Contents

Introduction *xxxvii*

Assessment Test *lix*

Chapter 1 Security Governance Through Principles and Policies 1

Security 101 3
Understand and Apply Security Concepts 4
Confidentiality 5
Integrity 6
Availability 7
DAD, Overprotection, Authenticity, Non-repudiation, and AAA Services 7
Protection Mechanisms 11
Security Boundaries 13
Evaluate and Apply Security Governance Principles 14
Third-Party Governance 15
Documentation Review 15
Manage the Security Function 16
Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives 17
Organizational Processes 19
Organizational Roles and Responsibilities 21
Security Control Frameworks 22
Due Diligence and Due Care 23
Security Policy, Standards, Procedures, and Guidelines 23
Security Policies 24
Security Standards, Baselines, and Guidelines 24
Security Procedures 25
Threat Modeling 26
Identifying Threats 26
Determining and Diagramming Potential Attacks 28
Performing Reduction Analysis 28
Prioritization and Response 30
Supply Chain Risk Management 31
Summary 33
Exam Essentials 33
Written Lab 36
Review Questions 37

COPYRIGHTED MATERIAL

Chapter 2 Personnel Security and Risk Management Concepts 43

Personnel Security Policies and Procedures 45
- Job Descriptions and Responsibilities 45
- Candidate Screening and Hiring 46
- Onboarding: Employment Agreements and Policies 47
- Employee Oversight 48
- Offboarding, Transfers, and Termination Processes 49
- Vendor, Consultant, and Contractor Agreements and Controls 52
- Compliance Policy Requirements 53
- Privacy Policy Requirements 54

Understand and Apply Risk Management Concepts 55
- Risk Terminology and Concepts 56
- Asset Valuation 58
- Identify Threats and Vulnerabilities 60
- Risk Assessment/Analysis 60
- Risk Responses 66
- Cost vs. Benefit of Security Controls 69
- Countermeasure Selection and Implementation 72
- Applicable Types of Controls 74
- Security Control Assessment 76
- Monitoring and Measurement 76
- Risk Reporting and Documentation 77
- Continuous Improvement 77
- Risk Frameworks 79

Social Engineering 81
- Social Engineering Principles 83
- Eliciting Information 85
- Prepending 85
- Phishing 85
- Spear Phishing 87
- Whaling 87
- Smishing 88
- Vishing 88
- Spam 89
- Shoulder Surfing 90
- Invoice Scams 90
- Hoax 90
- Impersonation and Masquerading 91
- Tailgating and Piggybacking 91
- Dumpster Diving 92
- Identity Fraud 93
- Typo Squatting 94
- Influence Campaigns 94

Establish and Maintain a Security Awareness, Education, and Training Program 96
    Awareness 97
    Training 97
    Education 98
    Improvements 98
    Effectiveness Evaluation 99
Summary 100
Exam Essentials 101
Written Lab 106
Review Questions 107

Chapter 3 Business Continuity Planning 113

Planning for Business Continuity 114
Project Scope and Planning 115
    Organizational Review 116
    BCP Team Selection 117
    Resource Requirements 119
    Legal and Regulatory Requirements 120
Business Impact Analysis 121
    Identifying Priorities 122
    Risk Identification 123
    Likelihood Assessment 125
    Impact Analysis 126
    Resource Prioritization 128
Continuity Planning 128
    Strategy Development 129
    Provisions and Processes 129
Plan Approval and Implementation 131
    Plan Approval 131
    Plan Implementation 132
    Training and Education 132
    BCP Documentation 132
Summary 136
Exam Essentials 137
Written Lab 138
Review Questions 139

Chapter 4 Laws, Regulations, and Compliance 143

Categories of Laws 144
    Criminal Law 144
    Civil Law 146
    Administrative Law 146
Laws 147
    Computer Crime 147
    Intellectual Property (IP) 152

Licensing 158
Import/Export 158
Privacy 160
State Privacy Laws 168
Compliance 169
Contracting and Procurement 171
Summary 171
Exam Essentials 172
Written Lab 173
Review Questions 174

