COMPTIA SECURITY+ SY0-601

CORRELATION OF STANDARDS WITH

GOODHEART-WILLCOX

SECURITY ESSENTIALS © 2022

BY ***LINDA K. LAVENDER***

Standard	Corresponding Page(s)
1.0: Threats, Attacks, and Vulnerabilities	
1.1: Compare and contrast different types of social engineering techniques.	
Phishing	Pgs. 47-48 Phishing
Smishing	Pg. 49 Smishing
Vishing	Pg. 49 Vishing
Spam	Pg. 50 Spam
Spam over Internet Messaging (SPIM)	Pg. 50 Spam over Internet Messaging (SPIM)
Spear phishing	Pg. 48 Spear Phishing
Dumpster diving	Pgs. 46-47 Dumpster Diving
Shoulder surfing	Pg. 47 Shoulder Surfing
Pharming	Pgs. 49-50 Pharming
Tailgating	Pgs. 160-161 Mantraps
Eliciting information	Pg. 43 Eliciting Information
Whaling	Pg. 48 Whale Phishing
Prepending	Pg. 49 Prepending
Identity fraud	Pg. 50 Identity Fraud
Invoice scams	Pg. 50 Invoice Scams
Credential harvesting	Pg. 49 Credential Harvesting
Reconnaissance	Pg. 47 Shoulder Surfing Pgs. 78-79 Reconnaissance
Hoax	Pg. 50 Hoax
Impersonation	Pg.50 Impersonation
Watering hole attack	Pg. 49 Watering Hole
Typo squatting	Pg. 228 Typo Squatting
Influence campaigns	Pgs. 50-51 Influence Campaigns
Hybrid warfare	Pg. 51 Hybrid Warfare
Social media	Pg. 51 Social Media
Principles (reasons for effectiveness)	Pgs. 42-43 Social Engineering
Authority	
Intimidation	
Consensus	
Scarcity	
Familiarity	
Trust	
Urgency	
1.2: Given a scenario, analyze potential indicators to determine the type of attack	
Malware	Pg. 35 Malware Attacks
Ransomware	Pgs. 39-40 Ransomware

Standard	Corresponding Page(s)
Trojans	Pg. 38 Trojan
Worms	Pg. 39 Worm
Potentially unwanted programs (PUPs)	Pg. 38 Potentially Unwanted Program (PUP)
Fileless virus	Pg. 41 Fileless Virus
Command and control	Pg. 35 Malware Attacks
Bots	Pg. 35 Malware Attacks
Crypto malware	Pg. 40 Ransomware
Logic bombs	Pg. 39 Logic Bomb
Spyware	Pg. 36 Keylogger
Keyloggers	Pg. 36 Keylogger
Remote access Trojan (RAT)	Pg. 38 Trojan
Rootkit	Pg. 40 Rootkit
Backdoor	Pg. 40 Backdoor
Password attacks	
Spraying	Pg. 285 Password Spraying
Dictionary	Pg. 283 Dictionary Attack
Brute Force	Pg. 284 Brute Force
Offline	Pg. 283 Password Attacks
Online	Pg. 283 Password Attacks
Rainbow tables	Pg. 284 Rainbow Table
Plaintext/unencrypted	Pg. 284 Plaintext/Unencrypted
Physical attacks	Pg. 57 Physical Attacks
Malicious universal serial bus (USB) cable	Pg. 58 Malicious USB Cables
Malicious flash drive	Pg. 58 Malicious Flash Drives
Card cloning	Pg. 58 Card Cloning and Skimming
Skimming	PG. 58 Card Cloning and Skimming
Adversarial artificial intelligence (AI)	Pgs. 41-42 Adversarial Artificial Intelligence (AI) Attack
Tainted training data for machine learning (ML)	
Security or machine learning algorithms	
Supply-chain attacks	Pgs. 510-511 Threat Assessment
Cloud-based vs. on-premises attacks	Pgs. 447-478 Cloud Vulnerabilities
Cryptographic attacks	
Birthday	Pg. 286 Birthday Attack
Collision	Pg. 286 Collision Attack
Downgrade	Pgs. 286-287 Downgrade Attack
1.3: Given a scenario, analyze potential indicators associated with application attacks.	
Privilege escalation	Pg. 227 Privilege Escalation
Cross-site scripting	Pgs. 225-226 Cross-Site Scripting
Injections	
Structured query language (SQL)	Pg. 225 SQL Injection
Dynamic link library (DLL)	Pg. 224 DLL Injection
Lightweight directory access protocol (LDAP)	Pg. 225 LDAP Injections
Extensible markup language (XML)	Pg. 225 XML Injections
Pointer/object dereference	Pg. 222 Pointer Dereference
Directory traversal	Pg. 228 Traversal

Standard	Corresponding Page(s)
Buffer overflow	Pg. 222 Buffer Overflow
Race conditions	Pg. 223 Conditions
Time of check/time of use	
Error handling	Pg. 218 Error Handling
Improper input handling	Pg. 218 Error Handling
Replay attack	Pg. 462 Replay Attacks
Session replays	Pg. 462 Replay Attacks
Integer overflow	Pg. 222 Integer Overflow
Request forgeries	Pg. 226 Request Forgeries
Server-side	
Client-side	
Cross-site	
Application programming interface (API) attacks	Pg. 224 Application Programming Interface (API) Attacks
Resource exhaustion	Pg. 221 Application Vulnerabilities
Memory leak	Pg. 223 Memory Leak
Secure sockets layer (SSL) stripping	Pg. 229 SSL Stripping
Driver manipulation	Pg. 229 Driver Manipulation
Shimming	
Refactoring	
Pass the hash	Pgs. 284-285 Pass the Hash
1.4: Given a scenario, analyze potential indicators associated with network attacks.	
Wireless	
Evil twin	Pgs. 462-463 Evil Twin
Rogue access point	Pgs. 462-463 Evil Twin
Bluesnarfing	Pg. 463 Bluejacking and Bluesnarfing
Bluejacking	Pg. 463 Bluejacking and Bluesnarfing
Disassociation	Pg. 463 Disassociation
Jamming	Pg. 464 Jamming
Radio frequency identifier (RFID)	Pg. 464 RFID Attacks
Near field communication (NFC)	Pg. 464 NFC Attacks
Initialization vector (IV)	Pgs. 464-465 Initialization Vectors (IVs)
Man in the middle	Pgs. 286-287 Downgrade Attack
Man in the browser	Pg. 229 SSL Stripping
Layer 2 attacks	
Address resolution protocol (ARP) poisoning	Pgs. 13-14 LAN Pgs. 426-427 ARP Poisoning
Media access control (MAC) flooding	pgs. 371-372 Flood Guards
MAC cloning	Pg. 427 MAC Cloning
Domain name system (DNS)	
Domain hijacking	Pg. 413 Domain Hijacking Attack
DNS poisoning	Pgs. 413-414 DNS Poisoning Attack
Universal resource locator (URL) redirection	Pg. 414 URL Redirection Attack
Domain reputation	Pg. 412 Domain Reputation
Distributed denial of service (DDoS)	Pgs. 412-413 DNS Attacks

