INFORMATION TECHNOLOGY CONTROL AND AUDIT

Second Edition

Frederick Gallegos, CGFM, CISA, CDE
Sandra Senft, CISA, CIA
Daniel P. Manson, Ph.D.
Carol Gonzales, CISA

AUERBACH

Contents

ABOUT THE AUTHORS xxix
FOREWORD AND ACKNOWLEDGMENT xxxiii

PART I A FOUNDATION FOR IT AUDIT AND CONTROL....... 1

Chapter 1
Information Technology Environment: Why Are Controls and Audit Important? 3
IT Today and Tomorrow 5
Information Integrity, Reliability, and Validity: Their Importance in Today's Global Business Environment.............................. 7
Legal Issues Impacting IT 9
Federal Financial Integrity Legislation 10
Federal Security Legislation.. 11
The Computer Fraud and Abuse Act (CFAA) 11
The Computer Security Act of 1987 12
The Homeland Security Act of 2002 (Inclusion of the Cyber Security Enhancement Act).. 13
Privacy on the Information Superhighway......................... 14
Private Information Available for the Taking 14
Privacy Legislation and the Federal Government Privacy Act 15
Electronic Communications Privacy Act 16
Communications Decency Act of 1995.............................. 17
Health Insurance Portability and Accountability Act — 1996 18
Current Legislative Activities: Security, Privacy, and Audit 18
Control and Audit: A Global Concern 20
E-Commerce and Electronic Funds Transfer 21
Future of Electronic Payment Systems.............................. 21
Conclusion 22
Review Questions 23
Multiple Choice... 23
Exercises 26
Answers to Multiple Choice Questions 26
References 26

Chapter 2

Audit and Review: Its Role in Information Technology 29
The Need for the IT Audit Function 30
Auditing Concerns 31
The Reviewers of Information System Policies, Procedures,
Standards, and Their Applications 32
What Are the Policies and Procedures of Management? 32
Auditors Have Standards of Practice 33
Auditors Must Have Independence 34
The Practice of Continuous Reassessment 35
High Ethical Standards 36
The Auditor: Knowledge, Skills, and Abilities 37
Broadest Experiences 38
Supplemental Skills 41
Trial and Error 42
Objective and Context 42
The Role of the IT Auditor 43
The IT Auditor as Counselor 44
The IT Auditor as Partner of Senior Management 45
Types of Auditors and Their Duties, Functions, and Responsibilities . . . 45
  The Internal Audit Function 46
  The External Auditor 46
Legal Implications 47
Management Responsibilities Today 48
Risk Assessment 48
  Three Perspectives on Risk 49
    The Guardians. 49
    The Gatekeepers. 50
  Application of Risk Assessment 51
Participation in Corporate IT Audit Planning 51
The Organization's Responsibility in Developing IT Audit Skills 52
Conclusion 53
Chapter Review Test 54
  Multiple Choice 54
  Exercises 56
  Answers to Multiple Choice Questions 56
    Notes 56
References 57

Chapter 3

The Audit Process in an Information Technology Environment 59
IT Auditing: What Is it? 59
The Audit Process 60
The Situation and the Problem — from EFCA to Enron 61

Audit Standards . . . 62
Similarities . . . 63
Differences . . . 63
The Importance of Audit Independence . . . 64
Past and Current Accounting and Auditing Pronouncements . . . 65
AICPA Pronouncements — from the Beginning to Now . . . 65
Other Standards . . . 67
Financial Auditing . . . 69
Generally Accepted Accounting Principles (GAAP) . . . 69
Generally Accepted Auditing Standards (GAAS) . . . 69
General Standards . . . 69
Field Work Standards . . . 70
Reporting Standards . . . 70
Planning the Audit . . . 70
Using the Plan to Identify Problems . . . 71
Organizing the Audit . . . 72
Preliminary Review . . . 72
General Data Gathering . . . 73
Identifying Financial Application Areas . . . 74
Preparing an Audit Plan . . . 74
Field Work and Implementing Audit Methodology . . . 74
Audit Tools and Techniques . . . 75
Flowcharting as an Analysis Tool . . . 76
Understanding How Computers Process Data . . . 77
Identifying Documents and Their Flow through the System . . . 78
Defining Critical Data . . . 80
Developing Audit Data Flow Diagrams . . . 80
Evaluating the Quality of System Documentation . . . 80
Assessing Controls over Documents . . . 81
Determining the Effectiveness of Processing under Computer Programs . . . 81
Evaluating the Usefulness of Reports . . . 81
Appropriateness of Flowcharting Techniques . . . 82
Validation of Work Performed . . . 83
Using Personal Computing Technology . . . 84
The Audit Report and Follow-Up . . . 85
Post-Audit . . . 87
Conclusion . . . 87
Chapter Review Questions . . . 88
Multiple Choice . . . 89
Exercises . . . 90
Multiple Choice Answers . . . 91
References . . . 92

