## Preface  xvii

### PART I: IT AUDIT PROCESS  1

#### Chapter 1: Technology and Audit  3

- Technology and Audit  4
- Batch and Online Systems  8
- Electronic Data Interchange  20
- Electronic Business  21
- Cloud Computing  22

#### Chapter 2: IT Audit Function Knowledge  25

- Information Technology Auditing  25
- What Is Management?  26
- Management Process  26
- Understanding the Organization’s Business  27
- Establishing the Needs  27
- Identifying Key Activities  27
- Establish Performance Objectives  27
- Decide the Control Strategies  27
- Implement and Monitor the Controls  28
- Executive Management’s Responsibility and Corporate Governance  28
- Audit Role  28
- Conceptual Foundation  29
- Professionalism within the IT Auditing Function  29
- Relationship of Internal IT Audit to the External Auditor  30
- Relationship of IT Audit to Other Company Audit Activities  30
- Audit Charter  30
- Charter Content  30
- Outsourcing the IT Audit Activity  31
- Regulation, Control, and Standards  31
## Chapter 3: IT Risk and Fundamental Auditing Concepts

- Computer Risks and Exposures
- Effect of Risk
- Audit and Risk
- Audit Evidence
- Conducting an IT Risk-Assessment Process
- NIST SP 800 30 Framework
- ISO 27005
- The “Cascarino Cube”
- Reliability of Audit Evidence
- Audit Evidence Procedures
- Responsibilities for Fraud Detection and Prevention
- Notes

## Chapter 4: Standards and Guidelines for IT Auditing

- IIA Standards
- Code of Ethics
- Advisory Aids
- Standards for the Professional Performance of Internal Auditing
- ISACA Standards
- ISACA Code of Ethics
- COSO: Internal Control Standards
- BS 7799 and ISO 17799: IT Security
- NIST
- BSI Baselines
- Note

## Chapter 5: Internal Controls Concepts Knowledge

- Internal Controls
- Cost/Benefit Considerations
- Internal Control Objectives
- Types of Internal Controls
- Systems of Internal Control
- Elements of Internal Control
- Manual and Automated Systems
- Control Procedures
- Application Controls
- Control Objectives and Risks
- General Control Objectives
- Data and Transactions Objectives
- Program Control Objectives
- Corporate IT Governance
- COSO and Information Technology
- Governance Frameworks
- Notes
# Chapter 6: Risk Management of the IT Function

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nature of Risk</td>
<td>73</td>
</tr>
<tr>
<td>Risk-Analysis Software</td>
<td>74</td>
</tr>
<tr>
<td>Auditing in General</td>
<td>75</td>
</tr>
<tr>
<td>Elements of Risk Analysis</td>
<td>77</td>
</tr>
<tr>
<td>Defining the Audit Universe</td>
<td>77</td>
</tr>
<tr>
<td>Computer System Threats</td>
<td>79</td>
</tr>
<tr>
<td>Risk Management</td>
<td>80</td>
</tr>
<tr>
<td>Notes</td>
<td>83</td>
</tr>
</tbody>
</table>

# Chapter 7: Audit Planning Process

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits of an Audit Plan</td>
<td>85</td>
</tr>
<tr>
<td>Structure of the Plan</td>
<td>89</td>
</tr>
<tr>
<td>Types of Audit</td>
<td>91</td>
</tr>
</tbody>
</table>

# Chapter 8: Audit Management

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>93</td>
</tr>
<tr>
<td>Audit Mission</td>
<td>94</td>
</tr>
<tr>
<td>IT Audit Mission</td>
<td>94</td>
</tr>
<tr>
<td>Organization of the Function</td>
<td>95</td>
</tr>
<tr>
<td>Staffing</td>
<td>95</td>
</tr>
<tr>
<td>IT Audit as a Support Function</td>
<td>97</td>
</tr>
<tr>
<td>Planning</td>
<td>97</td>
</tr>
<tr>
<td>Business Information Systems</td>
<td>98</td>
</tr>
<tr>
<td>Integrated IT Auditor versus Integrated IT Audit</td>
<td>98</td>
</tr>
<tr>
<td>Auditees as Part of the Audit Team</td>
<td>100</td>
</tr>
<tr>
<td>Application Audit Tools</td>
<td>100</td>
</tr>
<tr>
<td>Advanced Systems</td>
<td>100</td>
</tr>
<tr>
<td>Specialist Auditor</td>
<td>101</td>
</tr>
<tr>
<td>IT Audit Quality Assurance</td>
<td>101</td>
</tr>
</tbody>
</table>