Chapter 5 Protecting Security of Assets 179

Identifying and Classifying Information and Assets 180
Defining Sensitive Data 180
Defining Data Classifications 182
Defining Asset Classifications 185
Understanding Data States 185
Determining Compliance Requirements 186
Determining Data Security Controls 186
Establishing Information and Asset Handling Requirements 188
Data Maintenance 189
Data Loss Prevention 189
Marking Sensitive Data and Assets 190
Handling Sensitive Information and Assets 192
Data Collection Limitation 192
Data Location 193
Storing Sensitive Data 193
Data Destruction 194
Ensuring Appropriate Data and Asset Retention 197
Data Protection Methods 199
Digital Rights Management 199
Cloud Access Security Broker 200
Pseudonymization 200
Tokenization 201
Anonymization 202
Understanding Data Roles 204
Data Owners 204
Asset Owners 205
Business/Mission Owners 206
Data Processors and Data Controllers 206
Data Custodians 207
Administrators 207
Users and Subjects 208

Using Security Baselines 208
Comparing Tailoring and Scoping 209
Standards Selection 210
Summary 211
Exam Essentials 211
Written Lab 213
Review Questions 214

Chapter 6 Cryptography and Symmetric Key Algorithms 219

Cryptographic Foundations 220
Goals of Cryptography 220
Cryptography Concepts 223
Cryptographic Mathematics 224
Ciphers 230
Modern Cryptography 238
Cryptographic Keys 238
Symmetric Key Algorithms 239
Asymmetric Key Algorithms 241
Hashing Algorithms 244
Symmetric Cryptography 244
Cryptographic Modes of Operation 245
Data Encryption Standard 247
Triple DES 247
International Data Encryption Algorithm 248
Blowfish 249
Skipjack 249
Rivest Ciphers 249
Advanced Encryption Standard 250
CAST 250
Comparison of Symmetric Encryption Algorithms 251
Symmetric Key Management 252
Cryptographic Lifecycle 255
Summary 255
Exam Essentials 256
Written Lab 257
Review Questions 258

Chapter 7 PKI and Cryptographic Applications 263

Asymmetric Cryptography 264
Public and Private Keys 264
RSA 265
ElGamal 267
Elliptic Curve 268
Diffie–Hellman Key Exchange 269
Quantum Cryptography 270

Hash Functions 271
SHA 272
MD5 273
RIPEMD 273
Comparison of Hash Algorithm Value Lengths 274
Digital Signatures 275
HMAC 276
Digital Signature Standard 277
Public Key Infrastructure 277
Certificates 278
Certificate Authorities 279
Certificate Lifecycle 280
Certificate Formats 283
Asymmetric Key Management 284
Hybrid Cryptography 285
Applied Cryptography 285
Portable Devices 285
Email 286
Web Applications 290
Steganography and Watermarking 292
Networking 294
Emerging Applications 295
Cryptographic Attacks 297
Summary 301
Exam Essentials 302
Written Lab 303
Review Questions 304

Chapter 8 Principles of Security Models, Design, and Capabilities 309

Secure Design Principles 310
Objects and Subjects 311
Closed and Open Systems 312
Secure Defaults 314
Fail Securely 314
Keep It Simple 316
Zero Trust 317
Privacy by Design 319
Trust but Verify 319
Techniques for Ensuring CIA 320
Confinement 320
Bounds 320
Isolation 321
Access Controls 321
Trust and Assurance 321

Understand the Fundamental Concepts of Security Models 322
Trusted Computing Base 323
State Machine Model 325
Information Flow Model 325
Noninterference Model 326
Take-Grant Model 326
Access Control Matrix 327
Bell–LaPadula Model 328
Biba Model 330
Clark–Wilson Model 333
Brewer and Nash Model 334
Goguen–Meseguer Model 335
Sutherland Model 335
Graham–Denning Model 335
Harrison–Ruzzo–Ullman Model 336
Select Controls Based on Systems Security Requirements 337
Common Criteria 337
Authorization to Operate 340
Understand Security Capabilities of Information Systems 341
Memory Protection 341
Virtualization 342
Trusted Platform Module 342
Interfaces 343
Fault Tolerance 343
Encryption/Decryption 343
Summary 343
Exam Essentials 344
Written Lab 347
Review Questions 348