Standard	Corresponding Page(s)
Network application	
Operational technology (OT)	
Malicious code or script execution	Pg. 430 Malicious Code and Script Execution
PowerShell	
Python	
Bash	
Macros	
Visual Basic for Application (VBA)	
1.5: Explain different threat actors, vectors, and intelligence sources	
Actors and threats	Pg. 28 Threat Actors
Advanced persistent threat (APT)	Pg. 29 State Actor
Insider threats	Pg. 29 Insiders
State actors	Pg. 29 State Actor
Hacktivists	Pgs. 28-29 Hacktivist
Script kiddies	Pg. 29 Script Kiddie
Criminal syndicates	Pg. 29 Criminal Syndicate
Hackers	Pg. 30 Hackers
White hat	
Black hat	
Gray hat	
Shadow IT	Pg. 29 Insiders
Competitors	Pg. 30 Competitors
Attributes of actors	Pg. 30 Attributes of Threat Actors
Internal/external	
Level of sophistication/capability	
Resources/funding	
Intent/motivation	
Vectors	Pg. 30 Vectors
Direct access	
Wireless	
Email	
Supply chain	
Social media	
Removable media	
Cloud	
Threat intelligence sources	Pgs. 31-32 Threat Intelligence Sources
Open source intelligence (OSINT)	Pgs. 32-33 Open-Source Intelligence (OSINT)
Closed/proprietary	Pgs. 33 Closed/Proprietary Sources
Vulnerability databases	Pg. 32 Open-Source Intelligence (OSINT)
Public/private information sharing centers	Pg. 33 Information Sharing Centers
Dark web	Pg. 34 Dark Web
Indicators of compromise	Pg. 32 Threat Intelligence Sources
Automated indicator sharing (AIS)	Pgs. 33-34 Automated Indicator Sharing
Structured threat information exchange (STIX)/Trusted automated exchange of indicator	Pg. 34 Structured Threat Information eXpression (STIX)

Standard	Corresponding Page(s)
information (TAXII)	Pg. 34 Trusted Automated Exchange of Indicator Information (TAXII)
Predictive analysis	Pgs. 215-216 Software Diversity
Threat maps	Pg. 33 Closed/Proprietary Sources
File/code repositories	Pg. 213 DevOps
Research sources	
Vendor websites	Pgs. 32-33 Open-Source Intelligence (OSINT)
Vulnerability feeds	
Conferences	
Academic journals	
Request for comments (RFC)	
Local industry groups	
Social media	Pgs. 43-44 Social Media
Threat feeds	Pgs. 32-33 Open-Source Intelligence (OSINT)
Adversary tactics, techniques. and procedures (TTP)	
1.6: Explain the security concerns associated with various types of vulnerabilities	
Cloud-based vs. on-premises	Pgs. 477-478 Cloud Vulnerabilities
Zero-day	Pg. 52 Zero-Day Vulnerability
Weak configurations	Pgs. 52-53 Weak Configurations
Open permissions	Pg. 53 Open Permissions
Unsecured root accounts	Pg. 53 Unsecured Root Accounts
Errors	Pg. 53 Errors
Weak encryption	Pgs. 53-54 Weak Encryption
Unsecure protocols	Pg. 54 Unsecure Protocols
Default settings	Pg. 54 Default Settings
Open ports and services	Pg. 54 Open Ports and Services
Third-party risks	Pg. 55 Third-Party Risks
Vendor management	Pg. 55 Vendor Management
System integration	
Lack of vendor support	Pgs. 55-56 Lack of Vendor Support
Supply chain	Pg. 56 Supply Chain
Outsourced code development	Pg. 56 Outsourced Code Development
Data storage	Pg. 56 Data Storage
Improper or weak patch management	Pg. 188-189 Patch Management
Firmware	
Operating system (OS)	
Applications	
Legacy platforms	Pgs. 54-55 Legacy Platforms
Impacts	Pgs. 51-52 Vulnerabilities
Data loss	
Data breaches	
Data exfiltration	
Identity theft	
Financial	

Standard	Corresponding Page(s)
Reputation	
Availability loss	
1.7: Summarize the techniques used in security assessment	
Threat hunting	Pg. 72 Threat Hunting
Intelligence fusion	Pg. 72 Threat Hunting
Threat feeds	Pgs. 72-73 Threat Intelligence Feeds
Advisories and bulletins	Pg. 73 Advisories and Bulletins
Maneuver	Pg. 73 Maneuvers
Vulnerability scans	Pg. 73 Vulnerability Scan
False positives	Pgs. 74-75 Scanner Output
False negatives	
Log reviews	
Credentialed vs. non-credentialed	Pg. 73 Vulnerability Scan
Intrusive vs. non-intrusive	Pg. 73 Vulnerability Scanners
Application	Pg. 74 Vulnerability Scanning Techniques
Web application	
Network	
Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)	Pg. 75 Common Vulnerabilities and Exposure Resource
Configuration review	Pg. 75 Scanner Output
Syslog/Security information and event management (SIEM)	Pg. 84 Syslog Pgs. 85-87 Security Information and Event Management (SIEM)
Review reports	Pg. 84 Syslog
Packet capture	Pgs. 85-87 Security Information and Event Management (SIEM)
Data inputs	
User behavior analysis	
Sentiment analysis	
Security monitoring	
Log aggregation	
Log collectors	
Security orchestration, automation, response (SORAR)	Pg. 87 SOAR
1.8: Explain the techniques used in penetration testing	
Penetration testing	Pgs. 75-76 Penetration Testing
White box	Pg. 76 Types of Pen Tests
Black box	
Gray box	
Rules of engagement	Pg. 76 Rules of Engagement
Lateral movement	Pg. 79 Lateral Movement
Privilege escalation	Pg. 79 Escalation of Privilege
Persistence	Pg. 79 Persistence
Cleanup	Pg. 80 Penetration Testing Cleanup
Bug bounty	Pg. 76 Penetration Testing

Standard	Corresponding Page(s)
Pivoting	Pg. 79 Pivot
Passive and active reconnaissance	Pgs. 78-79 Reconnaissance
Drones/unmanned aerial vehicle (UAV)	Pg. 78 Passive Reconnaissance
Way flying	Pg. 78 Passive Reconnaissance
War driving	Pg. 78 Passive Reconnaissance
Footprinting	Pg. 78 Passive Reconnaissance
OSINT	Pg. 78 Passive Reconnaissance
Exercise types	Pg. 76-77 Exercise Types
Red team	
Blue team	
White team	
Purple team	
2.0: Architecture and Design	
2.1: Explain the importance of security concepts in an enterprise environment	
Configuration management	
Diagrams	pg. 385 Diagrams
Baseline configuration	Pg. 80 Establishing Baselines Pg. 395 Baseline Configuration
Standard naming conventions	Pg. 132 Standard Naming Convention Pg. 385 Standard Naming Conventions
Internet protocol (IP) schema	Pg. 385 Internet Protocol (IP) Schema
Data sovereignty	Pgs. 478-479 Storage Pgs. 515-516 Data Life Cycle
Data protection	
Data loss prevention (DLP)	Pgs. 183-184 Data Loss Prevention (DLP)
Masking	Pg. 272 Obfuscation
Encryption	Pgs. 273-274 Encryption
At rest	Pgs. 271-272 Cryptography
In transit/motion	Pgs. 271-272 Cryptography
In processing	Pgs. 271-272 Cryptography
Tokenization	Pg. 195 Database Hardening Pg. 518 Tokenization
Rights management	Pg. 514 Data Governance
Hardware security module (HSM)	Pg. 246 MicroSD Hardware Security Module
Geographical considerations	Pg. 384 Geographical Considerations
Cloud access security broker (CASB)	Pg. 485 Cloud Access Security Broker (CASB)
Response and recovery controls	Pg. 538 Incident Response (IR)
Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Inspection	Pg. 381 Figure 12-9
Hashing	Pg. 281 Hashing
API considerations	Pgs. 479-480 Applications Pg. 487 Cloud Native Controls vs. Third-Party Solutions
Site resiliency	Pg. 572 Recovery Sites
Hot site	