# Chapter 9: Audit Evidence Process

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Evidence</td>
<td>103</td>
</tr>
<tr>
<td>Audit Evidence Procedures</td>
<td>103</td>
</tr>
<tr>
<td>Criteria for Success</td>
<td>104</td>
</tr>
<tr>
<td>Statistical Sampling</td>
<td>105</td>
</tr>
<tr>
<td>Why Sample?</td>
<td>106</td>
</tr>
<tr>
<td>Judgmental (or Non-Statistical) Sampling</td>
<td>106</td>
</tr>
<tr>
<td>Statistical Approach</td>
<td>107</td>
</tr>
<tr>
<td>Sampling Risk</td>
<td>107</td>
</tr>
<tr>
<td>Assessing Sampling Risk</td>
<td>108</td>
</tr>
<tr>
<td>Planning a Sampling Application</td>
<td>109</td>
</tr>
<tr>
<td>Calculating Sample Size</td>
<td>111</td>
</tr>
<tr>
<td>Quantitative Methods</td>
<td>111</td>
</tr>
<tr>
<td>Project-Scheduling Techniques</td>
<td>116</td>
</tr>
<tr>
<td>Simulations</td>
<td>117</td>
</tr>
</tbody>
</table>
## Contents

Computer-Assisted Audit Solutions                   118  
Generalized Audit Software                        118  
Application and Industry-Related Audit Software    119  
Customized Audit Software                         120  
Information-Retrieval Software                    120  
Utilities                                          120  
On-Line Inquiry                                    120  
Conventional Programming Languages                120  
Microcomputer-Based Software                       121  
Test Transaction Techniques                       121  

**Chapter 10: Audit Reporting Follow-up**              123  
Audit Reporting                                     123  
Interim Reporting                                   124  
Closing Conferences                                 124  
Written Reports                                     124  
Clear Writing Techniques                            125  
Preparing to Write                                  126  
Basic Audit Report                                  127  
Executive Summary                                   127  
Detailed Findings                                   128  
Polishing the Report                                129  
Distributing the Report                             129  
Follow-up Reporting                                 129  
Types of Follow-up Action                           130  

**PART II: INFORMATION TECHNOLOGY GOVERNANCE**        131  

**Chapter 11: Management**                            133  
IT Infrastructures                                  133  
Project-Based Functions                             134  
Quality Control                                     138  
Operations and Production                           139  
Technical Services                                  140  
Performance Measurement and Reporting               140  
Measurement Implementation                          141  
Notes                                               145  

**Chapter 12: Strategic Planning**                    147  
Strategic Management Process                        147  
Strategic Drivers                                   148  
New Audit Revolution                                149  
Leveraging IT                                       149  
Business Process Re-Engineering Motivation          150  
IT as an Enabler of Re-Engineering                  151  
Dangers of Change                                   152  
System Models                                       152
Contents

Information Resource Management 153
Strategic Planning for IT 153
Decision Support Systems 155
Steering Committees 156
Strategic Focus 156
Auditing Strategic Planning 156
Design the Audit Procedures 158
Note 158

Chapter 13: Management Issues 159

Privacy 161
Copyrights, Trademarks, and Patents 162
Ethical Issues 162
Corporate Codes of Conduct 163
IT Governance 164
Sarbanes-Oxley Act 166
Payment Card Industry Data Security Standards 166
Housekeeping 167
Notes 167