Chapter 4
Auditing Information Technology Using Computer-Assisted Audit Tools and Techniques 93
Auditor Productivity Tools 94
Audit Planning and Tracking 95
Documentation and Presentations 95
Communication 95
Data Management 96
Resource Management 96
Groupware 97
Using CAATs in the Audit Process 97
Technical Skills and Tools 99
Generalized Audit Software 99
Application Testing 99
Designing Tests of Controls 99
Data Analysis 100
Compliance Testing 100
Continuous Monitoring 100
Application Controls 101
Spreadsheet Controls 101
Database Controls 102
Audit Functions 103
Items of Audit Interest 103
Audit Mathematics 103
Data Analysis 105
System Validation 106
Sampling 107
Random Attribute Sampling 107
Variable Sampling Techniques 108
Computer Forensics: Methods and Techniques 109
Conclusion 111
Chapter Review Questions 111
Multiple Choice 112
Exercises 113
Answers to Multiple Choice Questions 114
References 114

PART II AUDITING IT PLANNING AND ORGANIZATION 115

Chapter 5
IT Strategy and Standards 121
Architecture and Standards 123
Policies and Procedures 124
Audit Involvement 124

An Example of Standards: Technology Risk Management Regulations. 125
Where Does Technology Risk Management Belong? 127
The Strategy: An Effective Technology Risk Management Program 129
  Example: Importance of Business Strategy in Customer Relationship Management 131
  Focus on Technology 132
  Resistance to Change 133
  Barriers to User Adoption 134
Conclusion 136
Review Questions 136
  Multiple Choice Questions 136
  Exercises 138
  Multiple Choice 138
References 138

Chapter 6
Planning and Controlling 141
Governance Processes 141
Demand Management 141
Project Initiation 143
Technical Review. 143
Procurement and Vendor Management 143
Strategic Sourcing and Vendor Management 144
Resource Management and Service Management 144
Financial Management and Budgeting 147
  Operating Budget 147
    Chargeback 147
    Advantages 147
    Disadvantages. 147
  Capital Budgeting 148
The Importance of Project Planning and Control in the Systems Development Life Cycle (SDLC) 148
Project Planning and Control: E-Commerce Security as a Strategic and Structural Problem 151
Information Security Management Systems (ISMS) 152
The Planning and Control Approach to E-Commerce Security Management. 152
  Strategic Aspect 152
  Organizational Aspect 153
  Technical Aspect. 153
  Financial Aspect 154
  Legal Aspect 154

Conclusion 155
Audit Involvement in Planning and Analysis 155
Conception of the Plan 156
Project Organization 156
Review Questions 157
Multiple Choice Questions 157
Exercises 159
Answers to Multiple Choice Questions 159
References 159

Chapter 7
Project Management 161
Project Management Process 161
Project Management Body of Knowledge (PMBOK)™ 163
Project Management Framework 163
Project Management 164
Resource Management 165
Program Management versus Project Management 165
Project Planning 165
Project Tracking and Oversight 165
Project Management Tools 166
The Auditor's Role in the Project Management Process 171
Audit Risk Assessment 171
Audit Plan 173
Project Management Process Review 173
Project Management 174
Communication 174
Recommendations 175
Example of Project Management Checkpoints and Tools in a Telecom Project 175
Combating User Resistance to Telecommunications
Project Implementation: Involve the User 176
Project Management Tools: Project Management Software 176
Conclusion 179
Review Questions 180
Multiple Choice Questions 180
Exercises 181
Answers to Multiple Choice Questions 181
References 182

Chapter 8
Quality Management 183
Software Development Standards 183
Capability Maturity Model (CMM) 184