Standard	Corresponding Page(s)
Cold site	
Warm site	
Deception and disruption	
Honeypots	Pg. 389 Honeypot
Honeyfiles	Pg. 389 Honeyfile
Honeynets	Pg. 389 Honeypot
Fake telemetry	Pg. 389 Fake Telemetry
DNS sinkhole	Pg. 389 DNS Sinkhole
2.2: Summarize virtualization and cloud computing concepts	
Cloud models	
Infrastructure as a service (IaaS)	Pg. 482 Infrastructure as a Service (IaaS)
Platform as a service (PaaS)	Pg. 483 Platform as a Service (PaaS)
Software as a service (SaaS)	Pg. 483 Software as a Service (SaaS)
Anything as a service (XaaS)	Pg. 483 Anything as a Service (XaaS)
Public	Pg. 481 Public Cloud
Community	Pg. 481 Community Cloud
Private	Pg. 481 Personal Cloud
Hybrid	Pg. 481 Hybrid Cloud
Cloud service providers	Pgs. 481-482 Cloud Service Providers (CSPs)
Managed service provider (MSP)/Managed security service provider (MSSP)	Pgs. 481-482 Cloud Service Providers (CSPs)
On-premises vs. off-premises	Pgs. 475-476 Cloud Computing
Fog computing	Pg. 484 Non-Cloud Services
Edge computing	Pg. 484 Non-Cloud Services
Thin client	Pg. 484 Non-Cloud Services
Containers	Pg. 490 Containers
Micro-services/API	Pgs. 479-480 Applications
Infrastructure as code	Pgs. 479-480 Applications
Software-defined networking (SDN)	
Software-defined visibility (SDV)	
Serverless architecture	Pg. 483 Serverless Architecture
Services integration	Pg. 482 Cloud Services
Resources policies	Pgs. 488-489 Resource Policies
Transit gateway	Pg. 479 Hardware
Virtualization	Pg. 489 Virtualization
Virtual machine (VM) sprawl avoidance	Pgs. 490-492 VM Sprawl Avoidance
VM escape protection	Pg. 492 VM Escape Protection
2.3: Summarize secure application development, deployment, and automation concepts.	
Environment	
Development	Pg. 209 Application Development Pg. 215 Secure Application Development
Test	Pg. 210 Test Environment
Staging	Pg. 210 Staging Environment
Production	Pg. 210 Production Environment
Quality assurance (QA)	Pg. 210 Test Environment

Standard	Corresponding Page(s)
Provisioning and deprovisioning	Pg. 215 Development Resources
Integrity measurement	Pg. 217 Integrity Measurement
Secure coding techniques	
Normalization	Pg. 219 Normalization
Stored procedures	Pg. 220 Stored Procedures
Obfuscation/camouflage	Pg. 219 Obfuscation
Code reuse/dead code	Pgs. 219-220 Code Reuse
Server-side vs. client-side execution and validation	Pg. 218 Input Validation
Memory management	Pg. 220 Memory Management
Use of third-party libraries and software development kits (SDKs)	Pgs. 219-220 Code Reuse
Data exposure	Pg. 227 Data Exposure
Open Web Application Security Project (OWASP)	Pg. 217 Secure Coding Techniques
Software diversity	Pgs. 215-216 Software Diversity
Complier	
Binary	
Automation/scripting	Pgs. 213-214 DevOps
Automated courses of action	
Continuous monitoring	
Continuous validation	
Continuous integration	
Continuous delivery	
Continuous deployment	
Elasticity	Pgs. 216-217 Elasticity
Scalability	Pg. 216 Scalability
Version control	Pg. 217 Version Control
2.4: Summarize authentication and authorization design concept	
Authentication methods	
Directory services	Pgs. 120-121 Directory Services
Federation	Pgs. 124-125 Federated Identity Management (FIM)
Attestation	Pgs. 109-110 Authentication and Access Control
Technologies	
Time-based on-time password (TOTP)	Pgs. 157-159 Token
HMAC-based one-time password (HOTP)	Pgs. 157-159 Token
Short message service (SMS)	Pg. 245 Authentication Pgs. 109–110 Authentication and Access Control
Token key	Pgs. 114-115 Token Pgs. 157-159 Token
Static codes	Pg. 257 Multifunction Printers
Authentication applications	Pg. 115 Tokens
Push notifications	Pgs. 224-225 Authentication
Phone call	Pgs. 224-225 Authentication

Standard	Corresponding Page(s)
Smart card authentication	Pg. 157 Smart Card
Biometrics	Pgs. 115-116 Standard Biometrics
Fingerprint	
Retina	
Iris	
Facial	
Voice	
Vein	
Gait analysis	
Efficacy rates	
False acceptance	
False rejection	
Crossover error rate	
Multifactor authentication (MFA) factors and attributes	Pg. 113 Multifactor Authentication
Factors	
Something you know	
Something you have	
Something you are	
Attributes	
Somewhere you are	
Something you can do	
Something you exhibit	
Someone you know	
Authentication, authorization, and accounting (AAA)	Pg. 110 Authentication and Access Control
Cloud vs. on-premises requirements	Pgs. 486-487 Authentication
2.5 Given a scenario, implement cybersecurity resilience	
Redundancy	Pg. 565 Redundancy
Geographic dispersal	Pgs. 570-572 Data Backup
Disk	
Redundant array of inexpensive (RAID) levels	Pg. 565 RAID
Multipath	Pg. 568 Multipathing
Network	
Load balancers	Pg. 216 Scalability Pg. 373-374 Load Balancer
Network interface card (NIC) teaming	Pg. 373-374 Load Balancer
Power	
Uninterruptible power supply (UPS)	Pg. 568 Uninterruptible Power Supply (UPS)
Generator	Pg. 568 Generator
Dual supply	Pgs. 568-569 Dual Supply
Managed power distributed units (PDUs)	Pg. 569 Power Distribution Units (PDUs)
Replication	
Storage area network (SAN)	Pgs. 570-572 Data Backup
VM	Pgs. 570-572 Data Backup
On-premises vs. cloud	Pg. 488 Cloud Security Controls

