### Contents

**Introduction** xxxv

**Assessment Test** xlv

### Chapter 1 Access Control 1

Access Control Overview 2
- Users, Owners, and Custodians 3
- The CIA Triad 3
- Policies 4
- Compare Permissions, Rights, and Privileges 4
- Types of Access Control 5
- Defense in Depth 7
- Access Control Elements 8

Identification and Authentication Techniques 11
- Passwords 12
- Smart Cards and Tokens 14
- Biometrics 17
- Multifactor Authentication 20

Access Control Techniques 21
- Security Operations Principles 21
- Discretionary Access Controls 22
- Nondiscretionary Access Controls 22
- Mandatory Access Controls 24
- Role-Based Access Control 25
- Centralized versus Decentralized Access Control 26
- Single Sign-On 27
- AAA Protocols 31
- Authorization Mechanisms 33

Identity and Access Provisioning Life Cycle 35
- Provisioning 35
- Account Review 36
- Account Revocation 37

Summary 38

Exam Essentials 39

Written Lab 41

Review Questions 42

### Chapter 2 Access Control Attacks and Monitoring 47

Understanding Access Control Attacks 48
- Introduction to Risk Elements 49
Asset Valuation 49
Threat Modeling 50
Vulnerability Analysis 53
Common Access Control Attacks 53
Preventing Access Control Attacks 62
Logging and Monitoring 64
Assessing Effectiveness of Access Controls 73
Handling Audit Reports 77
Summary 79
Exam Essentials 80
Written Lab 82
Review Questions 83

Chapter 3 Secure Network Architecture and Securing Network Components 87
OSI Model 88
   History of the OSI Model 89
   OSI Functionality 89
   Encapsulation/Deencapsulation 90
   OSI Layers 92
   TCP/IP Model 99
      TCP/IP Protocol Suite Overview 100
Secure Network Components 113
   Network Access Control 114
   Firewalls 115
   Endpoint Security 119
   Other Network Devices 119
Cabling, Wireless, Topology, and Communications Technology 123
   Network Cabling 123
   Wireless Communications and Security 128
   Network Topologies 137
   LAN Technologies 140
Summary 144
Exam Essentials 145
Written Lab 146
Review Questions 147

Chapter 4 Secure Communications and Network Attacks 151
Network and Protocol Security Mechanisms 152
   Secure Communications Protocols 153
   Authentication Protocols 154
Virtual Private Network 155
   Tunneling 155
   How VPNs Work 157
   Common VPN Protocols 157
   Virtual LAN 159
Remote Access Security Management 160
   Plan Remote Access Security 163
   Dial-Up Protocols 164
   Centralized Remote Authentication Services 165
Network Address Translation 165
   Private IP Addresses 167
   Stateful NAT 168
   Static and Dynamic NAT 168
   Automatic Private IP Addressing 169
Switching Technologies 170
   Circuit Switching 170
   Packet Switching 171
   Virtual Circuits 172
WAN Technologies 172
   WAN Connection Technologies 174
   Dial-Up Encapsulation Protocols 178
Virtualization 178
Miscellaneous Security Control Characteristics 179
   Transparency 179
   Verify Integrity 180
   Transmission Mechanisms 181
Manage Email Security 181
   Email SecurityGoals 181
   Understand Email Security Issues 183
   Email Security Solutions 183
Secure Voice Communications 186
   Social Engineering 186
   Fraud and Abuse 187
   Phreaking 189
Security Boundaries 190
Network Attacks and Countermeasures 190
   DoS and DDoS 191
   Eavesdropping 192
   Impersonation/Masquerading 193
   Replay Attacks 193
   Modification Attacks 193
   Address Resolution Protocol Spoofing 194
   DNS Poisoning, Spoofing, and Hijacking 194
   Hyperlink Spoofing 195

Security Management Planning 206
Security Governance 208
Security Roles and Responsibilities 209
Protection Mechanisms 210
   Layering 210
   Abstraction 211
   Data Hiding 211
   Encryption 211
Privacy Requirements Compliance 212
Control Frameworks: Planning to Plan 213
Security Management Concepts and Principles 214
   Confidentiality 214
   Integrity 215
   Availability 217
   Other Security Concepts 218
Develop and Implement Security Policy 221
   Security Policies 221
   Security Standards, Baselines, and Guidelines 222
   Security Procedures 223
Change Control/Management 224
Data Classification 225
Summary 229
Exam Essentials 230
Written Lab 233
Review Questions 234

Chapter 6  Risk and Personnel Management 239

Manage Third-Party Governance 240
Risk Management 241
   Risk Terminology 242
   Risk Assessment Methodologies 245
   Quantitative Risk Analysis 248
   Qualitative Risk Analysis 253
   Handle Risk 255
Chapter 7  Software Development Security  275