How Maturity Correlates to Quality . . . 189
Raytheon's Example . . . 189
Approaches to Software Development . . . 190
Software Development Process . . . 191
Software Development Phases . . . 191
Analysis . . . 192
Design . . . 193
Construction . . . 193
Testing . . . 193
System Documentation . . . 193
Implementation . . . 194
Traditional Information Software Development . . . 195
Prototypes and Rapid Application Development (RAD) . . . 196
End-User Development (EUD) . . . 197
The Auditor's Role in the Development Process . . . 198
Risk Assessment . . . 200
Audit Plan . . . 201
Software Development Controls Review . . . 201
Software Development Life Cycle . . . 201
Analysis . . . 202
Design . . . 202
Construction . . . 203
Testing . . . 203
Documentation . . . 204
Implementation . . . 204
Post-Implementation . . . 204
Change Control . . . 204
Application Controls . . . 204
Auditing Quality Assurance . . . 205
Communication . . . 205
Recommendations . . . 205
Audit Report . . . 207
Conclusion . . . 207
Review Questions . . . 208
Multiple Choice Questions . . . 208
Exercises . . . 209
Answers to Multiple Choice Questions . . . 210
References . . . 210

PART III AUDITING IT ACQUISITION AND IMPLEMENTATION 211

Chapter 9
Software Acquisition 215
Software Acquisition Process 215
Defining the Information and System Requirements 215
Prototypes and Rapid Application Development (RAD) 216
The Requirements Document 216
Identifying Various Alternatives 217
Off-the-Shelf Solutions 217
Purchased Package 218
Contracted Development 218
Outsourcing a System from Another Organization 218
Performing a Feasibility Analysis 219
Conducting a Risk Analysis 220
Defining Ergonomic Requirements 220
Carrying Out the Selection Process 220
Request for Information (RFI) 221
Request for Bid (RFB) 221
Request for Proposal (RFP) 221
Evaluating Proposals 222
Procuring the Selected Software 223
Other Considerations for Software Contracts and Licenses 224
Completing Final Acceptance 225
Reviewing Software Acquisitions 225
Alignment with the Company's Business and IT Strategy 226
Definition of the Information Requirements 226
Prototypes 226
Feasibility Studies (Cost, Benefits, Etc.) 227
Identification of Functionality, Operational, Acceptance, and Maintenance Requirements 228
Conformity with Existing Information and System Architectures . . . 228
Adherence to Security and Control Requirements 229
Knowledge of Available Solutions 229
Understanding of the Related Acquisition and Implementation Methodologies 229
Involvement and Buy-In from the User 230
Supplier Requirements and Viability 230
Other Resources for Help and Assistance 231
Conclusion 232
Review Questions 232
Multiple Choice 233

Exercises . . . 235
Answers to Multiple Choice Questions . . . 235
References . . . 235

Chapter 10
System Implementation . . . 237
The System Implementation Process . . . 237
Implementation Approach . . . 238
System Testing . . . 238
User Processes and Procedures . . . 239
Management Reports and Controls . . . 240
Problem Management/Reporting . . . 240
User Acceptance Testing . . . 240
Acceptance Team . . . 241
Agreed-Upon Requirements . . . 241
Management Approval . . . 241
Help Desk and Production Support Training and Readiness . . . 241
Data Conversion and Data Correction Processes . . . 242
Operational Procedures and Readiness . . . 243
IT Disaster/Continuity Plans . . . 244
Security . . . 244
Case Example: GMA Business Overview and Profile . . . 245
IT Solutions for GMA . . . 246
Major E-Commerce Security Implementation Issues at GMA . . . 247
Awareness Assessment . . . 247
Implementing Risk Analysis and Controls at GMA . . . 249
Summary . . . 250
Conclusion . . . 251
Review Questions . . . 251
Multiple Choice . . . 252
Exercises . . . 254
Answers to Multiple Choice Questions . . . 254
References . . . 254

Chapter 11
Application Risks and Controls . . . 257
Application Risks . . . 257
Weak Security . . . 258
Unauthorized Access or Changes to Data or Programs . . . 258
Unauthorized Remote Access . . . 259
Inaccurate Information . . . 259
Erroneous or Falsified Data Input . . . 259
Misuse by Authorized End Users . . . 259
Incomplete Processing . . . 260
Duplicate Transaction Processing . . . 260