Standard	Corresponding Page(s)
Backup types	
Full	Pgs. 570-572 Data Backup
Incremental	Pgs. 570-572 Data Backup
Snapshot	Pgs. 570-572 Data Backup
Differential	Pgs. 570-572 Data Backup
Tape	Pgs. 570-572 Data Backup
Disk	Pgs. 570-572 Data Backup
Copy	Pgs. 570-572 Data Backup
Network attached storage (NAS)	Pgs. 570-572 Data Backup
SAN	Pgs. 570-572 Data Backup
Cloud	Pg. 476 Cloud Backup and Recovery Pgs. 570-572 Data Backup
Image	Pgs. 570-572 Data Backup
Online vs. offline	Pgs. 570-572 Data Backup
Offsite storage	Pgs. 570-572 Data Backup
Distance considerations	Pgs. 570-572 Data Backup
Non-persistence	Pg. 386 Non-Persistence
Revert to known state	
Last known good configuration	
Live boot media	
High availability	Pgs. 562-563 High Availability
Scalability	Pg. 216 Scalability Pg. 570 Disaster Recovery Plan
Restoration order	Pg. 572 Restoration Order
Diversity	
Technologies	Pgs. 11-12 Security Domains
Vendors	Pgs. 11-12 Security Domains
Crypto	Pgs. 271-272 Cryptography
Controls	Pgs. 11-12 Security Domains
2.6: Explain the security implications of embedded and specialized systems.	
Embedded systems	Pg. 249 Embedded Systems
Raspberry Pi	Pgs. 259-260 Raspberry Pi
Field programmable gate array (FPGA)	Pg. 260 Field-Programmable Gate Array (FPGA)
Arduino	Pg. 260 Arduino
System control and data acquisition (SCADA)/Industrial control system (ICS)	Pg. 251 Industrial Control Systems (ICS)
Facilities	
Industrial	
Manufacturing	
Energy	
Logistics	
Internet of Things (IoT)	Pg. 253 Internet of Things (IoT)
Sensors	Pg. 253 Internet of Things (IoT)
Smart devices	Pg. 254 Smart Devices

Standard	Corresponding Page(s)
Wearables	Pgs. 254-255 Wearable Technology
Facility automation	Pgs. 251-252Industrial Control System (ICS)
Weak defaults	Pg. 253 Internet of Things (IoT)
Specialized	
Medical systems	Pgs. 254-255 Wearable Technology Pg. 259 Medical Systems
Vehicles	Pgs. 255-266 Vehicles
Aircraft	Pg. 258 Aircraft
Smart meters	Pgs. 258-259 Smart Meters
Voice over IP (VoIP)	Pg. 260 VoIP
Heating, ventilation, air conditioning (HVAC)	Pgs. 251-252 Industrial Control System (ICS)
Drones/AVs	Pgs. 256-257 Drones
Multifunction printer (MFP)	Pg. 257 Multifunction Printers
Real-time operating system (RTOS)	Pg. 249 Real-Time Operating System (RTOS)
Surveillance systems	Pg. 259 Surveillance Systems
System on a chip (SoC)	Pg. 249 System on a Chip (SoC)
Communication considerations	
5G	Pgs. 456-457 Cellular Generations
Narrow-band	Pg. 459 Narrowband
Baseband radio	Pg. 460 Baseband
Subscriber identity module (SIM) cards	Pgs. 457-458 SIM Cards
Zigbee	Pg. 460 Zigbee
Constraints	Pg. 250 Constraints of Embedded Systems
Power	
Computer	
Network	
Crypto	
Inability to patch	
Authentication	
Range	
Cost	
Implied trust	
2.7 Explain the importance of physical security controls.	
Bollards/barricades	Pg. 156 Barricades
Mantraps	Pgs. 160-161 Mantraps
Badges	Pg. 157 Identification Badges
Alarms	Pg. 155 Alarms
Signage	Pg. 161 Signage
Cameras	Pg. 160 Closed-Circuit Television (CCTV)
Motion recognition	Pg. 160 Closed-Circuit Television (CCTV)
Object detection	Pg. 160 Closed-Circuit Television (CCTV)
Closed-circuit television (CCTV)	Pg. 160 Closed-Circuit Television (CCTV)
Industrial camouflage	Pg. 155 Industrial Camouflage
Personnel	Pg. 156 Personnel
Guards	

Standard	Corresponding Page(s)
Robot sentries	
Reception	
Two-person integrity/control	
Locks	Pgs. 159-160 Lock Access and Cable Locks
Biometrics	
Electronic	
Physical	
Cable locks	
USB data blocker	Pg. 58 USB Data Blocker
Lighting	Pg. 155 Lighting
Fencing	Pg. 155 Fencing
Fire suppression	Pgs. 164-165 Fire Control
Sensors	Pgs. 163-164 Hot and Cold Aisles
Motion detection	Pg. 155 Lighting PG. 155 Alarms
Noise detection	Pg. 155 Alarms
Proximity reader	Pg. 155 Gated Entrance Pgs. 159-160 Lock Access and Cable Locks
Moisture detection	Pg. 166 Water Control
Cards	Pg. 155 Gated Entrance Pgs. 159-160 Lock Access and Cable Locks
Temperature	Pg. 163 Temperature Control
Drones/UAV	Pgs. 256-257 Drones
Visitor logs	Pg. 161 Logs
Faraday cages	Pg. 162-163 Data Signal Protection
Air gap	Pg. 162 Air-Gap Network
Demilitarized zone (DMZ)	Pgs. 382-383 Demilitarized Zone (DMZ)
Protected cable distribution	Pg. 159 Protected Distribution and Cabling
Secure areas	
Air gap	Pgs. 160-161 Mantraps
Vault	Pgs. 159 Safes and Vaults
Safe	Pgs. 159 Safes and Vaults
Hot aisle	Pgs. 163-164 Hot and Cold Aisles
Cold aisle	Pgs. 163-164 Hot and Cold Aisles
Secure data destruction	Pg. 167 Data Destruction
Burning	Pg. 167 Destroying Paper-Based Data
Shredding	Pg. 167 Destroying Paper-Based Data
Pulping	Pg. 167 Destroying Paper-Based Data
Pulverizing	Pgs. 168-169 Physical Destruction
Degaussing	Pg. 168 Destroying Data on Digital Media
Third-party solutions	Pg. 168 Physical Destruction Tech Tip
2.8 Summarize the basics of cryptographic concepts	
Digital signatures	Pg. 301 Public Key Infrastructure
Key length	Pg. 273 Encryption
Key stretching	Pgs. 282-283 Key Stretching

Standard	Corresponding Page(s)
Salting	Pgs. 282-283 Key Stretching
Hashing	Pgs. 281-282 Hashing
Key exchange	Pgs. 275-276 Symmetric Encryption
Elliptical curve cryptography	Pg. 279 Elliptical-Curve Cryptography
Perfect forward secrecy	Pgs. 275-276 Symmetric Encryption
Quantum	Pgs. 287-288 Quantum Cryptography
Communications	
Computing	
Post-quantum	Pgs. 287-288 Quantum Cryptography
Ephemeral	Pg. 273 Encryption
Modes of operation	Pg. 273 Encryption
Authenticated	
Unauthenticated	
Counter	
Blockchain	Pg. 316 Blockchains
Public ledgers	
Cipher suites	Pg. 276 Symmetric Algorithm Types
Stream	
Block	
Symmetric vs. asymmetric	Pgs. 275-276 Symmetric Encryption Pg. 278 Asymmetric Encryption
Lightweight cryptography	Pg. 275 Low-Power Devices
Steganography	Pg. 282 Steganography
Audio	
Video	
Image	
Homomorphic encryption	Pg. 275 Low Latency
Common use cases	
Low power devices	Pg. 275 Low-Power Devices
Low latency	Pg. 275 Low Latency
High resiliency	Pg. 275 High Resilience
Supporting confidentiality	Pg. 272 Confidentiality
Supporting integrity	Pg. 272 Integrity
Supporting obfuscation	Pg. 272 Obfuscation
Supporting authentication	Pg. 272 Authentication
Supporting non-repudiation	Pg. 272 Nonrepudiation
Resource vs. security constraints	Pg. 275 Low-Power Devices
Limitations	
Speed	Pgs. 274-275 Cryptography Limitation
Size	Pgs. 273-274 Encryption
Weak keys	Pgs. 274-275 Cryptography Limitations
Time	Pgs. 274-275 Cryptography Limitations
Longevity	Pgs. 273-274 Encryption
Predictability	Pgs. 273-274 Encryption
Reuse	Pgs. 274-275 Cryptography Limitations

