

Contents

Introduction xiii

PART ONE: AUDITING INTERNAL CONTROLS IN AN IT ENVIRONMENT	1
Chapter 1: SOx and the COSO Internal Controls Framework	3
Roles and Responsibilities of IT Auditors	4
Importance of Effective Internal Controls and COSO	6
COSO Internal Control Systems Monitoring Guidance	21
Sarbanes-Oxley Act	22
Wrapping It Up: COSO Internal Controls and SOx	31
Notes	31
Chapter 2: Using CobiT to Perform IT Audits	32
Introduction to CobiT	33
CobiT Framework	35
Using CobiT to Assess Internal Controls	39
Using CobiT in a SOx Environment	51
CobiT Assurance Framework Guidance	54
CobiT in Perspective	55
Notes	55
Chapter 3: IIA and ISACA Standards for the Professional Practice of Internal Auditing	57
Internal Auditing's International Professional Practice Standards	58
Content of the IPPF and the IIA International Standards	61
Strongly Recommended IIA Standards Guidance	75
ISACA IT Auditing Standards Overview	76
Codes of Ethics: The IIA and ISACA	79
Notes	81
Chapter 4: Understanding Risk Management Through COSO ERM	82
Risk Management Fundamentals	83
Quantitative Risk Analysis Techniques	92
IIA and ISACA Risk Management Internal Audit Guidance	94
COSO ERM: Enterprise Risk Management	97

viii ■ Contents

IT Audit Risk and COSO ERM	113
Notes	115
Chapter 5: Performing Effective IT Audits	117
IT Audit and the Enterprise Internal Audit Function	118
Organizing and Planning IT Audits	122
Developing and Preparing Audit Programs	127
Gathering Audit Evidence and Testing Results	132
Workpapers and Reporting IT Audit Results	142
Preparing Effective IT Audits	148
Notes	149
PART TWO: AUDITING IT GENERAL CONTROLS	151
Chapter 6: General Controls in Today's IT Environments	153
Importance of IT General Controls	154
IT Governance General Controls	157
IT Management General Controls	158
IT Technical Environment General Controls	174
Note	174
Chapter 7: Infrastructure Controls and ITIL Service Management Best Practices	175
ITIL Service Management Best Practices	176
ITIL's Service Strategies Component	179
ITIL Service Design	181
ITIL Service Transition Management Processes	189
ITIL Service Operation Processes	194
Service Delivery Best Practices	198
Auditing IT Infrastructure Management	199
Note	200
Chapter 8: Systems Software and IT Operations General Controls	201
IT Operating System Fundamentals	202
Features of a Computer Operating System	206
Other Systems Software Tools	209
Chapter 9: Evolving Control Issues: Wireless Networks, Cloud Computing, and Virtualization	214
Understanding and Auditing IT Wireless Networks	215
Understanding Cloud Computing	220
Storage Management Virtualization	225
PART THREE: AUDITING AND TESTING IT APPLICATION CONTROLS	227
Chapter 10: Selecting, Testing, and Auditing IT Applications	229
IT Application Control Elements	230
Selecting Applications for IT Audit Reviews	239

Performing an Applications Controls Review: Preliminary Steps	242
Completing the IT Applications Controls Audit	249
Application Review Case Study: Client-Server Budgeting System	255
Auditing Applications under Development	258
Importance of Reviewing IT Application Controls	266
Notes	266
Chapter 11: Software Engineering and CMMi	267
Software Engineering Concepts	267
CMMi: Capability Maturity Model for Integration	269
CMMi Benefits	280
IT Audit, Internal Control, and CMMi	281
Note	282
Chapter 12: Auditing Service-Oriented Architectures and Record Management Processes	283
Service-Oriented Computing and Service-Driven Applications	284
IT Auditing in SOA Environments	294
Electronic Records Management Internal Control Issues and Risks	300
IT Audits of Electronic Records Management Processes	301
Notes	303
Chapter 13: Computer-Assisted Audit Tools and Techniques	304
Understanding Computer-Assisted Audit Tools and Techniques	305
Determining the Need for CAATTs	308
CAATT Software Tools	311
Steps to Building Effective CAATTs	326
Importance of CAATTs for Audit Evidence Gathering	327
Chapter 14: Continuous Assurance Auditing, OLAP, and XBRL	329
Implementing Continuous Assurance Auditing	330
Benefits of Continuous Assurance Auditing Tools	338
Data Warehouses, Data Mining, and OLAP	339
XBRL: The Internet-Based Extensible Markup Language	346
Newer Technologies, the Continuous Close, and IT Audit	351
Notes	351
PART FOUR: IMPORTANCE OF IT GOVERNANCE	353
Chapter 15: IT Controls and the Audit Committee	355
Role of the Audit Committee for IT Auditors	356
Audit Committee Approval of Internal Audit Plans and Budgets	357
Audit Committee Briefings on IT Audit Issues	359
Audit Committee Review and Action on Significant IT Audit Findings	360
IT Audit and the Audit Committee	362
Chapter 16: Val IT, Portfolio Management, and Project Management	363
Val IT: Enhancing the Value of IT Investments	364
IT Systems Portfolio and Program Management	371