Chapter 9 Security Vulnerabilities, Threats, and Countermeasures 353

Shared Responsibility 354
Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements 355
Hardware 356
Firmware 370
Client-Based Systems 372
Mobile Code 372
Local Caches 375
Server-Based Systems 375
Large-Scale Parallel Data Systems 376
Grid Computing 377
Peer to Peer 378

Industrial Control Systems 378
Distributed Systems 380
High-Performance Computing (HPC) Systems 382
Internet of Things 383
Edge and Fog Computing 385
Embedded Devices and Cyber-Physical Systems 386
Static Systems 387
Network-Enabled Devices 388
Cyber-Physical Systems 389
Elements Related to Embedded and Static Systems 389
Security Concerns of Embedded and Static Systems 390
Specialized Devices 393
Microservices 394
Infrastructure as Code 395
Virtualized Systems 397
Virtual Software 399
Virtualized Networking 400
Software-Defined Everything 400
Virtualization Security Management 403
Containerization 405
Serverless Architecture 406
Mobile Devices 406
Mobile Device Security Features 408
Mobile Device Deployment Policies 420
Essential Security Protection Mechanisms 426
Process Isolation 426
Hardware Segmentation 427
System Security Policy 427
Common Security Architecture Flaws and Issues 428
Covert Channels 428
Attacks Based on Design or Coding Flaws 430
Rootkits 431
Incremental Attacks 431
Summary 432
Exam Essentials 433
Written Lab 440
Review Questions 441

Chapter 10 Physical Security Requirements 447

Apply Security Principles to Site and Facility Design 448
Secure Facility Plan 448
Site Selection 449
Facility Design 450

Implement Site and Facility Security Controls 452
Equipment Failure 453
Wiring Closets 454
Server Rooms/Data Centers 455
Intrusion Detection Systems 458
Cameras 460
Access Abuses 462
Media Storage Facilities 462
Evidence Storage 463
Restricted and Work Area Security 464
Utility Considerations 465
Fire Prevention, Detection, and Suppression 470
Implement and Manage Physical Security 476
Perimeter Security Controls 477
Internal Security Controls 481
Key Performance Indicators of Physical Security 483
Summary 484
Exam Essentials 485
Written Lab 488
Review Questions 489

Chapter 11 Secure Network Architecture and Components 495

OSI Model 497
History of the OSI Model 497
OSI Functionality 498
Encapsulation/Deencapsulation 498
OSI Layers 500
TCP/IP Model 504
Analyzing Network Traffic 505
Common Application Layer Protocols 506
Transport Layer Protocols 508
Domain Name System 509
DNS Poisoning 511
Domain Hijacking 514
Internet Protocol (IP) Networking 516
IPv4 vs. IPv6 516
IP Classes 517
ICMP 519
IGMP 519
ARP Concerns 519
Secure Communication Protocols 521
Implications of Multilayer Protocols 522
Converged Protocols 523
Voice over Internet Protocol (VoIP) 524
Software-Defined Networking 525

Microsegmentation 526
Wireless Networks 527
Securing the SSID 529
Wireless Channels 529
Conducting a Site Survey 530
Wireless Security 531
Wi-Fi Protected Setup (WPS) 533
Wireless MAC Filter 534
Wireless Antenna Management 534
Using Captive Portals 535
General Wi-Fi Security Procedure 535
Wireless Communications 536
Wireless Attacks 539
Other Communication Protocols 543
Cellular Networks 544
Content Distribution Networks (CDNs) 545
Secure Network Components 545
Secure Operation of Hardware 546
Common Network Equipment 547
Network Access Control 549
Firewalls 550
Endpoint Security 556
Cabling, Topology, and Transmission Media Technology 559
Transmission Media 559
Network Topologies 563
Ethernet 565
Sub-Technologies 566
Summary 569
Exam Essentials 570
Written Lab 574
Review Questions 575