Untimely Processing . . . 260
Communications System Failure . . . 260
Inadequate Testing . . . 260
Inadequate Training . . . 260
Inadequate Support . . . 261
Insufficient Documentation . . . 262
End-User Computing (EUC) Application Risks . . . 262
Inefficient Use of Resources . . . 264
Incompatible Systems . . . 264
Redundant Systems . . . 264
Ineffective Implementations . . . 265
Absence of Segregation of Duties . . . 265
Incomplete System Analysis . . . 265
Unauthorized Access to Data or Programs . . . 265
Copyright Violations . . . 266
The Destruction of Information by Computer Viruses . . . 267
Electronic Data Interchange (EDI) Application Risks . . . 268
Implications of Risks in an EDI System . . . 270
Application Controls . . . 270
Input Controls . . . 271
Interfaces . . . 271
Authenticity . . . 271
Accuracy . . . 272
Processing Controls . . . 272
Completeness . . . 273
Error Correction . . . 274
Output Controls . . . 275
Reconciliation . . . 275
Distribution . . . 275
Retention . . . 276
Functional Testing and Acceptance . . . 276
Management Approval . . . 276
Documentation Requirements . . . 277
Application Software Life Cycle . . . 277
System Development Methodology . . . 277
User Interface . . . 278
Application Maintenance . . . 278
Application Maintenance: Defined . . . 278
Corrective Maintenance . . . 278
Adaptive Maintenance . . . 279
Perfective Maintenance . . . 279
Measuring Risk for Application Maintenance . . . 279
Conclusion . . . 280
Chapter Review Questions . . . 281
Multiple Choice . . . 281

Exercises . . . 283
Answers to Multiple Choice Questions . . . 284
References . . . 284

Chapter 12
Change Management . . . 285
Vulnerabilities in Software Development and Change Control . . . 285
Software Configuration Management . . . 286
IT Change Management . . . 287
Change Management System . . . 287
Change Request Process . . . 287
Impact Assessment . . . 289
Controls over Changes . . . 292
Emergency Change Process . . . 292
Revisions to Documentation and Procedures . . . 292
Authorized Maintenance . . . 293
Software Release Policy . . . 293
Software Distribution Process . . . 294
Change Management Example . . . 295
Objectives . . . 295
Scope . . . 296
Change Management Boards or Committees . . . 296
Criteria for Approving Changes . . . 297
Post-Implementation . . . 298
Organizational Change Management . . . 298
Organizational Culture Defined . . . 298
Managing Organizational Change Management . . . 299
Conclusion . . . 300
Review Questions . . . 301
Multiple Choice . . . 301
Exercises . . . 303
Answers to Multiple Choice Questions . . . 303
References . . . 304

PART IV AUDITING IT OPERATIONS: FROM STANDALONE TO GLOBAL . . . 305

Chapter 13
IT Operations Environments: Complexities and Control Issues . . . 307
The Virtual Environment . . . 308
Areas of Control and Risk Issues . . . 310
IT Operations Issues in Network Installation . . . 311
Types of WANs . . . 314

Elements of WANs . . . 315
  Access Methods . . . 315
  Connective Devices . . . 315
    Bridges . . . 315
    Routers . . . 315
    Protocols . . . 315
  Network Services . . . 316
    Frame Relay Network Services . . . 316
    Asynchronous Transfer Mode Network Services . . . 317
  The Network Management System . . . 317
  Network Topologies . . . 317
    Star Topology . . . 317
    Ring Topology . . . 317
    Bus Topology . . . 318
    Mesh Topology . . . 318
    Hybrid Topology . . . 318
Tools for Network Monitoring . . . 318
  Protocol Analyzers . . . 318
    WAN Protocol Analyzers . . . 319
  Network Monitors . . . 319
  Network Management Software . . . 319
  General Statistical Tools . . . 320
    Hybrids . . . 320
The Internet, Intranet, and Extranet . . . 320
  Personal Accounts . . . 323
  Commercial Gateways . . . 324
  Commercial Services . . . 324
  LAN Security Issues: Wired versus Wireless . . . 324
  What Can Be Done to the Wired LANs? . . . 324
    Physical Security: Site Control and Management . . . 324
    User Authentication . . . 325
    Eavesdropping Countermeasures . . . 325
  Why WLANs Are More Secure . . . 325
  Spread-Spectrum Technology . . . 325
  Station Authentication . . . 326
  Physical Security . . . 326
  Network Management Control Issues . . . 327
  Importance of National Information Infrastructure . . . 328
Conclusion . . . 329
Questions . . . 330
  Multiple Choice . . . 330
  Exercises . . . 332
  Answers to Multiple Choice Questions . . . 332
References . . . 332