x ■ Contents

Project Management for IT Auditors	374
Notes	383
Chapter 17: Compliance with IT-Related Laws and Regulations	384
Computer Fraud and Abuse Act	386
Computer Security Act of 1987	387
Gramm-Leach-Bliley Act	390
HIPAA: Healthcare and Much More	395
Other Personal Privacy and Security Legislative Requirements	403
IT-Related Laws, Regulations, and Audit Standards	404
Chapter 18: Understanding and Reviewing Compliance with ISO Standards	407
Background and Importance of ISO Standards in a World of Global Commerce	408
ISO Standards Overview	410
ISO 19011 Quality Management Systems Auditing	419
ISO Standards and IT Auditors	421
Notes	421
Chapter 19: Controls to Establish an Effective IT Security Environment	422
Generally Accepted Security Standards	423
Effective IT Perimeter Security	429
Establishing an Effective, Enterprise-Wide Security Strategy	430
Best Practices for IT Audit and Security	432
Notes	433
Chapter 20: Cybersecurity and Privacy Controls	434
IT Network Security Fundamentals	435
IT Systems Privacy Concerns	443
PCI-DSS Fundamentals	446
Auditing IT Security and Privacy	447
Security and Privacy in the Internal Audit Department	448
Notes	453
Chapter 21: IT Fraud Detection and Prevention	454
Understanding and Recognizing Fraud in an IT Environment	455
Red Flags: Fraud Detection Signs for IT and Other Internal Auditors	456
Public Accounting's Role in Fraud Detection	461
IIA Standards and ISACA Materials for Detecting and Investigating Fraud	462
IT Audit Fraud Risk Assessments	464
IT Audit Fraud Investigations	467

IT Fraud Prevention Processes	468
Fraud Detection and the IT Auditor	471
Notes	471
Chapter 22: Identity and Access Management	472
Importance of Identity and Access Management	473
Identity Management Processes	474
Separation of Duties Identify Management Controls	477
Access Management Provisioning	478
Authentication and Authorization	479
Auditing Identity and Access Management Processes	481
Note	485
Chapter 23: Establishing Effective IT Disaster Recovery Processes	486
IT Disaster and Business Continuity Planning Today	487
Building and Auditing an IT Disaster Recovery Plan	489
Building the IT Disaster Recovery Plan	497
Disaster Recovery Planning and Service Level Agreements	503
Newer Disaster Recovery Plan Technologies: Data Mirroring Techniques	505
Auditing Business Continuity Plans	506
Disaster Recovery and Business Continuity Planning Going Forward	508
Notes	508
Chapter 24: Electronic Archiving and Data Retention	509
Elements of a Successful Electronic Records Management Process	510
Electronic Documentation Standards	516
Implementing Electronic IT Data Archiving	517
Auditing Electronic Document Retention and Archival Processes	519
Chapter 25: Business Continuity Management, BS 25999, and ISO 27001	521
IT Business Continuity Management Planning Needs Today	522
BS 25999 Good Practice Guidelines	524
Auditing BCM Processes	540
Linking the BCM with Other Standards and Processes	543
Notes	543
Chapter 26: Auditing Telecommunications and IT Communications Networks	544
Network Security Concepts	545
Effective IT Network Security Controls	549
Auditing a VPN Installation	555
Note	557

Chapter 27: Change and Patch Management Controls	558
IT Change Management Processes	559
Auditing IT Change and Patch Management Controls	573
Notes	576
Chapter 28: Six Sigma and Lean Technologies	577
Six Sigma Background and Concepts	578
Implementing Six Sigma	580
Lean Six Sigma	587
Notes	590
Chapter 29: Building an Effective IT Internal Audit Function	591
Establishing an IT Internal Audit Function	592
Internal Audit Charter: An Important IT Audit Authorization	593
Role of the Chief Audit Executive	595
IT Audit Specialists	596
IT Audit Managers and Supervisors	598
Internal and IT Audit Policies and Procedures	599
Organizing an Effective IT Audit Function	601
Importance of a Strong IT Audit Function	604
Note	605
Chapter 30: Professional Certifications: CISA, CIA, and More	606
Certified Information Systems Auditor Credentials	607
Certified Information Security Manager Credentials	609
Certificate in the Governance of Enterprise IT	611
Certified Internal Auditor Responsibilities and Requirements	612
Beyond the CIA: Other ITA Certifications	623
CISSP Information Systems Security Professional Certification	628
Certified Fraud Examiner Certification	628
ASQ Internal Audit Certifications	629
Other Internal Auditor Certifications	630
Note	631
Chapter 31: Quality Assurance Auditing and ASQ Standards	632
Duties and Responsibilities of Quality Auditors	633
Role of the Quality Auditor	635
Performing ASQ Quality Audits	638
Quality Assurance Reviews of IT Audit Functions	641
Future Directions for Quality Assurance Auditing	647
Notes	648
Index	649