Chapter 12 Secure Communications and Network Attacks 581

Protocol Security Mechanisms 582
Authentication Protocols 582
Port Security 585
Quality of Service (QoS) 585
Secure Voice Communications 586
Public Switched Telephone Network 586
Voice over Internet Protocol (VoIP) 586
Vishing and Phreaking 588
PBX Fraud and Abuse 589
Remote Access Security Management 590
Remote Access and Telecommuting Techniques 591
Remote Connection Security 591
Plan a Remote Access Security Policy 592

Multimedia Collaboration 593
Remote Meeting 593
Instant Messaging and Chat 594
Load Balancing 595
Virtual IPs and Load Persistence 596
Active-Active vs. Active-Passive 596
Manage Email Security 596
Email Security Goals 597
Understand Email Security Issues 599
Email Security Solutions 599
Virtual Private Network 602
Tunneling 603
How VPNs Work 604
Always-On 606
Split Tunnel vs. Full Tunnel 607
Common VPN Protocols 607
Switching and Virtual LANs 610
Network Address Translation 614
Private IP Addresses 616
Stateful NAT 617
Automatic Private IP Addressing 617
Third-Party Connectivity 618
Switching Technologies 620
Circuit Switching 620
Packet Switching 620
Virtual Circuits 621
WAN Technologies 622
Fiber-Optic Links 624
Security Control Characteristics 624
Transparency 625
Transmission Management Mechanisms 625
Prevent or Mitigate Network Attacks 625
Eavesdropping 626
Modification Attacks 626
Summary 626
Exam Essentials 628
Written Lab 630
Review Questions 631

Chapter 13 Managing Identity and Authentication 637

Controlling Access to Assets 639
Controlling Physical and Logical Access 640
The CIA Triad and Access Controls 640
Managing Identification and Authentication 641
Comparing Subjects and Objects 642

Registration, Proofing, and Establishment of Identity 643
Authorization and Accountability 644
Authentication Factors Overview 645
Something You Know 647
Something You Have 650
Something You Are 651
Multifactor Authentication (MFA) 655
Two-Factor Authentication with Authenticator Apps 655
Passwordless Authentication 656
Device Authentication 657
Service Authentication 658
Mutual Authentication 659
Implementing Identity Management 659
Single Sign-On 659
SSO and Federated Identities 660
Credential Management Systems 662
Credential Manager Apps 663
Scripted Access 663
Session Management 663
Managing the Identity and Access Provisioning Lifecycle 664
Provisioning and Onboarding 665
Deprovisioning and Offboarding 666
Defining New Roles 667
Account Maintenance 667
Account Access Review 667
Summary 668
Exam Essentials 669
Written Lab 671
Review Questions 672

Chapter 14 Controlling and Monitoring Access 677

Comparing Access Control Models 678
Comparing Permissions, Rights, and Privileges 678
Understanding Authorization Mechanisms 679
Defining Requirements with a Security Policy 681
Introducing Access Control Models 681
Discretionary Access Control 682
Nondiscretionary Access Control 683
Implementing Authentication Systems 690
Implementing SSO on the Internet 691
Implementing SSO on Internal Networks 694
Understanding Access Control Attacks 699
Risk Elements 700
Common Access Control Attacks 700
Core Protection Methods 713

Summary 714
Exam Essentials 715
Written Lab 717
Review Questions 718

Chapter 15 Security Assessment and Testing 723

Building a Security Assessment and Testing Program 725
- Security Testing 725
- Security Assessments 726
- Security Audits 727

Performing Vulnerability Assessments 731
- Describing Vulnerabilities 731
- Vulnerability Scans 732
- Penetration Testing 742
- Compliance Checks 745

Testing Your Software 746
- Code Review and Testing 746
- Interface Testing 751
- Misuse Case Testing 751
- Test Coverage Analysis 752
- Website Monitoring 752

Implementing Security Management Processes 753
- Log Reviews 753
- Account Management 754
- Disaster Recovery and Business Continuity 754
- Training and Awareness 755
- Key Performance and Risk Indicators 755

Summary 756
Exam Essentials 756
Written Lab 758
Review Questions 759

Chapter 16 Managing Security Operations 763

Apply Foundational Security Operations Concepts 765
- Need to Know and Least Privilege 765
- Separation of Duties (SoD) and Responsibilities 767
- Two-Person Control 768
- Job Rotation 768
- Mandatory Vacations 768
- Privileged Account Management 769
- Service Level Agreements (SLAs) 771