Chapter 14

Operational Control Issues 335
Organizational Policy and Organization Controls 335
Data Files and Program Controls 336
Backup/Restart and Disaster Recovery Controls 337
Physical Security and Access Controls 337
Environmental Controls 338
CobiT Operational Controls 340
  Comparing CobiT and General Controls for Operational Auditing... 340
Problem Management Auditing 345
Problem Management Auditing in Action Overview 345
  Purpose 346
  Scope 346
  Objectives 346
  Key Success Factors 347
Introduction to Data Center Reviews 347
Data Center Audit Program 348
  A. Administration of IT Activities 348
    Audit Steps 348
  B. Operating Systems Software and Data 349
    Audit Steps 349
  C. Computer Operations/Business Resumption 349
    Audit Steps 349
  D. Security Administration 350
    Audit Steps 350
Software and Data Security Controls 350
    Physical and Environmental Controls Management 350
    Data Access Management 351
    Policy and Procedures Documentation 351
    Data and Software Backup Management 351
    Other Management Controls 351
The Call Center (CC) Concept 352
New Audit Responsibilities 354
Developing Audit Software in the CC 354
Auditing the CC 355
  The System Development Life Cycle 356
  Data Integrity 357
  Data Security 357
  Physical Security and Recovery Procedures 358
  Computer Resources 358
  Department Standards 358
Conclusion 359
Review Questions 359
  Multiple Choice 360

Exercises 361
Answers to Multiple Choice Questions 362
References 362

Chapter 15

Assessing Risk in IT Operations 363
Risk Assessment 363
Available Guidance 363
U.S. National Institute of Standards and Technology (NIST) 364
Government Accounting Office (GAO) 364
American Institute of Certified Public Accountants (AICPA) 365
Information Systems Audit and Control Association (ISACA) 369
Institute of Internal Auditors (IIA) 369
Committee of Sponsoring Organizations of the Treadway Commission (COSO) 370
Introduction to ERM/ORM 370
What Is ERM/ORM? 371
Enterprise/Operational Risk Management 371
Why ERM/ORM? 371
Organizational Oversight 371
Magnitude of Problem 373
Increasing Business Risks 373
Regulatory Issues 373
Market Factors 375
Corporate Governance 376
Best Practice 376
Concluding Thoughts on ERM/ORM 377
Web and Java Risk Issues 379
Perceived Risks 379
Internet Security 380
Security Tools and Technologies 380
Encryption Technologies 380
Security Policies and Procedures 381
Internet Firewalls 382
Internet Firewall Configurations — Bastion Host 384
Choke Router/Screened Host 384
Firewalls in a Partitioned Network 385
Practical Web Security Solutions 386
A Backdoor Connection 386
A Network Firewall 387
A Pseudo Firewall 387
Java Risk Issues 388
World Wide Web and Java Risk Conclusions 390
IT Insurance Risk 392
Problems Addressed 392

Insurance Requirements 392
Reduction and Retention of Risks 394
Risk Management 394
Determination of Objectives 396
IT Risk Identification 396
IT Risk Assessment Tools and Techniques 397
IT Risk Evaluation 398
IT Risk Management 398
How to Determine IT Insurance Coverage 400
Conclusion 402
Chapter Review Questions 403
Multiple Choice 403
Exercises 405
Answers to Multiple Choice Questions 405
Notes 405
References 405

Chapter 16
Audit Methods and Techniques for Operations 409
Auditing Contingency and Disaster Recovery Planning. 410
Audit of Disaster Recovery Planning Steps 410
Written Disaster Recovery Plan 411
Mission Statement for Disaster Recovery Plan 411
Disaster Recovery Plan Tests and Drill. 412
Auditing DBMS Recovery 412
Importance of DBMS Recovery 413
The Recovery Process 414
Transaction Properties 414
Causes of DBMS Failure 415
Database Users 416
Database Administrator 416
Applications and Systems Programmers 417
Web Designers and Developers 417
End Users 417
Backup and Recovery of the Data Warehouse 418
Data Warehouse Integrity Check List 419
Trends in Data Warehousing 419
Auditing Data Communications. 420
Data Communications Controls. 422
LAN Audit and Security Issues: Wired versus Wireless 425
What Can Be Done to the Wired LANs? 426
Physical Security: Site Control and Management 426
User Authentication. 426
Eavesdropping Countermeasures 426
For Wireless: Key Audit and Security Checkpoints 427

