Contents at a Glance

Introduction *xxxiii*

Assessment Test *xlii*

Chapter 1 Security Governance Through Principles and Policies 1

Chapter 2 Personnel Security and Risk Management Concepts 49

Chapter 3 Business Continuity Planning 97

Chapter 4 Laws, Regulations, and Compliance 125

Chapter 5 Protecting Security of Assets 159

Chapter 6 Cryptography and Symmetric Key Algorithms 195

Chapter 7 PKI and Cryptographic Applications 237

Chapter 8 Principles of Security Models, Design, and Capabilities 275

Chapter 9 Security Vulnerabilities, Threats, and Countermeasures 319

Chapter 10 Physical Security Requirements 399

Chapter 11 Secure Network Architecture and Securing Network Components 439

Chapter 12 Secure Communications and Network Attacks 521

Chapter 13 Managing Identity and Authentication 579

Chapter 14 Controlling and Monitoring Access 623

Chapter 15 Security Assessment and Testing 661

Chapter 16 Managing Security Operations 697

Chapter 17 Preventing and Responding to Incidents 737

Chapter 18 Disaster Recovery Planning 801

Chapter 19 Investigations and Ethics 845

Chapter 20 Software Development Security 871

Chapter 21 Malicious Code and Application Attacks 915

Appendix A Answers to Review Questions 949

Appendix B Answers to Written Labs 987

Index *1001*

Contents

Introduction *xxxiii*

Assessment Test *xlii*

Chapter 1 **Security Governance Through Principles and Policies** **1**

Understand and Apply Concepts of Confidentiality, Integrity, and Availability 2
Confidentiality 3
Integrity 4
Availability 6
Other Security Concepts 8
Protection Mechanisms 12
Layering 12
Abstraction 13
Data Hiding 13
Encryption 14
Evaluate and Apply Security Governance Principles 14
Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives 15
Organizational Processes 17
Organizational Roles and Responsibilities 23
Security Control Frameworks 25
Due Care and Due Diligence 26
Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines 26
Security Policies 26
Security Standards, Baselines, and Guidelines 28
Security Procedures 28
Understand and Apply Threat Modeling Concepts and Methodologies 30
Identifying Threats 31
Determining and Diagramming Potential Attacks 35
Performing Reduction Analysis 36
Prioritization and Response 37
Apply Risk-Based Management Concepts to the Supply Chain 38
Summary 40
Exam Essentials 42
Written Lab 44
Review Questions 45

Chapter 2 Personnel Security and Risk Management Concepts 49

Personnel Security Policies and Procedures 51
- Candidate Screening and Hiring 55
- Employment Agreements and Policies 55
- Onboarding and Termination Processes 57
- Vendor, Consultant, and Contractor Agreements and Controls 60
- Compliance Policy Requirements 60
- Privacy Policy Requirements 61

Security Governance 62

Understand and Apply Risk Management Concepts 63
- Risk Terminology 64
- Identify Threats and Vulnerabilities 67
- Risk Assessment/Analysis 68
- Risk Responses 76
- Countermeasure Selection and Implementation 77
- Applicable Types of Controls 79
- Security Control Assessment 81
- Monitoring and Measurement 81
- Asset Valuation and Reporting 82
- Continuous Improvement 83
- Risk Frameworks 83

Establish and Maintain a Security Awareness, Education, and Training Program 86

Manage the Security Function 87

Summary 88

Exam Essentials 89

Written Lab 92

Review Questions 93

Chapter 3 Business Continuity Planning 97

Planning for Business Continuity 98

Project Scope and Planning 99
- Business Organization Analysis 100
- BCP Team Selection 101
- Resource Requirements 103
- Legal and Regulatory Requirements 104

Business Impact Assessment 105
- Identify Priorities 106
- Risk Identification 107
- Likelihood Assessment 108
- Impact Assessment 110
- Resource Prioritization 111

Continuity Planning 111
Strategy Development 112
Provisions and Processes 112
Plan Approval and Implementation 114
Plan Approval 114
Plan Implementation 114
Training and Education 115
BCP Documentation 115
Summary 119
Exam Essentials 119
Written Lab 120
Review Questions 121

Chapter 4 Laws, Regulations, and Compliance 125

Categories of Laws 126
Criminal Law 126
Civil Law 128
Administrative Law 128
Laws 129
Computer Crime 129
Intellectual Property 134
Licensing 139
Import/Export 140
Privacy 141
Compliance 149
Contracting and Procurement 150
Summary 151
Exam Essentials 152
Written Lab 153
Review Questions 154