Chapter 14: Support Tools and Frameworks 169

General Frameworks 169
COSO: Internal Control Standards 172
Other Standards 173
Governance Frameworks 176
Note 178

Chapter 15: Governance Techniques 179

Change Control 179
Problem Management 181
Auditing Change Control 181
Operational Reviews 182
Performance Measurement 182
ISO 9000 Reviews 184

PART III: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT 185

Chapter 16: Information Systems Planning 187

Stakeholders 187
Operations 188
Systems Development 189
Technical Support 189
Other System Users 191
Segregation of Duties 191
Personnel Practices 192
Object-Oriented Systems Analysis 194
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Information Management and Usage</td>
<td>199</td>
</tr>
<tr>
<td>18</td>
<td>Development, Acquisition, and Maintenance of Information Systems</td>
<td>207</td>
</tr>
<tr>
<td>19</td>
<td>Impact of Information Technology on the Business Processes and Solutions</td>
<td>215</td>
</tr>
<tr>
<td>20</td>
<td>Software Development</td>
<td>221</td>
</tr>
<tr>
<td>21</td>
<td>Audit and Control of Purchased Packages and Services</td>
<td>229</td>
</tr>
</tbody>
</table>

**Chapter 17: Information Management and Usage**
- What Are Advanced Systems? 199
- Service Delivery and Management 201
- Computer-Assisted Audit Tools and Techniques 204

**Chapter 18: Development, Acquisition, and Maintenance of Information Systems**
- Programming Computers 207
- Program Conversions 209
- No Thanks Systems Development Exposures 209
- Systems Development Controls 210
- Systems Development Life Cycle Control: Control Objectives 210
- Micro-Based Systems 212
- Cloud Computing Applications 212
- Note 213

**Chapter 19: Impact of Information Technology on the Business Processes and Solutions**
- Impact 215
- Continuous Monitoring 216
- Business Process Outsourcing 218
- E-Business 219

**Chapter 20: Software Development**
- Developing a System 221
- Change Control 225
- Why Do Systems Fail? 225
- Auditor's Role in Software Development 227

**Chapter 21: Audit and Control of Purchased Packages and Services**
- IT Vendors 230
- Request For Information 231
- Requirements Definition 231
- Request for Proposal 232
- Installation 233
- Systems Maintenance 233
- Systems Maintenance Review 234
- Outsourcing 234
- SAS 70 Reports 234
Chapter 22: Audit Role in Feasibility Studies and Conversions 237

Feasibility Success Factors 237
Conversion Success Factors 240

Chapter 23: Audit and Development of Application Controls 243

What Are Systems? 243
Classifying Systems 244
Controlling Systems 244
Control Stages 245
Control Objectives of Business Systems 245
General Control Objectives 246
CAATs and Their Role in Business Systems Auditing 247
Common Problems 249
Audit Procedures 250
CAAT Use in Non-Computerized Areas 250
Designing an Appropriate Audit Program 250

PART IV: INFORMATION TECHNOLOGY SERVICE DELIVERY AND SUPPORT 253

Chapter 24: Technical Infrastructure 255

Auditing the Technical Infrastructure 257
Infrastructure Changes 259
Computer Operations Controls 260
Operations Exposures 261
Operations Controls 261
Personnel Controls 261
Supervisory Controls 262
Information Security 262
Operations Audits 263
Notes 264

Chapter 25: Service-Center Management 265

Private Sector Preparedness (PS Prep) 266
Continuity Management and Disaster Recovery 266
Managing Service-Center Change 269
Notes 269