Standard	Corresponding Page(s)
Entropy	Pgs. 273-274 Encryption
Computational overheads	Pg. 275 Low-Power Devices
Resource vs. security constraints	Pg. 275 Low-Power Devices
3.0: Implementation	
3.1: Given a scenario, implement secure protocols	
Protocols	
Domain Name System Security Extension (DNSSEC)	Pgs. 413-414 DNS Poisoning Attack
SSH	Pg. 313 SSH Pg. 411 Secure Shell (SSH)
Secure/multipurpose Internet mail exchanger (S/MIME)	Pg. 313 S/MIME Pg. 410 Figure 13-1
Secure real-time protocol (SRTP)	Pg. 313 SRTP Pg. 410 Figure 13-1
LDAPS	Pg. 411 Lightweight Directory Access Protocol, Secure (LDAPS)
File transfer protocol, secure (FTPS)	Pg. 411 File Transfer Protocol (FTP)
Secured file transfer protocol (SFTP)	
Simple Network Management Protocol, version 3 (SNMPv3)	Pgs. 163-164 Hot and Cold Aisles Pg. 410 Figure 13-1
Hypertext transfer protocol over SSL/TLS (HTTPS)	Pg. 313HTTPS Pg. 410 Figure 13-1
IPSec	Pg. 314 IP Security Pg. 410 Figure 13-1
Authentication header (AH)/Encapsulated security payload (ESP)	Pg. 314 IP Security
Tunnel/Transport	
Secure post office protocol (POP)/Internet message access protocol (IMAP)	Pg. 412 E-Mail Protocols
Use cases	
Voice and audio	Pg. 409 Secure Protocols Pg. 410 Figure 13-1
Time synchronization	
Email and Web	
File transfer	
Directory Services	Pgs. 120-121 Directory Services Pg. 409 Secure Protocols Pg. 410 Figure 13-1
Remote access	Pg. 409 Secure Protocols Pg. 410 Figure 13-1
Domain name resolution	
Routing and switching	
Network address allocation	
Subscription services	
3.2: Given a scenario, implement host or application security solutions.	
Endpoint protection	Pg. 182 Endpoint Protection
Antivirus	Pg. 183 Antivirus and Antimalware
Anti-malware	Pg. 183 Antivirus and Antimalware

Standard	Corresponding Page(s)
Endpoint detection and response (EDR)	Pgs. 182-183 Endpoint Detection and Response
DLP	Pg. 183 Data Loss Prevention (DLP)
Next-generation firewall	Pg. 183 Firewall
Host intrusion prevention system (HIPS)	Pg. 183 Host Intrusion Systems
Host intrusion detection system (HIDS)	Pg. 183 Host Intrusion Systems
Host-based firewall	Pg. 183 Firewall
Boot integrity	Pg. 192 Boot Integrity
Boot security/Unified Extensible Firmware Interface (UEFI)	Pg. 193 UEFI
Measured boot	Pgs. 193-194 Measured Boot
Boot attestation	Pg. 193 Boot Attestation
Database	Pg. 195 Database Hardening
Tokenization	
Salting	
Hashing	
Application security	
Input validation	Pg. 218 Input Validation
Secure cookies	Pg. 220 Secure Cookies
Hypertext Transfer Protocol (HTTP) headers	Pg. 220 Secure HTTP Headers
Code signing	Pgs. 219-220 Code Reuse
Whitelisting	Pgs. 194-195 Application Hardening
Blacklisting	Pgs. 194-195 Application Hardening
Secure coding practices	Pg. 219 Normalization Pgs. 220-221 Stored Procedures Pg. 219 Obfuscation Pgs. 219-220 Code Reuse Pg. 218 Input Validation Pg. 220 Memory Management Pg. 227 Data Exposure
Static code analysis	Pg. 221 Black-Box Testing
Manual code review	Pg. 221 Black-Box Testing
Dynamic code analysis	Pg. 221 Black-Box Testing
Fuzzing	Pg. 221 Black-Box Testing
Hardening	
Open ports and services	Pg. 196 Services Pgs. 196-197 Ports
Registry	Pg. 191 Securing the Windows Registry
Disk encryption	Pg. 194 Disk Encryption
OS	Pgs. 185-186Operating System Hardening
Patch management	Pgs. 188-189 Patch Management
Third-party updates	
Auto-update	
Self-encrypting drive (SED)/full disk encryption (FDE)	Pg. 194 Disk Encryption
Opal	

Standard	Corresponding Page(s)
Hardware root of trust	Pgs. 193-194 Measured Boot
Trusted Platform Module (TPM)	Pgs. 193-194 Measured Boot
Sandboxing	Pg. 210 Test Environment
3.3 Given a scenario, implement secure network designs.	
Load balancing	Pgs. 373-374 Load Balancer
Active/active	
Active/passive	
Scheduling	
Virtual IP	
Persistence	
Network segmentation	
Virtual local area network (VLAN)	Pg. 390 Virtual Local Area Network (VLAN)
DMZ	Pgs. 382-383 Demilitarized Zone (DMZ)
East-west traffic	Pgs. 395-396 Microsegmentation
Extranet	Pg. 383 Intranets and Extranets
Intranet	Pg. 383 Intranets and Extranets
Zero trust	Pg. 383-384 Incorporating Zero Trust
Virtual private network (VPN)	
Always on	Pg. 390-392 Virtual Private Network (VPN)
Split tunnel vs. full tunnel	Pg. 390-392 Virtual Private Network (VPN)
Remote access vs. site-to-site	Pg. 390-392 Virtual Private Network (VPN)
IPSec	Pg. 392-393 VPN Protocols
SSL/TLS	Pgs. 311-312 SSL/TLS
HTML5	Pgs. 392-393 VPN Protocols
Layer 2 tunneling protocol (L2TP)	Pgs. 392-393 VPN Protocols
DNS	Pgs. 410-411 Domain Name System (DNS)
Network access control (NAC)	Pgs. 414-415Network Access Control (NAC)
Agent and agentless	
Out-of-band management	Pg. 379 Network Intrusion Detection
Port security	
Broadcast storm prevention	Pg. 371 Loop Prevention
Bridge Protocol Data Unit (BPDU) guard	Pg. 371 Loop Prevention
Loop prevention	Pg. 371 Loop Prevention
Dynamic Host Configuration Protocol (DHCP) snooping	Pg. 371 DHCP Snooping
Media access control (MAC) filtering	Pgs. 370-371 Port Security Pg. 461 MAC Address Filtering
Network appliances	
Jump servers	Pg. 375 Jump Server
Proxy servers	Pg. 374 Proxy Server
Forward	
Reverse	
Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS)	Pgs. 379-380 Network Detection System Pg. 381 Intrusion-Prevention Systems