Control Concerns with IEEE 802.11 Wired Equivalent Privacy (WEP) Protocol . . . 427
Station Authentication . . . 427
Physical Security . . . 427
IEEE 802.11i Robust Security Network Standard . . . 428
Auditing End-User Computing . . . 428
Preliminary Audit Planning . . . 428
Defining the Audit Methodology . . . 429
Defining the Scope and Content of the Audit . . . 429
The Audit Plan . . . 429
Reviewing the EUC Group's Procedures and Objectives . . . 430
Evaluating the EUC Groups' Effectiveness by Reviewing Their Documentation . . . 431
Audit Testing . . . 431
The Audit Report . . . 432
Conclusion . . . 432
Chapter Review Questions . . . 433
Multiple Choice . . . 434
Exercises . . . 435
Answers to Multiple Choice Questions . . . 435
References . . . 436

Chapter 17
Using Tools and Techniques in IT Operation Reviews . . . 439
Computer-Assisted Audit Tools and Techniques for Operational Reviews . . . 440
Systems Maintenance . . . 443
Definition of Systems Maintenance . . . 443
Change Control . . . 444
Points of Change Origination and Initiation . . . 445
Approval Points . . . 448
Changes to Documentation . . . 448
Review Points . . . 449
Reviewing Operating Systems . . . 449
Types and Uses of System Software . . . 451
Reliance on Systems Software . . . 452
Controlling Access to Systems Software . . . 454
Controlling Changes to System Software . . . 455
SAP Implementation and Control Issues . . . 455
Understanding the Corporate Culture . . . 455
Understood and Complete Process Changes . . . 456
Communication: Never Enough! . . . 456
Management Support . . . 456
SAP Project Manager Competence . . . 457
The Team . . . 457

Project Methodology: It Is Important 458
Training 458
Commit to the Change 458
Establishing Security and Controls 459
Security Features of the Basis Component 459
Summary of Access Control 460
Administrative Controls 460
Accountability 460
Access Control 461
Confidentiality, Integrity, and Security Management 461
EDI and Internet Security 462
The ISO 9001 Review 463
CRBE (Formerly Known as CTQA) 463
SEI 463
ISO 9000 464
Getting Started: ISO 9000 464
E-Q-NET 465
More about NSAI 465
Principal Themes of an ISO 9000 Review 466
Computer Forensics 467
WebMetrics: An Introduction 468
WebMetrics as an Audit Tool 470
Overview 470
Conclusion 471
Review Questions 472
Multiple Choice 473
Exercises 475
Multiple Choice Answers 475
References 475

PART V EMERGING ISSUES IN IT AUDIT 479

Chapter 18
The Legal Environment and Its Impact on Information Technology: From IT Crime Law to IT Contract Law to Netlaw 483
IT Crime Issues 484
Protection against Computer Fraud 486
The Computer Fraud and Abuse Act (CFAA) 487
Computer Abuse Amendments Act 489
Sarbanes–Oxley Act (Public Law 107-204) 489
Major Points from the Sarbanes–Oxley Act of 2002 491
Criminal Intent 494
Penalties and Requirements under Title VIII of the Act 495
Penalties and Requirements under Title IX of the Act 495

Remedies and Effectiveness 495
Legislation Providing for Civil and Criminal Penalties 497
The Computer Security Act of 1987 498
The Homeland Security Act of 2002 500
IT Contract Issues 502
Netlaw: Privacy on the Information Superhighway. 505
Private Information Available for the Taking. 505
The National Strategy for Securing Cyberspace 508
Methods that Provide for Protection of Information 511
The Web Copyright Law 511
Privacy Legislation and the Federal Government Privacy Act 512
Electronic Communications Privacy Act 513
Communications Decency Act of 1995 515
Encrypted Communications Privacy Act of 1996 515
Health Insurance Portability and Accountability Act of 1996 (HIPAA) 515
HIPAA Compliance 516
Risk Assessment and Communications Act of 1997 516
Risk Gramm–Leach–Bliley Act of 1999 516
Current Pending Bills and Other Legislative Material 516
Internet Governance 518
Conclusion 518
Review Questions 519
Multiple Choice 520
Exercises 522
Answers to Multiple Choice Questions 522
Notes 522
References 522
Other Internet Sites 523