Chapter 5 Protecting Security of Assets 159

Identify and Classify Assets 160
Defining Sensitive Data 160
Defining Data Classifications 162
Defining Asset Classifications 165
Determining Data Security Controls 165
Understanding Data States 168
Handling Information and Assets 169
Data Protection Methods 176
Determining Ownership 178
Data Owners 179
Asset Owners 179

Business/Mission Owners 180
Data Processors 181
Administrators 184
Custodians 184
Users 185
Protecting Privacy 185
Using Security Baselines 186
Scoping and Tailoring 187
Selecting Standards 187
Summary 187
Exam Essentials 188
Written Lab 189
Review Questions 190

Chapter 6 Cryptography and Symmetric Key Algorithms 195

Historical Milestones in Cryptography 196
Caesar Cipher 196
American Civil War 197
Ultra vs. Enigma 198
Cryptographic Basics 198
Goals of Cryptography 198
Cryptography Concepts 200
Cryptographic Mathematics 202
Ciphers 207
Modern Cryptography 214
Cryptographic Keys 214
Symmetric Key Algorithms 215
Asymmetric Key Algorithms 216
Hashing Algorithms 219
Symmetric Cryptography 219
Data Encryption Standard 220
Triple DES 222
International Data Encryption Algorithm 223
Blowfish 223
Skipjack 223
Advanced Encryption Standard 224
Symmetric Key Management 226
Cryptographic Lifecycle 228
Summary 229
Exam Essentials 229
Written Lab 231
Review Questions 232

Chapter 7	**PKI and Cryptographic Applications**	**237**
	Asymmetric Cryptography	238
	Public and Private Keys	238
	RSA	239
	El Gamal	241
	Elliptic Curve	242
	Hash Functions	242
	SHA	244
	MD2	244
	MD4	245
	MD5	245
	Digital Signatures	246
	HMAC	247
	Digital Signature Standard	248
	Public Key Infrastructure	249
	Certificates	249
	Certificate Authorities	250
	Certificate Generation and Destruction	251
	Asymmetric Key Management	253
	Applied Cryptography	254
	Portable Devices	254
	Email	255
	Web Applications	256
	Digital Rights Management	259
	Networking	262
	Cryptographic Attacks	265
	Summary	268
	Exam Essentials	269
	Written Lab	270
	Review Questions	271
Chapter 8	**Principles of Security Models, Design, and Capabilities**	**275**
	Implement and Manage Engineering Processes Using Secure Design Principles	276
	Objects and Subjects	277
	Closed and Open Systems	277
	Techniques for Ensuring Confidentiality, Integrity, and Availability	279
	Controls	280
	Trust and Assurance	281
	Understand the Fundamental Concepts of Security Models	281
	Trusted Computing Base	282
	State Machine Model	284

Information Flow Model 285
Noninterference Model 285
Take-Grant Model 286
Access Control Matrix 286
Bell-LaPadula Model 288
Biba Model 290
Clark-Wilson Model 292
Brewer and Nash Model (aka Chinese Wall) 293
Goguen-Meseguer Model 294
Sutherland Model 294
Graham-Denning Model 294
Select Controls Based On Systems Security Requirements 295
Rainbow Series 296
ITSEC Classes and Required Assurance and Functionality 301
Common Criteria 302
Industry and International Security Implementation Guidelines 305
Certification and Accreditation 306
Understand Security Capabilities of Information Systems 309
Memory Protection 309
Virtualization 310
Trusted Platform Module 310
Interfaces 311
Fault Tolerance 311
Summary 311
Exam Essentials 312
Written Lab 313
Review Questions 314

Chapter 9 Security Vulnerabilities, Threats, and Countermeasures 319

Assess and Mitigate Security Vulnerabilities 320
Hardware 321
Firmware 341
Client-Based Systems 342
Applets 342
Local Caches 344
Server-Based Systems 346
Database Systems Security 347
Aggregation 347
Inference 348
Data Mining and Data Warehousing 348
Data Analytics 349
Large-Scale Parallel Data Systems 350

Distributed Systems and Endpoint Security 350
Cloud-Based Systems and Cloud Computing 353
Grid Computing 357
Peer to Peer 358
Internet of Things 358
Industrial Control Systems 359
Assess and Mitigate Vulnerabilities in Web-Based Systems 360
Assess and Mitigate Vulnerabilities in Mobile Systems 365
Device Security 366
Application Security 370
BYOD Concerns 372
Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems 375
Examples of Embedded and Static Systems 376
Methods of Securing Embedded and Static Systems 377
Essential Security Protection Mechanisms 379
Technical Mechanisms 380
Security Policy and Computer Architecture 383
Policy Mechanisms 383
Common Architecture Flaws and Security Issues 384
Covert Channels 385
Attacks Based on Design or Coding Flaws and Security Issues 385
Programming 388
Timing, State Changes, and Communication Disconnects 389
Technology and Process Integration 389
Electromagnetic Radiation 389
Summary 390
Exam Essentials 391
Written Lab 394
Review Questions 395