Standard	Corresponding Page(s)
Signature based	Pg. 380 Signature-Based Monitoring
Heuristic/behavior	Pg. 380 Heuristic-Based Monitoring
Anomaly	Pg. 380 Anomaly Monitoring
Inline vs. passive	Pgs. 379-380 Network Detection System Pg. 381 Intrusion-Prevention System
HSM	Pg. 246 MicroSD Hardware Security Module Pg. 381 Figure 12-9
Sensors	Pgs. 379-380 Network Detection System
Collectors	Pgs. 379-380 Network Detection System
Aggregators	Pg. 375 Aggregator
Firewalls	
Web application firewall (WAF)	Pg. 379 Web Application Firewall (WAF)
Next-generation firewall	Pg. 183 Firewall
Stateful	Pg. 377-378 Stateful Firewall
Stateless	Pg. 378 Stateless Firewall
Unified threat management (UTM)	Pg. 379 Unified Threat Management Device
Network address translation (NAT) gateway	Pg. 383 Network Address Translation
Content/URL filter	Pg. 379 Content Filter
Open-source vs. proprietary	Pgs. 375-377 Firewalls
Hardware vs. software	Pgs. 375-377 Firewalls
Appliance vs. host-based vs. virtual	Pgs. 375-377 Firewalls
Access control list (ACL)	Pg. 373 Access Control Lists (ACLs)
Route security	Pg. 372 Route Security
Quality of service (QoS)	Pg. 368 Secure Network Design
Implications of IPv6	Pg. 385-386 Internet Protocol (IP) Schema
Port spanning/port mirroring	Pgs. 379-380 Network Detection System
Port taps	Pgs. 379-380 Network Detection System
Monitoring services	Pg. 416 Monitoring Services
File integrity monitors	Pg. 416 File Integrity Monitoring
3.4: Given a scenario, install and configure wireless security settings.	
Cryptographic protocols	
Wi-Fi protected access II (WPA2)	Pg. 449 Wi-Fi Protected Access II (WPA2)
Wi-Fi protected access III (WPA3)	Pgs. 450-451 Wi-Fi Protected Access III (WPA3)
Counter-mode/CBC-MAC protocol (CCMP)	Pg. 449 Wi-Fi Protected Access 2 (WPA2)
Simultaneous Authentication of Equals (SAE)	Pgs. 450-451 Wi-Fi Protected Access III (WPA3)
Authentication protocols	
Extensible Authentication Protocol (EAP)	Pg. 448 Wi-Fi Protected Access (WPA)
Protected Extensible Application Protocol (PEAP)	Pg. 450 PEAP
EAP-FAST	Pg. 450 EAP-FAST
EAP-TLS	Pg. 450 EAP-TLS
EAP-TTLS	Pg. 450 EAP-TTLS
IEEE 802.1X	Pg. 157 Smart Card Pgs. 449-450 802.1X

Standard	Corresponding Page(s)
Remote Authentication Dial-In User Sever (RADIUS) Federation	Pg. 127 Remote Access Authentication Pgs. 449-450 802.1X
Methods	
Pre-shared key (PSK) vs. Enterprise Vs. Open	Pg. 448 Wi-Fi Protected Access (WPA) Pgs. 449-450 802.1X
Wi-Fi Protected Setup (WPS)	Pg. 448 Wi-Fi Protected Setup (WPS)
Captive Portals	Pg. 456 Captive Portal
Installation considerations	
Site surveys	Pg. 451 Site Survey
Heat maps	Pg. 451-452 Predictive Site Survey
Wi-Fi analyzers	Pg. 452 Wi-Fi Survey
Channel overlays	Pg. 451 Site Survey
Wireless access point (WAP) placement	Pgs. 455-456 Antennae Types and Placement
Controller and access point security	Pgs. 452-453 Wireless Access Point
3.5: Given a scenario, implement secure mobile solutions.	
Connection methods and receivers	
Cellular	Pg. 241 Cellular Pg. 456 Cellular
Wi-Fi	Pg. 242 Wi-Fi Pg. 458 WLAN
Bluetooth	Pg. 241 Bluetooth Pg. 458 Bluetooth
NFC	Pg. 458 NFC
Infrared	Pg. 459 Infrared
USB	Pg. 241 USB
Point to point	Pgs. 455-456 Antennae Types and Placement
Point to multipoint	Pgs. 455-456 Antennae Types and Placement
Global Positioning System (GPS)	Pgs. 243-244 Physical Security Pg. 459 GPS
RFID	Pg. 459 Radio Frequency Identification (RFID)
Mobile device management (MDM)	
Application management	Pgs. 242-243 Management Tools
Content management	Pgs. 242-243 Management Tools
Remote wipe	Pgs. 243-244 Physical Security
Geofencing	Pgs. 243-244 Physical Security
Geolocation	Pgs. 243-244 Physical Security
Screen locks	Pgs. 244-245 Authentication
Push notifications	Pgs. 244-245 Authentication Pg. 246 Push Notification
Passwords and pins	Pgs. 242-243Management Tools
Biometrics	Pgs. 244-245 Authentication
Context-aware authentication	Pg. 245 Context-Aware Authentication
Containerization	Pg. 246 Storage Segmentation
Storage segmentation	Pg. 246 Storage Segmentation
Full device encryption	Pgs. 239-240 Mobile Devices

Standard	Corresponding Page(s)
Mobile devices	
MicroSD HSM	Pg. 246 MicroSD Hardware Security Module
MDM/Unified endpoint management (UEM)	Pgs. 242-243 Management Tools
Mobile application management (MAM)	Pgs. 242-243 Management Tools
SEAndorid	Pg. 246 SEAndorid
Enforcement and monitoring of:	
Third-party app stores	Pg. 247 Third-Party App Stores
Rooting/jailbreaking	Pg. 248 Bypassing Device Restrictions
Sideloading	Pg. 247 Third-Party App Stores
Custom firmware	Pgs. 248-249 Custom and Unauthorized Firmware
Carrier unlocking	Pg. 248 Bypassing Device Restrictions
Firmware over-the-air (OTA) updates	Pgs. 248-249Custom and Unauthorized Firmware
Camera use	Pg. 244 Cameras and Microphones
SMS/Multimedia message service (MMS)/Rich communication services (RCS)	Pg. 247-248 Text-Message Threats
External media	Pg. 247 External Media
USB on the go (OTG)	Pgs. 241-242 USB
Recording microphone	Pg. 244 Cameras and Microphones
GPS tagging	Pgs. 243-244 Physical Security
Wi-Fi direct/ad hoc	Pg. 242 Wi-Fi
Tethering	Pg. 241 Bluetooth
Hotspot	Pg. 242 Wi-Fi
Payment methods	Pg. 248 Mobile Payments
Deployment models	Pgs. 239-240 Mobile Devices
Bring your own device (BYOD)	
Corporate-owned personally enabled (COPE)	
Choose your own device (CYOD)	
Corporate-owned	
Virtual desktop infrastructure (VDI)	
3.6: Given a scenario, apply cybersecurity solutions to the cloud.	
Cloud security controls	
High availability across zones	Pg. 497 High Availability across Zones
Resource policies	Pgs. 488-489 Resource Policies
Secrets management	Pg. 489 Secrets Management
Integration and auditing	Pg. 488 Integration and Auditing
Storage	Pgs. 478-479 Storage
Permissions	
Encryptions	
Replication	
High availability	
Network	
Virtual networks	Pgs. 489-490 Virtual Networks
Public and private subnets	Pgs. 489-490 Virtual Networks

