## Contents

*Introduction* .............................. xxiv  

*Assessment Test* ......................... xli  

### Chapter 1  Managing Risk  1

- Risk Terminology ...................... 3  
- Threat Assessment ..................... 6  
- 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  45

- 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
## Contents

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 151
   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 159
   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 163
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  183
Cloud-Related Terminology  184
Working with Cloud Computing  186
  Software as a Service (SaaS)  186
  Platform as a Service (PaaS)  186
  Infrastructure as a Service (IaaS)  188
Private Cloud  189
Public Cloud  189
Community Cloud  189
Hybrid Cloud  190
Working with Virtualization  190
  Understanding Hypervisors  190
  Understanding Containers and Application Cells  192
VDI/VDE  192
On-Premise vs. Hosted vs. Cloud  192
VM Escape Protection  193
VM Sprawl Avoidance  193
Security and the Cloud  194
  Cloud Access Security Brokers  195
  Cloud Storage  195
  Security as a Service  195
Summary  196
Exam Essentials  196
Review Questions  197

Chapter 7  Host, Data, and Application Security  201
Threat Actors and Attributes  204
  Script Kiddies  205
  Hacktivist  206
  Organized Crime  207
  Nation-States/APT  207
  Insiders  207
  Competitors  207
Use of Open Source Intelligence  208
Types of Vulnerabilities  211
  Configuration Issues  211
  User Issues  212
  Zero-Day Exploits  212
  Other Issues  214
Embedded Systems Security  214
Application Vulnerabilities  216
  Input Vulnerabilities  216
  Memory Vulnerabilities  217
Secure Programming  217
  Programming Models  218
  Software Testing  218
Specific Types of Testing 219
Secure Coding Standards 220
Application Configuration Baselining 221
Operating System Patch Management 221
Application Patch Management 222
Other Application Security Issues 222
Databases and Technologies 222
Database Security 225
Secure Configurations 225
Code Issues 225
Summary 226
Exam Essentials 226
Review Questions 227

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
Chapter 9  
Threats, Attacks, and Vulnerabilities  
277

Chapter 10  
Social Engineering and Other Foes  
315
Understanding Physical Security 330
  Lighting 331
  Signs 331
  Fencing, Gates, and Cages 332
  Security Guards 333
  Alarms 333
  Safe 334
  Secure Cabinets and Enclosures 334
  Protected Distribution 335
  Protected Cabling 336
  Airgap 336
  Mantrap 336
  Faraday Cage 337
  Lock Types 337
  Biometrics 338
  Barricades/Bollards 339
  Tokens/Cards 339
  Environmental Controls 339
  Cable Locks 345
  Screen Filters 346
  Cameras 346
  Motion Detection 347
  Logs 347
  Infrared Detection 348
  Key Management 348
Various Control Types 348
  An Analogy of Control Types 349
Data Security and Privacy Practices 350
  Data Destruction and Media Sanitation 350
  Data Sensitivity Labeling and Handling 352
  Data Roles 355
  Data Retention 355
  Legal and Compliance 356
Summary 356
Exam Essentials 356
Review Questions 358

Chapter 11 Security Administration 363
Connection Types 365
  Cellular 365
  Bluetooth 365
  Wi-Fi 366
  Infrared 368
  SATCOM 369
Mobile Devices
BYOD Issues
Enforcement
Account Management Concepts
Account Types
General Concepts
Summary
Exam Essentials
Review Questions

Chapter 12 Disaster Recovery and Incident Response 383
Disaster and Incident Related Terminology 385
Penetration Testing 387
What Should You Test? 387
Vulnerability Scanning 388
Issues Associated with Business Continuity 389
Types of Storage Mechanisms 390
Crafting a Disaster-Recovery Plan 392
Incident Response Procedures 403
Understanding Incident Response 404
Tabletop Exercises 412
Summary 412
Exam Essentials 413
Review Questions 414

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

Index 435
## Table of Exercises

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