PART V: PROTECTION OF INFORMATION ASSETS 271

Chapter 26: Information Assets Security Management 273

Control Techniques 276
Workstation Security 276
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Security</td>
<td>276</td>
</tr>
<tr>
<td>Logical Security</td>
<td>277</td>
</tr>
<tr>
<td>User Authentication</td>
<td>277</td>
</tr>
<tr>
<td>Communications Security</td>
<td>277</td>
</tr>
<tr>
<td>Encryption</td>
<td>277</td>
</tr>
<tr>
<td>How Encryption Works</td>
<td>278</td>
</tr>
<tr>
<td>Encryption Weaknesses</td>
<td>279</td>
</tr>
<tr>
<td>Potential Encryption</td>
<td>280</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>280</td>
</tr>
<tr>
<td>Double Public Key Encryption</td>
<td>281</td>
</tr>
<tr>
<td>Steganography</td>
<td>281</td>
</tr>
<tr>
<td>Information Security Policy</td>
<td>282</td>
</tr>
<tr>
<td>Notes</td>
<td>282</td>
</tr>
</tbody>
</table>

### Chapter 27: Logical Information Technology Security 283

- Computer Operating Systems                                           283
- Tailoring the Operating System                                       284
- Auditing the Operating System                                        285
- Security Criteria                                                    286
- Security Systems: Resource Access Control Facility                   287
- Auditing RACF                                                         288
- Access Control Facility 2                                             289
- Top Secret                                                           290
- User Authentication                                                  291
- Bypass Mechanisms                                                    293
- Security Testing Methodologies                                        293
- Notes                                                                295

### Chapter 28: Applied Information Technology Security 297

- Communications and Network Security                                  297
- Network Protection                                                   298
- Hardening the Operating Environment                                  300
- Client Server and Other Environments                                 301
- Firewalls and Other Protection Resources                             301
- Intrusion-Detection Systems                                          303
- Note                                                                 304

### Chapter 29: Physical and Environmental Security 305

- Control Mechanisms                                                   306
- Implementing the Controls                                            310
PART VI: BUSINESS CONTINUITY AND DISASTER RECOVERY 311

Chapter 30: Protection of the Information Technology Architecture and Assets: Disaster-Recovery Planning 313
- Risk Reassessment 314
- Disaster—Before and After 315
- Consequences of Disruption 317
- Where to Start 317
- Testing the Plan 319
- Auditing the Plan 320

Chapter 31: Displacement Control 323
- Insurance 323
- Self-Insurance 327

PART VII: ADVANCED IT AUDITING 329

Chapter 32: Auditing E-commerce Systems 331
- E-Commerce and Electronic Data Interchange: What Is It? 331
- Opportunities and Threats 332
- Risk Factors 335
- Threat List 335
- Security Technology 336
- “Layer” Concept 336
- Authentication 336
- Encryption 337
- Trading Partner Agreements 338
- Risks and Controls within EDI and E-Commerce 338
- E-Commerce and Auditability 340
- Compliance Auditing 340
- E-Commerce Audit Approach 341
- Audit Tools and Techniques 341
- Auditing Security Control Structures 342
- Computer-Assisted Audit Techniques 343
- Notes 343

Chapter 33: Auditing UNIX/Linux 345
- History 345
- Security and Control in a UNIX/Linux System 347
- Architecture 348
- UNIX Security 348
- Services 349
- Daemons 350
- Auditing UNIX 350
- Scrutiny of Logs 351
- Audit Tools in the Public Domain 351
## Contents

UNIX Password File 352  
Auditing UNIX Passwords 353  

Chapter 34: Auditing Windows VISTA and Windows 7 355  
History 355  
NT and Its Derivatives 356  
Auditing Windows Vista/Windows 7 357  
Password Protection 358  
VISTA/Windows 7 359  
Security Checklist 359  

Chapter 35: Foiling the System Hackers 361  

Chapter 36: Preventing and Investigating Information Technology Fraud 367  
Preventing Fraud 367  
Investigation 369  
Identity Theft 376  
Note 376  

Appendix A Ethics and Standards for the IS Auditor 377  
ISACA Code of Professional Ethics 377  
Relationship of Standards to Guidelines and Procedures 378  

Appendix B Audit Program for Application  
Systems Auditing 379  

Appendix C Logical Access Control Audit Program 393  

Appendix D Audit Program for Auditing UNIX/Linux Environments 401  

Appendix E Audit Program for Auditing Windows VISTA and Windows 7 Environments 407  

About the Author 415  
About the Website 417  
Index 419