Standard	Corresponding Page(s)
Segmentation	Pg. 386 Segmentation
API inspection and integration	Pg. 487 Cloud Native Controls vs. Third-Party Solutions
Compute	
Security groups	Pg. 486 Security Groups
Dynamic resource allocation	Pg. 488 Integration and Auditing
Instance awareness	Pg. 478 Servers
Virtual private cloud (VPS) endpoint	Pgs. 489-490 Virtual Networks
Container security	Pg. 490 Containers
Solutions	
CASB	Pg. 485 Cloud Access Security Broker (CASB)
Application security	Pg. 490 Containers
Next-generation secure web gateway (SWG)	Pg. 486 Next-Generation Secure Web Gateway (SWG)
Firewall considerations in a cloud environment	
Cost	Pgs. 485-486 Firewalls
Need for segmentation	Pg. 386 Segmentation
Open Systems Interconnection (OSI) layers	Pgs. 485-486 Firewalls Pg.386 Segmentation
Cloud native controls vs. third-party solutions	Pg. 487 Cloud Native Controls vs. Third-Party Solutions
3.7: Given a scenario, implement identity and account management controls.	
Identity	
Identity provider (IdP)	Pg. 125 Security Assertion Markup Language (SAML)
Attributes	Pg. 125 Security Assertion Markup Language (SAML) Pg. 116 Attributes
Certificates	Pgs. 301-302 Digital Certificate
Tokens	Pg. 114 Tokens Pgs. 157-158 Token
SSH Keys	Pg. 313 SSH
Smart cards	Pg. 157 Smart Cards
Account types	Pgs. 127-128 Account Types
User account	
Shared and generic accounts/credentials	
Guest accounts	
Service accounts	
Account policies	
Password complexity	Pg. 129 Password Policy
Password history	Pg. 129 Password Policy
Password reuse	Pg. 129 Password Policy
Time of day	Pg. 133 Group-Based Access Control
Network location	Pg. 133 Group-Based Access Control
Geofencing	Pg. 117 Somewhere You Are

Standard	Corresponding Page(s)
Geotagging	Pg. 117 Somewhere You Are
Geolocation	Pg. 117 Somewhere You Are
Time-based logins	Pg. 245 Context-Aware Authentication
Access policies	Pg. 128 Account Policy Enforcement
Account permissions	Pg. 133 Account Auditing
Account audits	Pg. 133 Account Auditing
Impossible travel time/risky login	Pgs. 244-245 Authentication Pg. 245 Context-Aware Authentication
Lockout	Pg. 130 Account Policy Enforcement Pg. 245 Lockout
Disablement	Pg. 128 Account Policy Enforcement
3.8: Given a scenario, implement authentication and authorization solutions.	
Authentication management	
Password keys	Pg. 111 Weak Passwords Tech Tip
Password vaults	Pgs. 242-243 Management Tools
TPM	Pg. 193 Measured Boot
HSM	Pg. 246MicroSD Hardware Security Module
Knowledge-based authentication	Pg. 113What You Know
Authentication	
EAP	Pgs. 394-395 Extensible Authentication Protocol (EAP) Pg. 448 Wi-Fi Protected Access (WPA)
Challenge Handshake Authentication Protocol (CHAP)	Pg. 394 Challenge Handshake Authentication Protocol (CHAP)
Password Authentication Protocol (PAP)	Pg. 393 Password Authentication Protocol (PAP)
802.1X	Pg. 157 Smart Card Pg. 449 802.1X
RADIUS	Pg. 127 Remote Access Authentication Pg. 449 802.1X
Single sign-on (SSO)	Pg. 124 Single Sign-On (SSO)
Security Assertions Markup Language (SAML)	Pg. 125 Security Assertion Markup Language (SAML)
Terminal Access Controller Access Control System Plus (TACACS+)	Pg. 127 Remote Access Authentication
OAuth	Pg. 125 OAuth
OpenID	Pg. 126 OpenID Connect
Kerberos	Pg. 121 Directory Authentication
Access control schemes	
Attribute-based access control (ABAC)	Pg. 118 Attribute-Based Access Control (ABAC)
Role-based access control	Pg. 118 Discretionary Access Control (DAC)
Rule-based access control	Pg. 118 Discretionary Access Control (DAC)
MAC	Pg. 118 Mandatory Access Control (MAC)
Discretionary access control (DAC)	Pg. 118 Discretionary Access Control (DAC)

Standard	Corresponding Page(s)
Conditional access	Pg. 243 Securing Mobile Devices
Privilege access management	Pg. 127 Account Management Practices Pg. 128 Account Types Pg. 133 File System Permissions
File system permissions	Pg. 133 File System Permissions
3.9: Given a scenario, implement public key infrastructure.	
Public key infrastructure (PKI)	
Key management	Pg. 301 Public Key Infrastructure
Certificate authority (CA)	Pg. 302 Certificate Authority
Intermediate CA	Pg. 302 Certificate Signing Request (CSR)
Registration authority (RA)	Pg. 302 Certificate Signing Request (CSR)
Certificate revocation list (CRL)	Pg. 304 Certificate Revocation List (CRL)
Certificate attributes	Pg. 310 Certificate Attributes
Online Certificate Status Protocol (OCSP)	Pg. 304 Online Certificate Status Protocol (OCSP)
Certificate signing request (CSR)	Pg. 302 Certificate Signing Request (CSR)
CN	Pg. 310 Certificate Attributes
SAN	Pg. 308 Subject Alternative Name (SAN) Certificate
Expiration	Pg. 310 PKI Management
Types of certificates	
Wildcard	Pgs. 307-308 Wildcard Certificate
SAN	Pg. 308 Subject Alternative Name (SAN) Certificate
Code signing	Pg. 309 Code Signing
Self-signed	Pg. 309 Self-Signed Digital Certificates
Machine/computer	Pg. 308 Machine
E-mail	Pg. 309 E-Mail
User	Pg. 309 User
Root	Pg. 307 Root Digital Certificate
Domain validation	Pg. 307 Domain Validation (DV) Certificate
Extended validation	Pg. 307 Extended Validation (EV) Certificate
Certificate formats	Pgs. 309-310 Certificate Formats
Distinguished encoding rules (DER)	
Privacy enhanced mail (PEM)	
Personal information exchange (PFX)	
.cer	
P12	
P7B	
Concepts	
Online vs. offline CA	Pgs. 302-303Certificate Signing Request (CSR)
Stapling	Pgs. 304-305 Online Certificate Status Protocol (OCSP)
Pinning	Pgs. 306-307 Pinning
Trust model	Pg. 303 Trust Model

