## Contents

**Introduction**  

**Assessment Test**  

### Chapter 1  Information Security: The Systems Security Certified Practitioner Certification  

1. About the (ISC)² Organization  
2. (ISC)² History  
3. Organizational Structure and Programs  
4. Exams, Testing, and Certification  
5. Certification Qualification: The SSCP Common Body of Knowledge  
6. After Passing the Exam  
7. Certification Maintenance  
8. Types of IT Certifications?  
9. About the Systems Security Certified Practitioner Certification  
10. How Do I Use My SSCP Knowledge on the Job?  
11. The SSCP Exam  
12. Preparing for the Exam  
13. Booking the Exam  
14. Taking the Exam  
15. Summary  
16. Exam Essentials  

### Chapter 2  Security Basics: A Foundation  

17. The Development of Security Techniques  
18. Understanding Security Terms and Concepts  
19. The Problem (Opportunity) and the Solution  
20. Evolution of Items  
21. Security Foundation Concepts  
22. CIA Triad  
23. Primary Security Categories  
24. Access Control  
25. Nonrepudiation  
26. Risk  
27. Prudent Man, Due Diligence, and Due Care  
28. User Security Management  
29. Least Privilege  
30. AAA  
31. Mandatory Vacation
Separation of Duties 46
M of N Requirement 46
Two-Man Rule 47
Job Rotation 48
Geographic Access Control 48
Temporal Access Control, Time of Day Control 48
Privacy 49
Transparency 49
Implicit Deny 50
Personal Device (BYOD) 51
Privilege Management, Privilege Life Cycle 51
Participating in Security Awareness Education 52
Types of Security Awareness Education Programs 52
Working with Human Resources and Stakeholders 53
Senior Executives 53
Customers, Vendors, and Extranet Users Security Awareness Programs 54
Summary 54
Exam Essentials 55
Written Lab 56
Review Questions 57

Chapter 3 Domain 1: Access Controls 61
What Are Controls? 62
What Should Be Protected? 63
Why Control Access? 64
Types of Access Controls 67
Physical Access Controls 67
Logical Access Controls 68
Administrative Access Controls 69
Identification 70
Authentication 72
Factors of Authentication 74
Single-Factor Authentication 84
Multifactor Authentication 84
Token-Based Access Controls 85
System-Level Access Controls 86
Discretionary Access Control (DAC) 86
Nondiscretionary Access Control 87
Mandatory Access Control 87
Administering Mandatory Access Control 89
Trusted Systems 90
Mandatory Access Control Architecture Models 91
Risk Management Frameworks and Guidance for Managing Risks
  ISO/IEC 27005 191
  NIST Special Publication 800-37 Revision 1 192
  NIST Special Publication 800-39 194
Risk Analysis and Risk Assessment 194
  Risk Analysis 195
  Risk Assessments 199
Managing Risks 202
  Treatment Plan 202
  Risk Treatment 202
  Risk Treatment Schedule 203
  Risk Register 205
Risk Visibility and Reporting 207
  Enterprise Risk Management 207
  Continuous Monitoring 208
  Security Operations Center 209
  Threat Intelligence 210
Analyzing Monitoring Results 211
  Security Analytics, Metrics, and Trends 212
  Event Data Analysis 213
  Visualization 214
  Communicating Findings 215
Summary 216
Exam Essentials 217
Written Lab 218
Review Questions 219

Chapter 6 Domain 4: Incident Response and Recovery 223
Event and Incident Handling Policy 224
  Standards 225
  Procedures 225
  Guidelines 226
Creating and Maintaining an Incident Response Plan 226
  Law Enforcement and Media Communication 229
  Building in Incident Response Team 231
  Incident Response Records 232
  Security Event Information 233
  Incident Response Containment and Restoration 233
  Implementation of Countermeasures 235
Understanding and Supporting Forensic Investigations 235
  Incident Scene 236
  Volatility of Evidence 237
Contents

Chapter 7  Domain 5: Cryptography  261

---

Chapter 8  Domain 6: Networks and Communications  317
Contents

Media Access Models 335
Ports and Protocols 336
  Ports 336
  Common Protocols 338
Converged Network Communications 340
Network Monitoring and Control 341
  Continuous Monitoring 341
  Network Monitors 341
  Managing Network Logs 342
Access Control Protocols and Standards 343
  Remote Network Access Control 343
Remote User Authentication Services 346
  RADIUS 347
  TACACS/TACACS+/XTACACS 347
Local User Authentication Services 348
  LDAP 348
  Kerberos 348
  Single Sign-On 350
Network Segmentation 351
  Subnetting 352
  Virtual Local Area Networks 353
  Demilitarized Zones 353
  Network Address Translation 354
Securing Devices 355
  MAC Filtering and Limiting 356
  Disabling Unused Ports 356
Security Posture 356
Firewall and Proxy Implementation 357
  Firewalls 357
  Firewall Rules 359
Network Routers and Switches 361
  Routers 361
  Switches 363
Intrusion Detection and Prevention Devices 363
  Intrusion Detection Systems 364
  Intrusion Prevention Systems 364
  Wireless Intrusion Prevention Systems 365
  Comparing Intrusion Detection Systems and Intrusion Prevention Systems 366
  Spam Filter to Prevent Email Spam 368
Telecommunications Remote Access 368
  Network Access Control 368
Wireless & Cellular Technologies 369
  IEEE 802.11x Wireless Protocols 370
Chapter 9  Domain 7: Systems and Application Security 389

Understand Malicious Code and Apply Countermeasures 390
  Malicious Code Terms and Concepts 393
  Managing Spam to Avoid Malware 401
  Cookies and Attachments 402
  Malicious Code Countermeasures 405
Malicious Add-Ons 409
  Java Applets 409
  ActiveX 410
User Threats and Endpoint Device Security 410
  General Workstation Security 411
  Physical Security 416
  Securing Mobile Devices and Mobile Device Management 426
Understand and Apply Cloud Security 428
  Cloud Concepts and Cloud Security 429
  Cloud Deployment Model Security 434
  Cloud Service Model Security 436
  Cloud Management Security 438
  Cloud Legal and Privacy Concepts 442
  Cloud Virtualization Security 449
Secure Data Warehouse and Big Data Environments 449
  Data Warehouse and Big Data Deployment and Operations 450
  Securing the Data Warehouse and Data Environment 451
Secure Software-Defined Networks and Virtual Environments 451
Software-Defined Networks 452
Security Benefits and Challenges of Virtualization 455
Summary 457
Exam Essentials 458
Written Lab 459
Review Questions 460

Appendix A  Answers to Written Labs 465
Chapter 2 466
Chapter 3 466
Chapter 4 467
Chapter 5 468
Chapter 6 468
Chapter 7 469
Chapter 8 470
Chapter 9 471

Appendix B  Answers to Review Questions 473
Chapter 2 474
Chapter 3 475
Chapter 4 476
Chapter 5 478
Chapter 6 479
Chapter 7 481
Chapter 8 483
Chapter 9 484

Appendix C  Diagnostic Tools 487
Microsoft Baseline Security Analyzer 488
Using the Tool 488
Microsoft Password Checker 491
Using the Tool 491
Internet Explorer Phishing and Malicious Software Filter 492
Using the Tool 493
Manage Internet Cookies 494
Using the Tool 494
Observing Logs with Event Viewer 495
Using the Tool 495
Viewing a Digital Certificate 497
Using the Tool 497
Monitoring PC Activities with Windows Performance Monitor 500
Using the Tool 500