Chapter 10 Physical Security Requirements 399

Apply Security Principles to Site and Facility Design 400
Secure Facility Plan 401
Site Selection 401
Visibility 402
Natural Disasters 402
Facility Design 402
Implement Site and Facility Security Controls 403
Equipment Failure 404
Wiring Closets 405
Server Rooms/Data Centers 407
Media Storage Facilities 412

Evidence Storage 413
Restricted and Work Area Security 413
Utilities and HVAC Considerations 414
Fire Prevention, Detection, and Suppression 417
Implement and Manage Physical Security 422
Perimeter Security Controls 422
Internal Security Controls 425
Summary 431
Exam Essentials 432
Written Lab 434
Review Questions 435

Chapter 11 Secure Network Architecture and Securing Network Components 439

OSI Model 440
History of the OSI Model 441
OSI Functionality 441
Encapsulation/Deencapsulation 442
OSI Layers 444
TCP/IP Model 451
TCP/IP Protocol Suite Overview 452
Converged Protocols 470
Content Distribution Networks 472
Wireless Networks 472
Securing Wireless Access Points 473
Securing the SSID 475
Conducting a Site Survey 476
Using Secure Encryption Protocols 476
Determining Antenna Placement 479
Antenna Types 480
Adjusting Power Level Controls 480
WPS 481
Using Captive Portals 481
General Wi-Fi Security Procedure 481
Wireless Attacks 482
Secure Network Components 486
Network Access Control 487
Firewalls 487
Endpoint Security 491
Secure Operation of Hardware 492
Cabling, Wireless, Topology, Communications, and Transmission Media Technology 495
Transmission Media 496
Network Topologies 500

Wireless Communications and Security 503
LAN Technologies 509
Summary 513
Exam Essentials 514
Written Lab 516
Review Questions 517

Chapter 12 Secure Communications and Network Attacks 521

Network and Protocol Security Mechanisms 522
Secure Communications Protocols 523
Authentication Protocols 524
Secure Voice Communications 525
Voice over Internet Protocol (VoIP) 525
Social Engineering 526
Fraud and Abuse 527
Multimedia Collaboration 529
Remote Meeting 529
Instant Messaging 530
Manage Email Security 530
Email Security Goals 531
Understand Email Security Issues 532
Email Security Solutions 533
Remote Access Security Management 536
Plan Remote Access Security 538
Dial-Up Protocols 539
Centralized Remote Authentication Services 540
Virtual Private Network 540
Tunneling 541
How VPNs Work 542
Common VPN Protocols 543
Virtual LAN 545
Virtualization 546
Virtual Software 547
Virtual Networking 548
Network Address Translation 549
Private IP Addresses 550
Stateful NAT 551
Static and Dynamic NAT 552
Automatic Private IP Addressing 552
Switching Technologies 553
Circuit Switching 554
Packet Switching 554
Virtual Circuits 555

WAN Technologies 556
- WAN Connection Technologies 558
- Dial-Up Encapsulation Protocols 561

Miscellaneous Security Control Characteristics 561
- Transparency 561
- Verify Integrity 562
- Transmission Mechanisms 562

Security Boundaries 563

Prevent or Mitigate Network Attacks 564
- DoS and DDoS 564
- Eavesdropping 565
- Impersonation/Masquerading 566
- Replay Attacks 567
- Modification Attacks 567
- Address Resolution Protocol Spoofing 567
- DNS Poisoning, Spoofing, and Hijacking 568
- Hyperlink Spoofing 568

Summary 569

Exam Essentials 571

Written Lab 573

Review Questions 574

Chapter 13 Managing Identity and Authentication 579

Controlling Access to Assets 580
- Comparing Subjects and Objects 581
- The CIA Triad and Access Controls 581
- Types of Access Control 582

Comparing Identification and Authentication 584
- Registration and Proofing of Identity 585
- Authorization and Accountability 586
- Authentication Factors 587
- Passwords 588
- Smartcards and Tokens 592
- Biometrics 595
- Multifactor Authentication 599
- Device Authentication 600
- Service Authentication 601