Chapter 19
Security and Privacy of Information Technology: From the Individual to the Extranet/Intranet/Internet 525
Information Systems Security and Privacy in 1998. 526
Information Systems Security and Privacy Today. 527
Interconnected Systems and Electronic Commerce: Global Issues 531
International Organization for Standardization and ISO 17799 531
The Battleground: The Internet 533
The Tools 534
Scanners. 534
Password Crackers 535
Trojan Horse 536
Sniffers 538
Destructive Devices 538
E-Mail Bombs and Worms 539

The IT Audit and Auditor Assessment Form 579
IT Audit Areas 582
  Audit Preparation 582
  Audit Objectives 582
  Fact Gathering 582
  Audit Program 582
  Audit Tests 583
  Use of Audit Tools 583
  Conclusions 583
  Findings 583
  Recommendations 583
  The Audit Report 584
  Working Papers 584
  Relations with the Auditee 584
  Relations with Audit Management 584
  Follow-Up of Audit Recommendations 584
Criteria for Assessing the Audit 585
  Completeness 585
  Pertinence 585
  Accuracy 585
  Appropriate Conclusions, Findings, and Recommendations 586
  Follow-Up of Findings and Recommendations 586
Criteria for Assessing the Auditor 586
Metrics and Management 586
Implementation of Measurements 588
Applying the Concept 589
Evaluation of IT Audit Performance 589
What Is a Best Practice? 590
  Why Is It Important to Learn about Best Practices? 591
  Overview of Best Practices in IT Audit Planning 591
  Research 592
  Benchmarking 593
  Planning Memo 593
  Budget Coordination 594
  Risk Analysis 594
  Kick-Off Meeting 595
  Staff Mentoring 597
  Coaching 597
  Lunch Meetings 597
  Understand Requirements 598
Conclusion 598
Review Questions 599
  Multiple Choice 600

Exercises 601
Answers to Multiple Choice Questions 602
References 602

Chapter 21

IT Auditing in the New Millennium 605
IT Auditing Trends 606
The New Dimension: Information Assurances 608
IT Audit: The Profession 610
A Common Body of Knowledge 610
Certification 611
Continuing Education 611
A Code of Ethics and Professional Standards 612
Educational Curricula 612
New Trends in Developing IT Auditors and Education 613
Career Opportunities in the 21st Century 619
Public Accounting 620
Private Industry 620
Management Consulting 620
Government 621
The Role of the IT Auditor in IT Governance 621
The IT Auditor as Counselor 623
The IT Auditor as Partner of Senior Management 623
Educating the Next Generation on IT Audit and Control Opportunities 624
Conclusion 624
Review Questions 625
Multiple Choice 625
Exercises 627
Answers to Multiple Choice Questions 627
References 627

PART VI APPENDICES 629

Appendix I

Information Technology Audit Cases 631
Computer-Assisted Audit Cases 631
Case 1: Wooback City 631
Part 1 631
Part 2 631
Case 2: Ready or Not Auto Insurance 632
Case 3: Holt Valley Hospital Services, Inc. 632
Case 4: Acme Insurance Corporation 633

Controls 633
Case 5: OnTheRise Corporation 633
Case 6: Wedco Electronics 633
Case 7: Amazon Industries 634
Legal Issues 635
Case 8: OhMY Corporation 635
Case 9: Ideal Financial 635
Security Issues 636
Case 10: Real-Wire 636
Required 637