Application Issues  276
  Local/Nondistributed Computing  276
  Distributed Computing  278
Databases and Data Warehousing  282
  Database Management System Architecture  282
  Database Transactions  286
  Security for Multilevel Databases  287
  ODBC  289
  Aggregation  290
  Data Mining  291
Data/Information Storage  293
  Types of Storage  293
  Storage Threats  294
Knowledge-Based Systems  294
  Expert Systems  295
  Neural Networks  296
  Decision Support Systems  297
  Security Applications  297
Systems Development Controls  297
  Software Development  297
  Systems Development Life Cycle  303
  Life Cycle Models  306
  Gantt Charts and PERT  312
  Change and Configuration Management  313
  Software Testing  314
  Security Control Architecture  316
  Service-Level Agreements  318
Summary  319
Exam Essentials  319
Chapter 8 Malicious Code and Application Attacks 327

Malicious Code 328
Sources of Malicious Code 328
Viruses 329
Logic Bombs 335
Trojan Horses 335
Worms 336
Spyware and Adware 339
Active Content 339
Countermeasures 339
Password Attacks 341
Password Guessing 341
Dictionary Attacks 342
Social Engineering 343
Countermeasures 344
Application Attacks 344
Buffer Overflows 344
Time-of-Check-to-Time-of-Use 345
Back Doors 346
Escalation of Privilege and Rootkits 346
Web Application Security 346
Cross-Site Scripting (XSS) 347
SQL Injection 348
Reconnaissance Attacks 350
IP Probes 351
Port Scans 351
Vulnerability Scans 351
Dumpster Diving 352
Masquerading Attacks 352
IP Spoofing 352
Session Hijacking 353
Summary 353
Exam Essentials 354
Written Lab 355
Review Questions 356

Chapter 9 Cryptography and Symmetric Key Algorithms 361

Historical Milestones in Cryptography 362
Caesar Cipher 362
American Civil War 363
Ultra vs. Enigma 364
Cryptographic Basics 364
  Goals of Cryptography 364
  Cryptography Concepts 366
  Cryptographic Mathematics 368
  Ciphers 374
Modern Cryptography 380
  Cryptographic Keys 381
  Symmetric Key Algorithms 382
  Asymmetric Key Algorithms 383
  Hashing Algorithms 386
Symmetric Cryptography 386
  Data Encryption Standard 387
  Triple DES 389
  International Data Encryption Algorithm 390
  Blowfish 390
  Skipjack 390
  Advanced Encryption Standard 391
  Symmetric Key Management 393
Cryptographic Life Cycle 395
Summary 396
Exam Essentials 396
Written Lab 398
Review Questions 399

Chapter 10 PKI and Cryptographic Applications 403
Asymmetric Cryptography 405
  Public and Private Keys 405
  RSA 406
  El Gamal 408
  Elliptic Curve 408
Hash Functions 409
  SHA 410
  MD2 411
  MD4 411
  MD5 412
Digital Signatures 413
  HMAC 414
  Digital Signature Standard 415
Public Key Infrastructure 415
  Certificates 415
  Certificate Authorities 416
  Certificate Generation and Destruction 417
Asymmetric Key Management 419
Applied Cryptography 420
  Portable Devices 420
  Electronic Mail 421
  Web Applications 422
  Networking 425
Cryptographic Attacks 428
Summary 430
Exam Essentials 431
Written Lab 432
Review Questions 433

**Chapter 11 Principles of Security Models, Design, and Capabilities** 437

Understand the Fundamental Concepts of Security Models 438
  Trusted Computing Base 440
  State Machine Model 441
  Information Flow Model 441
  Noninterference Model 442
  Take-Grant Model 443
  Access Control Matrix 443
  Bell-LaPadula Model 444
  Biba Model 446
  Clark-Wilson Model 448
  Brewer and Nash Model (aka Chinese Wall) 449
  Goguen-Meseguer Model 449
  Sutherland Model 450
  Graham-Denning Model 450

Objects and Subjects 450
  Closed and Open Systems 451
  Techniques for Ensuring Confidentiality, Integrity, and Availability 452
  Controls 453
  Trust and Assurance 454

Understand the Components of Information Systems 454
  Security Evaluation Models 454
    Rainbow Series 455
    ITSEC Classes and Required Assurance and Functionality 460
    Common Criteria 461
    Industry and International Security Implementation Guidelines 465
    Certification and Accreditation 466
Chapter 12 Security Architecture Vulnerabilities, Threats, and Countermeasures 477

Computer Architecture 478
   Hardware 479
   Input/Output Structures 499
   Firmware 500
Avoiding Single Points of Failure 501
   Redundant Servers 501
   Failover Solutions 502
   RAID 502
Distributed Architecture 504
   Cloud Computing 508
Security Protection Mechanisms 510
   Technical Mechanisms 511
   Security Policy and Computer Architecture 513
   Policy Mechanisms 514
Common Flaws and Security Issues 515
   Covert Channels 515
   Attacks Based on Design or Coding
      Flaws and Security Issues 516
   Programming 520
   Timing, State Changes, and Communication
      Disconnects 520
   Technology and Process Integration 521
   Electromagnetic Radiation 521
Summary 522
Exam Essentials 522
Written Lab 525
Review Questions 526