Addressing Personnel Safety and Security 771
- Duress 771
- Travel 772

Emergency Management 773
Security Training and Awareness 773
Provision Resources Securely 773
Information and Asset Ownership 774
Asset Management 774
Apply Resource Protection 776
Media Management 776
Media Protection Techniques 776
Managed Services in the Cloud 779
Shared Responsibility with Cloud Service Models 780
Scalability and Elasticity 782
Perform Configuration Management (CM) 782
Provisioning 783
Baselining 783
Using Images for Baselining 783
Automation 784
Managing Change 785
Change Management 787
Versioning 788
Configuration Documentation 788
Managing Patches and Reducing Vulnerabilities 789
Systems to Manage 789
Patch Management 789
Vulnerability Management 791
Vulnerability Scans 792
Common Vulnerabilities and Exposures 792
Summary 793
Exam Essentials 794
Written Lab 796
Review Questions 797

Chapter 17 Preventing and Responding to Incidents 801

Conducting Incident Management 803
Defining an Incident 803
Incident Management Steps 804
Implementing Detective and Preventive Measures 810
Basic Preventive Measures 810
Understanding Attacks 811
Intrusion Detection and Prevention Systems 820
Specific Preventive Measures 828
Logging and Monitoring 834
Logging Techniques 834
The Role of Monitoring 837
Monitoring Techniques 840

Log Management 844
Egress Monitoring 844
Automating Incident Response 845
Understanding SOAR 845
Machine Learning and AI Tools 846
Threat Intelligence 847
The Intersection of SOAR, Machine Learning, AI, and Threat Feeds 850
Summary 851
Exam Essentials 852
Written Lab 855
Review Questions 856

Chapter 18 Disaster Recovery Planning 861

The Nature of Disaster 863
Natural Disasters 864
Human-Made Disasters 869
Understand System Resilience, High Availability, and Fault Tolerance 875
Protecting Hard Drives 875
Protecting Servers 877
Protecting Power Sources 878
Trusted Recovery 879
Quality of Service 880
Recovery Strategy 880
Business Unit and Functional Priorities 881
Crisis Management 882
Emergency Communications 882
Workgroup Recovery 883
Alternate Processing Sites 883
Database Recovery 888
Recovery Plan Development 890
Emergency Response 891
Personnel and Communications 891
Assessment 892
Backups and Off-site Storage 892
Software Escrow Arrangements 896
Utilities 897
Logistics and Supplies 897
Recovery vs. Restoration 897
Training, Awareness, and Documentation 898
Testing and Maintenance 899
Read-Through Test 899
Structured Walk-Through 900

Simulation Test 900
Parallel Test 900
Full-Interruption Test 900
Lessons Learned 901
Maintenance 901
Summary 902
Exam Essentials 902
Written Lab 903
Review Questions 904

Chapter 19 Investigations and Ethics 909

Investigations 910
Investigation Types 910
Evidence 913
Investigation Process 919
Major Categories of Computer Crime 923
Military and Intelligence Attacks 924
Business Attacks 925
Financial Attacks 926
Terrorist Attacks 926
Grudge Attacks 927
Thrill Attacks 928
Hacktivists 928
Ethics 929
Organizational Code of Ethics 929
(ISC)^2 Code of Ethics 930
Ethics and the Internet 931
Summary 933
Exam Essentials 934
Written Lab 935
Review Questions 936

Chapter 20 Software Development Security 941

Introducing Systems Development Controls 943
Software Development 943
Systems Development Lifecycle 952
Lifecycle Models 955
Gantt Charts and PERT 964
Change and Configuration Management 964
The DevOps Approach 966
Application Programming Interfaces 967
Software Testing 969
Code Repositories 970
Service-Level Agreements 971
Third-Party Software Acquisition 972