Appendix II
Bibliography of Selected Publications for Information Technology Auditors 639
Government Publications 639
Department of Justice of the United States 639
General Accounting Office of the United States (GAO) 641
National Institute of Standards and Technology (NIST) 645
National Technical Information Service (NTIS) 648
Publications Available from Professional Association 649
American Institute of Certified Public Accountants (AICPA) 649
Association for Computing Machinery 650
The Canadian Institute of Chartered Accountants (CICA) 651
The Information Systems Audit and Control Association & Foundation (ISACA) 651
The Institute of Internal Auditors (IIA) 655
International Federation for Information Processing 656
International Federation of Accountants (IFAC) 657
Quality Assurance Institute 657
Other Publications 658
Best Practices in Information Technology 658
Computer Hardware and Software 658
Computer, Network, and Information Security 659
Enterprise Resource Planning (ERP) Systems 659
Information Technology and Accounting Systems 660
The Internet, E-Commerce, and Web Security 661
IT Auditing and Control Systems 662
Privacy of Information 663
Quality Assurance 664
Risk Management 665

Appendix III
Professional Standards That Apply to Information Technology (Audit, Security, and Privacy Issues) 667
American Institute of Certified Public Accountants (AICPA) 667

Information Source 668
Authoritative Guide 668
The Institute of Internal Auditors (IIA). 685
Information Source 686
Authoritative Guide 686
Information Systems Audit and Control Association (ISACA) 690
Authoritative Guide 690
The Canadian Institute of Chartered Accountants (CICA). 703
Information Source 704
Authoritative Guide 704
International Federation of Accountants (IFAC) 704
Information Source 708
Authoritative Guides 708
Information System Security Association (ISSA) 710
Information Source 711
Authoritative Guide 711
Society for Information Management (SIM) 711
Information Source 711
Authoritative Guide 712
Association of Information Technology Professionals (AITP). 712
Information Source 712
Authoritative Guide 712
Information Executive 712
The Nanosecond 713
International Federation for Information Processing (IFIP). 713
Information Source 713
Authoritative Guide 713
IFIP Technical Committee (TC) and Working Group (WG) — Aims and Scopes 713
Association for Computing Machinery (ACM) 714
Information Source 714
Authoritative Guide 721
Editor-in-Chief: Carl Cargill, SunSoft (A division of Sun Microsystems) 721
The Institute of Chartered Accountants in Australia (ICAA). 725
Information Source 725
Authoritative Guide 725
National Institute of Standards and Technology (NIST). 725
Information Source 730
Authoritative Guide 730
General Accounting Office (GAO) 736
Information Source 737
Authoritative Guide 737
International Organization of Supreme Audit Institutions (INTOSAI) 737

Information Source 744
Authoritative Guide 744
Auditing Standards 744
Guidelines for Internal Control Standards 744

Appendix IV
Glossary 747

Appendix V
Sample Audit Programs 799
Audit Program for Systems Maintenance 799
ISO 9001 Review: Conclusion and Documents 801
Lessons Learned — 9001 Review 802
Conclusion 803
Unisys Quality Policy 805
UTOP Seven Quality Beliefs 805
Orange County Quality System 805
Audit Program for Operating System Security Evaluation 810
Initial Checklist 810

Index 823

Information Technology

Information Technology Control and Audit, Second Edition is an excellent introductory reference to IT auditing, covering a wide range of topics in the field including the audit pocess, the legal environment of IT auditing, security and privacy, and more.

This book examines the foundation of IT audit and control, analyzes the process of audit and review, explores IT governance and control, and discusses the steps that align IT decisions with business strategy. It also covers project management processes that ensure that projects are controlled from inception through integration.

The text also addresses auditing IT acquisition and implementation, as well as the auditing of IT operations in both standalone and global environments. It concludes with a review of emerging issues, completing a thorough overview of a topic that is critical for organizational security and financial integrity.

Information Technology Control and Audit, Second Edition:

- Provides a complete overview for beginning IT auditors on the mechanisms of auditing applications, development systems, and operations
- Analyzes the use of the COBIT approach
- Covers advanced topics in the audit of operations such as E-commerce, wireless technologies, and ERP systems and implementation
- Provides examples of Computer Assisted Audit Tools and Techniques in development, application, and operational reviews such as computer forensics
- Discusses legal issues facing IT auditors as a result of HIPAA, Sarbanes–Oxley, the Homeland Security Act, and a method of evaluating the quality of IT audit work
- Includes an Instructor's Guide (with qualifying course adoption) that provides a complete map to teaching the course. It consists of course summary and objectives, analogies for chapter concepts, PowerPoint slides, and other supplementary materials

AU2032

ISBN 0-8493-2032-1

90000

9 780849 320323

AUERBACH PUBLICATIONS

www.auerbach-publications.com