# Contents

*Introduction*  
*Assessment Test*

## Chapter 1  Managing Risk

- Risk Terminology 1  
- Threat Assessment 3  
- Risk Assessment 6  
  - Computing Risk Assessment 7  
  - Assessing Privacy 12  
  - Acting on Your Risk Assessment 12  
  - Risks Associated with Cloud Computing 15  
  - Risks Associated with Virtualization 16  
- Developing Policies, Standards, and Guidelines 17  
  - Implementing Policies 17  
  - Understanding Control Types and False Positives/Negatives 26  
- Risk Management Best Practices 28  
  - Change Management 38  
- Summary 38  
- Exam Essentials 38  
- Review Questions 40

## Chapter 2  Monitoring and Diagnosing Networks

- Monitoring and Diagnosing Networks Terminology 47  
- Frameworks, Best Practices, and Configuration Guides 48  
  - Industry-Standard Frameworks and Reference Architectures 48  
  - National Institute of Standards and Technology (NIST) 51  
  - Benchmarks/Secure Configuration Guides 54  
- Secure Network Architecture Concepts 57  
  - Zones 57  
  - Tunneling/VPN 63  
  - Placing Security Devices 64  
  - SDN 67  
  - IDS vs. IPS 67  
- Secure Systems Design 68  
  - Hardware and Firmware Security 68  
  - Operating Systems 69  
  - Peripherals 73  
- Secure Staging Deployment Concepts 73
Summary 74
Exam Essentials 74
Review Questions 76

Chapter 3  Understanding Devices and Infrastructure 79

Infrastructure Terminology 81
Designing with Security in Mind 84
   Firewalls 84
   VPNs and VPN Concentrators 89
   Intrusion Detection Systems 91
Router 104
Switch 106
Proxy 107
Load Balancer 108
Access Point 108
SIEM 111
DLP 111
Network Access Control (NAC) 112
Mail Gateway 112
Bridge 113
SSL/TLS Accelerators 113
SSL Decryptors 113
Media Gateway 114
Hardware Security Module 114
Summary 115
Exam Essentials 115
Review Questions 116

Chapter 4  Identity and Access Management 121

Using Tools to Assess Your Network 125
   Protocol Analyzer 125
   Network Scanners 127
   Password Cracker 130
   Vulnerability Scanners 131
   Command-Line Tools 135
   Additional Tools 142
Troubleshooting Common Security Issues 143
   Access Issues 144
   Configuration Issues 145
Security Technologies 147
   Intrusion Detection Systems 147
   Antimalware 148
   Firewalls and Related Devices 149
   Other Systems 150
Identity and Access Management Concepts
  Identification vs. Authentication 151
  Authentication (Single Factor) and Authorization 152
  Multifactor Authentication 153
  Biometrics 153
  Federations 154
  Potential Authentication and Access Problems 154
  LDAP 155
  PAP, SPAP, and CHAP 155
  Kerberos 156
  Working with RADIUS 157
  TACACS, TACACS+, XTACACS 158
  OATH 158
  One-Time Passwords 158
  SAML 159
Install and Configure Identity and Access Services
  Mandatory Access Control 159
  Discretionary Access Control 160
  Role-Based Access Control 160
  Rule-Based Access Control 160
  ABAC 161
  Smartcards 161
  Tokens 162
File and Database Security
  Summary 163
Exam Essentials 164
Review Questions 165

Chapter  5  Wireless Network Threats 169
Wireless Threat Terminology 170
Wireless Vulnerabilities to Know 171
  Replay 172
  Rogue APs and Evil Twins 174
  Jamming 174
  WPS 175
  Bluejacking 175
  Bluesnarfing 175
  NFC and RFID 176
  Disassociation 176
Wireless Commonsense 176
Wireless Attack Analogy 176
Summary 177
Exam Essentials 178
Review Questions 179
**Chapter 6**

**Securing the Cloud**

- Cloud-Related Terminology
- Working with Cloud Computing
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud
- Working with Virtualization
  - Understanding Hypervisors
  - Understanding Containers and Application Cells
  - VDI/VDE
  - On-Premise vs. Hosted vs. Cloud
  - VM Escape Protection
  - VM Sprawl Avoidance
- Security and the Cloud
  - Cloud Access Security Brokers
  - Cloud Storage
  - Security as a Service
- Summary
- Exam Essentials
- Review Questions

**Chapter 7**

**Host, Data, and Application Security**

- Threat Actors and Attributes
  - Script Kiddies
  - Hacktivist
  - Organized Crime
  - Nation-States/APT
  - Insiders
  - Competitors
- Use of Open Source Intelligence
- Types of Vulnerabilities
  - Configuration Issues
  - User Issues
  - Zero-Day Exploits
  - Other Issues
- Embedded Systems Security
- Application Vulnerabilities
  - Input Vulnerabilities
  - Memory Vulnerabilities
- Secure Programming
  - Programming Models
  - Software Testing
Chapter 8  Cryptography  231