Establishing Databases and Data Warehousing 973
Database Management System Architecture 973
Database Transactions 977
Security for Multilevel Databases 978
Open Database Connectivity 982
NoSQL 982
Storage Threats 983
Understanding Knowledge-Based Systems 984
Expert Systems 984
Machine Learning 985
Neural Networks 986
Summary 987
Exam Essentials 987
Written Lab 988
Review Questions 989

Chapter 21 Malicious Code and Application Attacks 993

Malware 994
Sources of Malicious Code 995
Viruses 995
Logic Bombs 999
Trojan Horses 1000
Worms 1001
Spyware and Adware 1004
Ransomware 1004
Malicious Scripts 1005
Zero-Day Attacks 1006
Malware Prevention 1006
Platforms Vulnerable to Malware 1007
Antimalware Software 1007
Integrity Monitoring 1008
Advanced Threat Protection 1008
Application Attacks 1009
Buffer Overflows 1009
Time of Check to Time of Use 1010
Backdoors 1011
Privilege Escalation and Rootkits 1011
Injection Vulnerabilities 1012
SQL Injection Attacks 1012
Code Injection Attacks 1016
Command Injection Attacks 1016
Exploiting Authorization Vulnerabilities 1017
Insecure Direct Object References 1018

Directory Traversal 1018
File Inclusion 1020
Exploiting Web Application Vulnerabilities 1020
Cross-Site Scripting (XSS) 1021
Request Forgery 1023
Session Hijacking 1024
Application Security Controls 1025
Input Validation 1025
Web Application Firewalls 1027
Database Security 1028
Code Security 1029
Secure Coding Practices 1031
Source Code Comments 1031
Error Handling 1032
Hard-Coded Credentials 1033
Memory Management 1034
Summary 1035
Exam Essentials 1035
Written Lab 1036
Review Questions 1037

Appendix A Answers to Review Questions 1041

Chapter 1: Security Governance Through Principles and Policies 1042
Chapter 2: Personnel Security and Risk Management Concepts 1045
Chapter 3: Business Continuity Planning 1049
Chapter 4: Laws, Regulations, and Compliance 1051
Chapter 5: Protecting Security of Assets 1053
Chapter 6: Cryptography and Symmetric Key Algorithms 1056
Chapter 7: PKI and Cryptographic Applications 1058
Chapter 8: Principles of Security Models, Design, and Capabilities 1060
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures 1062
Chapter 10: Physical Security Requirements 1067
Chapter 11: Secure Network Architecture and Components 1071
Chapter 12: Secure Communications and Network Attacks 1075
Chapter 13: Managing Identity and Authentication 1078
Chapter 14: Controlling and Monitoring Access 1080
Chapter 15: Security Assessment and Testing 1082
Chapter 16: Managing Security Operations 1084
Chapter 17: Preventing and Responding to Incidents 1086

Chapter 18: Disaster Recovery Planning 1089
Chapter 19: Investigations and Ethics 1091
Chapter 20: Software Development Security 1093
Chapter 21: Malicious Code and Application Attacks 1095

Appendix B Answers to Written Labs 1099

Chapter 1: Security Governance Through Principles and Policies 1100
Chapter 2: Personnel Security and Risk Management Concepts 1100
Chapter 3: Business Continuity Planning 1101
Chapter 4: Laws, Regulations, and Compliance 1102
Chapter 5: Protecting Security of Assets 1102
Chapter 6: Cryptography and Symmetric Key Algorithms 1103
Chapter 7: PKI and Cryptographic Applications 1104
Chapter 8: Principles of Security Models, Design, and Capabilities 1104
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures 1105
Chapter 10: Physical Security Requirements 1106
Chapter 11: Secure Network Architecture and Components 1108
Chapter 12: Secure Communications and Network Attacks 1109
Chapter 13: Managing Identity and Authentication 1110
Chapter 14: Controlling and Monitoring Access 1111
Chapter 15: Security Assessment and Testing 1111
Chapter 16: Managing Security Operations 1112
Chapter 17: Preventing and Responding to Incidents 1113
Chapter 18: Disaster Recovery Planning 1113
Chapter 19: Investigations and Ethics 1114
Chapter 20: Software Development Security 1114
Chapter 21: Malicious Code and Application Attacks 1115

Index 1117