Contents

Preface xi

CHAPTER 1
Introduction: Sarbanes-Oxley and Establishing Effective Internal Controls 1

Changes Since SOx Was FirstIntroduced 3
Converging Trends: ITIL, CobiT, and Others 7

CHAPTER 2
Sarbanes-Oxley Act Today: Changing Perspectives 13

Sarbanes-Oxley Act: Key Elements 14
Impact of the Sarbanes-Oxley Act 51

CHAPTER 3
AS5 Standards for Auditing Internal Controls 53

AS5 Objectives 54
Reviewing Section 404 Internal Controls Under AS5:
Introduction 57
Planning the SOx AS5 Audit 59
AS5’s Top-Down Approach 66
Testing Internal Controls 72
Evaluating Identified Audit Deficiencies 75
Wrapping Up the AS5 Audit 76
Reporting on AS5 Audit Internal Controls 78
Improving Internal Controls Using AS5 Guidance 79
Going Forward: Potential Risks and Rewards 80

CHAPTER 4
Establishing Internal Controls Through COSO 83

Importance of Effective Internal Controls 84
Internal Control Standards: Background 86
## CONTENTS

- Events Leading to the Treadway Commission 90
- COSO Internal Control Framework 94
- Other Dimensions of the COSO Internal Control Framework 116

### CHAPTER 5
**Using CobiT Framework to Improve SOx Controls and Governance** 119
- CobiT Framework 122
- Using CobiT to Assess Internal Controls 127
- CobiT and Sarbanes-Oxley 141

### CHAPTER 6
**Performing Section 404 Reviews Under AS5: An Ongoing Process** 149
- SOx Section 404 Assessments of Internal Controls Today 150
- SOx Section 404 Requirements 152
- Section 404 Filing Rules: Changing Deadlines for Eligibility 168
- Gaps and Compliance Committees Under Today’s SOx Rules 173
- Documenting Internal Controls Going Forward 178
- Control Objectives and Risks Under Section 404 180

### CHAPTER 7
**Other SOx Requirements: Sections 302, 409, and Others** 183
- Other Important SOx Compliance Rules 184
- Section 302: Management’s Financial Report Responsibilities 184
- Section 401: Off-Balance Sheet Disclosures 188
- Section 409: Disclosures on Financial Conditions and Operations 190
- Section 802: Penalties for Altering Documents 192
- Section 806: Whistleblower Provisions 193
- Keeping SOx Rules in Focus 201

### CHAPTER 8
**Using ITIL to Align IT with Business Processes** 203
- Importance of the Information Technology Infrastructure 204
- ITIL Framework 206
- ITIL Service Delivery Best Practices 208
- ITIL Service Support Best Practices 221
- Security Management 237
- Linking ITIL with CobiT and SOx Internal Controls 239
CHAPTER 9
Importance of Enterprise Risk Management 241
  Importance of Risk Management 243
  COSO ERM Framework 247
  Other Dimensions of the COSO ERM Framework 270
  Putting It All Together 280
  Auditing COSO ERM Processes 281
  COSO ERM in Perspective 282

CHAPTER 10
International Standards: ISO, Quality Auditing, and SOx 285
  Importance of ISO Standards in Today’s Global World 286
  ISO Standards Overview 289
  Quality Audit Process 301
  IFAC International Accounting Standards 310

CHAPTER 11
Internal Audit in a Sarbanes-Oxley Environment 315
  Profession of Internal Auditing 316
  Internal Audit Professional Standards 322
  CBOK: Internal Audit’s Common Body of Knowledge 341

CHAPTER 12
Importance of Effective Corporate Governance 351
  Reporting Whistleblower Incidents: Establishing a Hotline Facility 352
  Building an Enterprise-Wide Ethical Culture 356
  Chief Compliance Officer Roles and Responsibilities 361
  Board of Directors and the Audit Committee 364
  Assessing SOx Internal Controls 366

Index 369