An Overview of Cryptography  234
  Historical Cryptography  234
Modern Cryptography  238
  Working with Symmetric Algorithms  239
  Working with Asymmetric Algorithms  243
  Cryptography Concepts  246
  Hashing Algorithms  247
  Rainbow Tables and Salt  249
  Key Stretching  249
  Cryptanalysis Methods  250
  Wi-Fi Encryption  252
Using Cryptographic Systems  254
  Confidentiality and Strength  254
  Integrity  254
  When to Encrypt  255
  Digital Signatures  256
  Authentication  257
  Nonrepudiation  257
  Key Features  258
Understanding Cryptography Standards and Protocols  258
  The Origins of Encryption Standards  259
  Public Key Infrastructure X.509/Public Key
    Cryptography Standards  261
    X.509  262
  Public Key Infrastructure  264
    Pretty Good Privacy  264
    SSL and TLS  266
Using Public Key Infrastructure  269
  Hardware-Based Encryption Devices  269
  Data Encryption  269
Authentication 270
Summary 271
Exam Essentials 271
Review Questions 273

Chapter 9  Threats, Attacks, and Vulnerabilities 277
Threat and Attack Terminology 278
Living in a World of Viruses 282
Symptoms of a Virus Infection 282
How Viruses Work 283
Types of Viruses 284
Managing Spam to Avoid Viruses 286
Antivirus Software 287
Malware and Crypto-Malware 288
Understanding Various Types of Application/Service Attacks 296
Identifying Denial-of-Service and Distributed
Denial-of-Service Attacks 296
Man-in-the-Middle Attacks 298
Buffer Overflow 299
Injection 299
Cross-Site Scripting and Request Forgery 302
Privilege Escalation 303
ARP Poisoning 304
Amplification 304
DNS Poisoning 304
Domain Hijacking 304
Man-in-the-Browser 305
Zero-Day Exploits 305
Replay Attacks 305
Pass the Hash 306
Hijacking and Related Attacks 306
Driver Manipulation 307
MAC and IP Spoofing Attacks 308
Summary 309
Exam Essentials 309
Review Questions 311

Chapter 10  Social Engineering and Other Foes 315
Social Engineering and Physical Security Terminology 316
Understanding Social Engineering 318
Types of Social Engineering Attacks 319
What Motivates an Attack? 325
The Principles Behind Social Engineering 326
Social Engineering Attack Examples 327
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Physical Security</td>
<td>330</td>
</tr>
<tr>
<td>Lighting</td>
<td>331</td>
</tr>
<tr>
<td>Signs</td>
<td>331</td>
</tr>
<tr>
<td>Fencing, Gates, and Cages</td>
<td>332</td>
</tr>
<tr>
<td>Security Guards</td>
<td>333</td>
</tr>
<tr>
<td>Alarms</td>
<td>333</td>
</tr>
<tr>
<td>Safe</td>
<td>334</td>
</tr>
<tr>
<td>Secure Cabinets and Enclosures</td>
<td>334</td>
</tr>
<tr>
<td>Protected Distribution</td>
<td>335</td>
</tr>
<tr>
<td>Protected Cabling</td>
<td>336</td>
</tr>
<tr>
<td>Airgap</td>
<td>336</td>
</tr>
<tr>
<td>Mantrap</td>
<td>336</td>
</tr>
<tr>
<td>Faraday Cage</td>
<td>337</td>
</tr>
<tr>
<td>Lock Types</td>
<td>337</td>
</tr>
<tr>
<td>Biometrics</td>
<td>338</td>
</tr>
<tr>
<td>Barricades/Bollards</td>
<td>339</td>
</tr>
<tr>
<td>Tokens/Cards</td>
<td>339</td>
</tr>
<tr>
<td>Environmental Controls</td>
<td>339</td>
</tr>
<tr>
<td>Cable Locks</td>
<td>345</td>
</tr>
<tr>
<td>Screen Filters</td>
<td>346</td>
</tr>
<tr>
<td>Cameras</td>
<td>346</td>
</tr>
<tr>
<td>Motion Detection</td>
<td>347</td>
</tr>
<tr>
<td>Logs</td>
<td>347</td>
</tr>
<tr>
<td>Infrared Detection</td>
<td>348</td>
</tr>
<tr>
<td>Key Management</td>
<td>348</td>
</tr>
<tr>
<td>Various Control Types</td>
<td>348</td>
</tr>
<tr>
<td>An Analogy of Control Types</td>
<td>349</td>
</tr>
<tr>
<td>Data Security and Privacy Practices</td>
<td>350</td>
</tr>
<tr>
<td>Data Destruction and Media Sanitation</td>
<td>350</td>
</tr>
<tr>
<td>Data Sensitivity Labeling and Handling</td>
<td>352</td>
</tr>
<tr>
<td>Data Roles</td>
<td>355</td>
</tr>
<tr>
<td>Data Retention</td>
<td>355</td>
</tr>
<tr>
<td>Legal and Compliance</td>
<td>356</td>
</tr>
<tr>
<td>Summary</td>
<td>356</td>
</tr>
<tr>
<td>Exam Essentials</td>
<td>356</td>
</tr>
<tr>
<td>Review Questions</td>
<td>358</td>
</tr>
</tbody>
</table>