Implementing Identity Management 602
- Single Sign-On 602
- Credential Management Systems 607
- Integrating Identity Services 608
- Managing Sessions 608
- AAA Protocols 609

Managing the Identity and Access Provisioning Lifecycle 611
Provisioning 611
Account Review 612
Account Revocation 613
Summary 614
Exam Essentials 615
Written Lab 617
Review Questions 618

Chapter 14 Controlling and Monitoring Access 623

Comparing Access Control Models 624
Comparing Permissions, Rights, and Privileges 624
Understanding Authorization Mechanisms 625
Defining Requirements with a Security Policy 626
Implementing Defense in Depth 627
Summarizing Access Control Models 628
Discretionary Access Controls 629
Nondiscretionary Access Controls 630
Understanding Access Control Attacks 635
Risk Elements 636
Identifying Assets 637
Identifying Threats 638
Identifying Vulnerabilities 640
Common Access Control Attacks 641
Summary of Protection Methods 652
Summary 653
Exam Essentials 654
Written Lab 656
Review Questions 657

Chapter 15 Security Assessment and Testing 661

Building a Security Assessment and Testing Program 662
Security Testing 662
Security Assessments 664
Security Audits 665
Performing Vulnerability Assessments 668
Describing Vulnerabilities 668
Vulnerability Scans 668
Penetration Testing 679
Testing Your Software 681
Code Review and Testing 682
Interface Testing 686
Misuse Case Testing 686

Test Coverage Analysis 686
Website Monitoring 687
Implementing Security Management Processes 688
Log Reviews 688
Account Management 689
Backup Verification 689
Key Performance and Risk Indicators 690
Summary 690
Exam Essentials 691
Written Lab 692
Review Questions 693

Chapter 16 Managing Security Operations 697

Applying Security Operations Concepts 698
Need-to-Know and Least Privilege 698
Separation of Duties and Responsibilities 700
Job Rotation 703
Mandatory Vacations 703
Privileged Account Management 704
Managing the Information Lifecycle 706
Service-Level Agreements 707
Addressing Personnel Safety and Security 708
Securely Provisioning Resources 710
Managing Hardware and Software Assets 710
Protecting Physical Assets 711
Managing Virtual Assets 712
Managing Cloud-Based Assets 713
Media Management 714
Managing Configuration 718
Baselining 718
Using Images for Baselining 718
Managing Change 719
Security Impact Analysis 721
Versioning 722
Configuration Documentation 723
Managing Patches and Reducing Vulnerabilities 723
Systems to Manage 723
Patch Management 724
Vulnerability Management 725
Common Vulnerabilities and Exposures 728
Summary 728
Exam Essentials 729
Written Lab 731
Review Questions 732

Chapter 17 Preventing and Responding to Incidents 737

Managing Incident Response 738
- Defining an Incident 738
- Incident Response Steps 739

Implementing Detective and Preventive Measures 745
- Basic Preventive Measures 745
- Understanding Attacks 746
- Intrusion Detection and Prevention Systems 756
- Specific Preventive Measures 763

Logging, Monitoring, and Auditing 773
- Logging and Monitoring 773
- Egress Monitoring 781
- Auditing to Assess Effectiveness 783
- Security Audits and Reviews 787
- Reporting Audit Results 788

Summary 790

Exam Essentials 792

Written Lab 795

Review Questions 796

Chapter 18 Disaster Recovery Planning 801

The Nature of Disaster 802
- Natural Disasters 803
- Man-Made Disasters 807

Understand System Resilience and Fault Tolerance 812
- Protecting Hard Drives 813
- Protecting Servers 814
- Protecting Power Sources 815
- Trusted Recovery 816
- Quality of Service 817

Recovery Strategy 818
- Business Unit and Functional Priorities 818
- Crisis Management 819
- Emergency Communications 820
- Workgroup Recovery 820
- Alternate Processing Sites 820
- Mutual Assistance Agreements 825
- Database Recovery 825

Recovery Plan Development 827
- Emergency Response 828
- Personnel and Communications 828
- Assessment 829
- Backups and Offsite Storage 829

Software Escrow Arrangements 833
External Communications 833
Utilities 834
Logistics and Supplies 834
Recovery vs. Restoration 834
Training, Awareness, and Documentation 835
Testing and Maintenance 836
Read-Through Test 836
Structured Walk-Through 837
Simulation Test 837
Parallel Test 837
Full-Interruption Test 837
Maintenance 837
Summary 838
Exam Essentials 838
Written Lab 839
Review Questions 840

