>
<tr>
<td>Pursuit of Objectives</td>
<td></td>
</tr>
</tbody>
</table>
Principle 4: Commitment to Attract, Develop, and Retain Competent Individuals in Alignment with Objectives 110
Principle 5: The Organization Holds Individuals Accountable for Their Internal Control Responsibilities in the Pursuit of Objectives 113
Appendix 4A: Understanding and Awareness of Control Responsibilities 117

Chapter 5: Control Activities 120
Principle 10: Selects and Develops Control Activities to Mitigate Risk and Achieve Objectives 120
Principle 11: Selects and Develops General Controls over Technology 132
Principle 12: Deploys through Policies and Procedures 141
Summing Up 143
Appendix 5A: Linking Common Control Activities and Assertions 146
Appendix 5B: Linkage of Principles to Controls, Policies, and Procedures 158

Chapter 6: Information and Communication 165
Principle 13: Generates Relevant Information 166
Principle 14: Communicates Internally 168
Principle 15: CommunicatesExternally 170

Chapter 7: Monitoring 173
Principle 16: Select, Develop, and Perform Ongoing and/or Separate Evaluations 174
Principle 17: Evaluate and Communicate Deficiencies as Appropriate 176

Chapter 8: Evidence and Testing 179
Sufficient Evidence 179
Gathering Information 187
Testing and Sampling 194
Nonsampling Situations 202
Confusion of Sample Size Guidance in Practice Today 203
Information Technology General Controls 204
Testing Security and Access 205
Appendix 8A: Sample Size Tutorial 211
Contents

Chapter 9: Developing Questionnaires and Conducting Interviews 217
   Surveys of Employees 219
   Conducting Interviews 224
   Management Inquiries: Sample Questions 234
Appendix 9A: Sample Practice Aids 239

Chapter 10: Assessing the Severity of Identified Controls Deficiencies 248
   It's Inevitable 248
   Alignment of Public and Private Company Standards for Assessing Deficiency Severity 251
   Control Deficiencies and Definitions 252
   Key Factors When Assessing the Severity of a Deficiency 263
   Conditions Indicating Control Deficiencies 270
   Examples of Evaluating the Severity of Deficiencies 277
   Overall Assessment 281
Appendix 10A: A Framework for Evaluating Control Exceptions and Deficiencies 283
Appendix 10B: Assessing the Potential Magnitude of a Control Deficiency 299

Chapter 11: Reporting Requirements 302
   Nonpublic Entity Reporting 302
   Public Company Annual and Quarterly Reporting Requirements 304
   Reporting on Management’s Responsibilities for Internal Control 309
   Required Company and Auditor Communications 312
   Reporting the Remediation of Weaknesses 314
   Coordinating with the Independent Auditors and Legal Counsel 315
Appendix 11A: Illustrative AICPA Report on Internal Controls 316

Chapter 12: Project Management and Tools Assessment Design 318
   Project Management 318
   Structuring the Project Team 319
   Tools Assessment Design 325
   Features of a Good Tools Solution 326
   Value of a Pilot Project 331
   Coordinating with the Independent Auditors 334
Chapter 13: Illustrative Forms and Templates 337
   Historical Perspective 338
   2013 Framework Examples 340
Appendix 13A: Information-Gathering Form—Principle Focused 348
Appendix 13B: Information Gathering Form—Revenue 350
Appendix 13C: Walk-through Documentation Form 353
Appendix 13D: Information Technology General Controls Assessment Form 355
Appendix 13E: Documentation of Financial Reporting Software and Spreadsheets 364
Appendix 13F: Sampling Form for Tests of Controls 368
Appendix 13G: Summary of Internal Control Deficiencies 371
Appendix 13H: Control Environment Component Evaluation Summary 372

Chapter 14: Summing Up 373

About the Author 375

Index 377