Chapter 13 Security Operations 531

Security Operations Concepts 532
   Need to Know and Least Privilege 532
   Separation of Duties and Responsibilities 534
   Job Rotation 538
Chapter 14 Incident Management

Managing Incident Response 572
  Defining an Incident 572
  Incident Response Steps 573
Implement Preventive Measures Against Attacks 578
  Basic Preventive Measures 579
  Malicious Code 580
  Zero-Day-Exploit 582
  Denial-of-Service Attacks 583
  Miscellaneous Attacks 588
  Intrusion Detection and Prevention 590
  Penetration Testing 598
  Warning Banners 602
Understand System Resilience and Fault Tolerance 603
  Protecting Hard Drives 603
  Protecting Servers 605
  Protecting Power Sources 606
  Trusted Recovery 606
Summary 608
Exam Essentials 609
Written Lab 611
Review Questions 612
## Chapter 15  Business Continuity Planning 617

- Planning for Business Continuity 618
- Project Scope and Planning 619
  - Business Organization Analysis 620
  - BCP Team Selection 620
  - Resource Requirements 622
  - Legal and Regulatory Requirements 624
- Business Impact Assessment 625
  - Identify Priorities 626
  - Risk Identification 626
  - Likelihood Assessment 627
  - Impact Assessment 628
  - Resource Prioritization 629
- Continuity Planning 630
  - Strategy Development 630
  - Provisions and Processes 631
  - Plan Approval 633
  - Plan Implementation 633
  - Training and Education 633
- BCP Documentation 634
  - Continuity Planning Goals 634
  - Statement of Importance 634
  - Statement of Priorities 635
  - Statement of Organizational Responsibility 635
  - Statement of Urgency and Timing 635
  - Risk Assessment 635
  - Risk Acceptance/Mitigation 636
  - Vital Records Program 636
  - Emergency-Response Guidelines 636
  - Maintenance 636
  - Testing and Exercises 637

### Summary 637

Exam Essentials 637

Written Lab 638

Review Questions 639

## Chapter 16  Disaster Recovery Planning 643

- The Nature of Disaster 644
  - Natural Disasters 645
  - Man-Made Disasters 649
- Recovery Strategy 654
  - Business Unit and Functional Priorities 655
  - Crisis Management 656
Emergency Communications 656
Work Group Recovery 656
Alternate Processing Sites 657
Mutual Assistance Agreements 661
Database Recovery 662
Recovery Plan Development 663
Emergency Response 664
Personnel and Communications 664
Assessment 665
Backups and Offsite Storage 666
Software Escrow Arrangements 669
External Communications 670
Utilities 670
Logistics and Supplies 670
Recovery vs. Restoration 670
Training and Documentation 671
Testing and Maintenance 672
Checklist Test 672
Structured Walk-Through 673
Simulation Test 673
Parallel Test 673
Full- Interruption Test 673
Maintenance 674
Summary 674
Exam Essentials 675
Written Lab 675
Review Questions 676

Chapter 17  Laws, Regulations, and Compliance 681

Categories of Laws 682
Criminal Law 682
Civil Law 684
Administrative Law 684
Laws 685
Computer Crime 685
Intellectual Property 689
Licensing 695
Import/Export 696
Privacy 697
Compliance 703
Contracting and Procurement 704
Summary 705
Exam Essentials 706
Chapter 18 Incidents and Ethics

Investigations
Evidence
Investigation Process

Major Categories of Computer Crime
Military and Intelligence Attacks
Business Attacks
Financial Attacks
Terrorist Attacks
Grudge Attacks
Thrill Attacks

Incident Handling
Common Types of Incidents
Response Teams
Incident Response Process
Interviewing Individuals
Incident Data Integrity and Retention
Reporting Incidents

Ethics
(ISC)² Code of Ethics
Ethics and the Internet

Summary

Chapter 19 Physical Security Requirements

Site and Facility Design Considerations
Secure Facility Plan
Physical Security Controls
Site Selection
Visibility
Accessibility and Perimeter Security
Natural Disasters
Facility Design
Work Areas and Internal Security
Server Rooms and Data Center Security
Visitors

Forms of Physical Access Controls
Fences, Gates, Turnstiles, and Mantraps
Lighting 755
Security Guards and Dogs 755
Keys and Combination Locks 756
Badges 757
Motion Detectors 757
Intrusion Alarms 758
Secondary Verification Mechanisms 759
Technical Controls 760
Smart Cards 760
Proximity Readers 760
Access Abuses 761
Intrusion Detection Systems 761
Emanation Security 762
Environment and Life Safety 763
Personnel Privacy and Safety 763
Power and Electricity 764
Noise 765
Temperature, Humidity, and Static 766
Water 766
Fire Prevention, Detection, and Suppression 767
Equipment Failure 772
Privacy Responsibilities and Legal Requirements 772
Protection of Privacy 772
Regulatory Requirements 773
Summary 773
Exam Essentials 774
Written Lab 776
Review Questions 777

Appendix A  Answers to Review Questions 781
Appendix B  Answers to Written Labs 815
Appendix C  About the Additional Study Tools 829

Index 833