Chapter 19 Investigations and Ethics 845

Investigations 846
Investigation Types 846
Evidence 849
Investigation Process 853
Major Categories of Computer Crime 857
Military and Intelligence Attacks 857
Business Attacks 858
Financial Attacks 859
Terrorist Attacks 859
Grudge Attacks 859
Thrill Attacks 861
Ethics 861
(ISC)^2 Code of Ethics 862
Ethics and the Internet 862
Summary 864
Exam Essentials 864
Written Lab 865
Review Questions 866

Chapter 20 Software Development Security 871

Introducing Systems Development Controls 872
Software Development 872
Systems Development Lifecycle 878
Lifecycle Models 881

Gantt Charts and PERT 887
Change and Configuration Management 888
The DevOps Approach 889
Application Programming Interfaces 890
Software Testing 891
Code Repositories 893
Service-Level Agreements 894
Software Acquisition 894
Establishing Databases and Data Warehousing 895
Database Management System Architecture 896
Database Transactions 899
Security for Multilevel Databases 901
Open Database Connectivity 903
NoSQL 904
Storing Data and Information 904
Types of Storage 905
Storage Threats 905
Understanding Knowledge-Based Systems 906
Expert Systems 907
Machine Learning 908
Neural Networks 908
Security Applications 909
Summary 909
Exam Essentials 909
Written Lab 910
Review Questions 911

Chapter 21 Malicious Code and Application Attacks 915

Malicious Code 916
Sources of Malicious Code 916
Viruses 917
Logic Bombs 923
Trojan Horses 924
Worms 925
Spyware and Adware 928
Zero-Day Attacks 928
Password Attacks 929
Password Guessing 929
Dictionary Attacks 930
Social Engineering 931
Countermeasures 932
Application Attacks 933
Buffer Overflows 933
Time of Check to Time of Use 934

Back Doors 934
Escalation of Privilege and Rootkits 935
Web Application Security 935
Cross-Site Scripting 935
Cross-Site Request Forgery 936
SQL Injection 937
Reconnaissance Attacks 940
IP Probes 940
Port Scans 940
Vulnerability Scans 941
Masquerading Attacks 941
IP Spoofing 942
Session Hijacking 942
Summary 942
Exam Essentials 943
Written Lab 944
Review Questions 945

Appendix A Answers to Review Questions 949

Chapter 1: Security Governance Through Principles and Policies 950
Chapter 2: Personnel Security and Risk Management Concepts 951
Chapter 3: Business Continuity Planning 952
Chapter 4: Laws, Regulations, and Compliance 954
Chapter 5: Protecting Security of Assets 956
Chapter 6: Cryptography and Symmetric Key Algorithms 958
Chapter 7: PKI and Cryptographic Applications 960
Chapter 8: Principles of Security Models, Design, and Capabilities 961
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures 963
Chapter 10: Physical Security Requirements 965
Chapter 11: Secure Network Architecture and Securing Network Components 966
Chapter 12: Secure Communications and Network Attacks 968
Chapter 13: Managing Identity and Authentication 969
Chapter 14: Controlling and Monitoring Access 971
Chapter 15: Security Assessment and Testing 973
Chapter 16: Managing Security Operations 975
Chapter 17: Preventing and Responding to Incidents 977
Chapter 18: Disaster Recovery Planning 980

Chapter 19: Investigations and Ethics 981
Chapter 20: Software Development Security 983
Chapter 21: Malicious Code and Application Attacks 984

Appendix B Answers to Written Labs 987

Chapter 1: Security Governance Through Principles and Policies 988
Chapter 2: Personnel Security and Risk Management Concepts 988
Chapter 3: Business Continuity Planning 989
Chapter 4: Laws, Regulations, and Compliance 990
Chapter 5: Protecting Security of Assets 991
Chapter 6: Cryptography and Symmetric Key Algorithms 991
Chapter 7: PKI and Cryptographic Applications 992
Chapter 8: Principles of Security Models, Design, and Capabilities 992
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures 993
Chapter 10: Physical Security Requirements 994
Chapter 11: Secure Network Architecture and Securing Network Components 994
Chapter 12: Secure Communications and Network Attacks 995
Chapter 13: Managing Identity and Authentication 996
Chapter 14: Controlling and Monitoring Access 996
Chapter 15: Security Assessment and Testing 997
Chapter 16: Managing Security Operations 997
Chapter 17: Preventing and Responding to Incidents 998
Chapter 18: Disaster Recovery Planning 999
Chapter 19: Investigations and Ethics 999
Chapter 20: Software Development Security 1000
Chapter 21: Malicious Code and Application Attacks 1000

Index 1001