### Chapter 11 Security Administration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Types</td>
<td>363</td>
</tr>
<tr>
<td>Cellular</td>
<td>365</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>365</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>366</td>
</tr>
<tr>
<td>Infrared</td>
<td>368</td>
</tr>
<tr>
<td>SATCOM</td>
<td>369</td>
</tr>
<tr>
<td>Chapter</td>
<td>Disaster Recovery and Incident Response</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Disaster and Incident Related Terminology</td>
</tr>
<tr>
<td></td>
<td>Penetration Testing</td>
</tr>
<tr>
<td></td>
<td>What Should You Test?</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Scanning</td>
</tr>
<tr>
<td></td>
<td>Issues Associated with Business Continuity</td>
</tr>
<tr>
<td></td>
<td>Types of Storage Mechanisms</td>
</tr>
<tr>
<td></td>
<td>Crafting a Disaster-Recovery Plan</td>
</tr>
<tr>
<td></td>
<td>Incident Response Procedures</td>
</tr>
<tr>
<td></td>
<td>Understanding Incident Response</td>
</tr>
<tr>
<td></td>
<td>Tabletop Exercises</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
</tr>
<tr>
<td></td>
<td>Exam Essentials</td>
</tr>
<tr>
<td></td>
<td>Review Questions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Answers to Review Questions</th>
<th>419</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chapter 1: Managing Risk</td>
<td>420</td>
</tr>
<tr>
<td></td>
<td>Chapter 2: Monitoring and Diagnosing Networks</td>
<td>421</td>
</tr>
<tr>
<td></td>
<td>Chapter 3: Understanding Devices and Infrastructure</td>
<td>422</td>
</tr>
<tr>
<td></td>
<td>Chapter 4: Identity and Access Management</td>
<td>423</td>
</tr>
<tr>
<td></td>
<td>Chapter 5: Wireless Network Threats</td>
<td>425</td>
</tr>
<tr>
<td></td>
<td>Chapter 6: Securing the Cloud</td>
<td>426</td>
</tr>
<tr>
<td></td>
<td>Chapter 7: Host, Data, and Application Security</td>
<td>427</td>
</tr>
<tr>
<td></td>
<td>Chapter 8: Cryptography</td>
<td>428</td>
</tr>
<tr>
<td></td>
<td>Chapter 9: Threats, Attacks, and Vulnerabilities</td>
<td>429</td>
</tr>
<tr>
<td></td>
<td>Chapter 10: Social Engineering and Other Foes</td>
<td>430</td>
</tr>
<tr>
<td></td>
<td>Chapter 11: Security Administration</td>
<td>431</td>
</tr>
<tr>
<td></td>
<td>Chapter 12: Disaster Recovery and Incident Response</td>
<td>432</td>
</tr>
</tbody>
</table>

| Index    |                                  | 435 |
Table of Exercises

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Risk Assessment Computations</td>
<td>8</td>
</tr>
<tr>
<td>3.1</td>
<td>Verifying the Presence of a TPM Chip in Windows</td>
<td>114</td>
</tr>
<tr>
<td>5.1</td>
<td>Configuring a Wireless Connection Not Broadcasting an SSID</td>
<td>172</td>
</tr>
<tr>
<td>8.1</td>
<td>Encrypting a Filesystem in Linux</td>
<td>238</td>
</tr>
<tr>
<td>8.2</td>
<td>TLS Settings in Windows Server 2016</td>
<td>268</td>
</tr>
<tr>
<td>9.1</td>
<td>Viewing Running Processes on a Windows-Based Machine</td>
<td>290</td>
</tr>
<tr>
<td>9.2</td>
<td>Viewing Running Processes on a Linux-Based Machine</td>
<td>291</td>
</tr>
<tr>
<td>10.1</td>
<td>Test Social Engineering</td>
<td>328</td>
</tr>
<tr>
<td>10.2</td>
<td>Security Zones in the Physical Environment</td>
<td>347</td>
</tr>
<tr>
<td>12.1</td>
<td>Creating a Backup in SUSE Linux</td>
<td>396</td>
</tr>
</tbody>
</table>