Standard	Corresponding Page(s)
Key escrow	Pg. 310 PKI Management
Certificate chaining	Pgs. 305-306 Certificate Chaining
4.0: Operations and Incident Response	
4.1: Given a scenario, use the appropriate tool to assess organizational security.	
Network reconnaissance and discovery	
tracert/treaceroute	Pg. 329 Tracert
nslookup/dig	Pg. 329 NSlookup and dig
ipconfig/ifconfig	Pg. 330 IPConfig
nmap	Pg. 420 Nmap
ping/pathping	Pg. 329 Ping Pg. 328 Pathping
hping	Pg. 422 hping
netstat	Pg. 420 Netstat
netcat	Pg. 420 Netcat
IP scanners	Pg. 419 IP Scanners
arp	Pg. 330 ARP
route	Pg. 330 Route
curl	Pg. 420 Curl
the harvester	Pg. 423 Harvester
sn1per	Pg. 424 Sn1per
scanless	Pg. 423 Scanless
dnsenum	Pg. 422 DNSenum
Nessus	Pg. 425 Nessus
Cuckoo	Pg. 424 Cuckoo
File manipulation	
head	Pgs. 330-331 Piping
tail	Pgs. 330-331 Piping
cat	Pgs. 348-349 Cat 3
grep	Pg. 349 Grep
chmod	Pg. 349 Chmod
logger	Pgs. 351-353 Logger
Shell and script environments	
SSH	Pg. 411 Secure Shell (SSH)
PowerShell	Pgs. 337-338 Windows PowerShell
Python	Pg. 352 Python
OpenSSL	Pg. 352 OpenSSL
Packet capture and replay	Pgs. 417-419 Packet Capture and Replay
Tcpreplay	
Tcpdump	
Wireshark	
Forensics	Pgs. 449-450 Data Acquisition
dd	
Memdump	
WinHex	
FTK imager	

Standard	Corresponding Page(s)
Autopsy	
Exploitation frameworks	Pgs. 416-417 Exploitation Frameworks
Password crackers	Pg. 287 Password Cracking
Data sanitization	Pg. 168 Disk Sanitization Pg. 518 Sanitization
4.2: Summarize the importance of policies, processes, and procedures for incident response	
Incident response plans	Pg. 539 Incident Response Plan (IRP)
Incident response process	
Preparation	Pg. 538 Preparation
Identification	Pg. 538 Identification
Containment	Pg. 538 Containment
Eradication	Pg. 539 Eradication
Recovery	Pg. 539 Recovery
Lessons learned	Pg. 539 Lessons Learned
Exercises	Pg. 539 Incident Response Plan (IRP)
Tabletop	
Walkthroughs	
Simulations	
Attack frameworks	Pg. 542 Cybersecurity Frameworks
MITRE ATT&CK	
The Diamond Model of Intrusion Analysis	
Cyber Kill Chain	
Stakeholder management	Pg. 538 Preparation
Communication plan	Pg. 538 Preparation
Disaster recovery plan	Pg. 570 Disaster Recovery Plan (DRP)
Business continuity plan	Pg. 561 Business Continuity
Continuity of operation planning (COOP)	Pg. 561 Business Continuity
Incident response team	Pg. 539 Incident Response Plan(IRP)
Retention policies	Pg. 517 Data Retention Pgs. 449-450 Data Acquisition
4.3: Given an incident, utilize appropriate data sources to support an investigation	
Vulnerability scan output	Pgs. 74-75 Scanner Output
SIEM dashboards	Pg. 431 Security Information and Event Management (SIEM) 85-87SIEM Dashboard
Sensor	
Sensitivity	
Trends	
Alerts	
Correlation	
Log files	Pg. 88 Log Files Pgs. 431-432 Log File
Network	
System	
Application	
Security	
Web	
DNS	

Standard	Corresponding Page(s)
Authentication	
Dump files	
VoIP and call managers	
Session Initiation Protocol (SIP) traffic	
syslog/rsyslog/syslog-ng	Pg. 84 Syslog Pgs. 431-432 Log Files
journalctl	Pg. 84 Syslog Pgs. 431-432 Log Files
nxlog	Pg. 84 Syslog Pgs. 431-432 Log Files
Retention	Pgs. 449-450 Data Acquisition
Bandwidth monitors	Pg. 432 Bandwidth Monitors
Metadata	Pg. 546 Metadata
E-mail	
Mobile	
Web	
File	
Netflow/sflow	Pgs. 432-433 Netflow Pg. 433 sFlow
Echo	Pg. 433 ICMP Monitoring
IPfix	Pg. 433 IPfix
Protocol analyzer output	Pgs. 417-419 Packet Capture and Replay
4.4: Given an incident, apply mitigation techniques or controls to secure an environment.	
Reconfigure endpoint security solutions	
Application whitelisting	Pgs. 194-195 Application Hardening Pg. 541 Endpoint Security Solutions
Application blacklisting	Pgs. 194-195 Application Hardening Pg. 541 Endpoint Security Solutions
Quarantine	Pg. 541 Endpoint Security Solutions
Configuration changes	
Firewall rules	Pg. 541 Configuration Changes
MDM	Pgs. 242-243 Management Tools Pgs. 243-244 Physical Security Pgs. 244-245 Authentication Pgs. 246 Push Notification Pg. 245 Context-Aware Authentication Pg. 246 Storage Segmentation Pgs. 239-240 Mobile Devices Pg. 541 Configuration Changes
DLP	Pg. 183 Data Loss Prevention (DLP) Pg. 541 Configuration Changes
Content filter/URL filter	Pg. 541 Configuration Changes
Update or revoke certificates	Pg. 541 Configuration Changes
Isolation	Pg. 541 Endpoint Security Solutions
Containment	Pg. 538 Containment

Standard	Corresponding Page(s)
Segmentation	Pg. 538 Containment
Secure Orchestration, Automation, and Response (SOAR)	Pg. 541 SOAR
Runbooks	
Playbooks	
4.5: Explain the key aspects of digital forensics.	
Documentation/evidence	
Legal hold	Pgs. 545-546 Secure the Area
Video	Pg. 548 Capture Video
Admissibility	Pgs. 543–544 Digital Forensics Pgs. 545–546 Secure the Area
Chain of custody	Pg. 544 Chain of Custody
Timeliness of sequence of events	Pg. 546 Metadata
Time stamps	
Time offset	
Tags	Pgs. 549-550 Data Acquisition
Reports	Pg. 550 Forensics Report
Event logs	Pg. 546 Metadata
Interviews	Pg. 548 Interviews
Acquisition	
Order of volatility	Pgs. 544-545 Order of Volatility
Disk	Pgs. 544-545 Order of Volatility
Random-access memory (RAM)	Pgs. 544-545 Order of Volatility
Swap/pagefile	Pgs. 544-545 Order of Volatility
OS	Pgs. 544-545 Order of Volatility
Device	Pgs. 544-545 Order of Volatility
Firmware	Pgs. 544-545 Order of Volatility
Snapshot	Pgs. 549-550 Data Acquisition
Cache	Pgs. 544-545 Order of Volatility
Network	Pgs. 544-545 Order of Volatility
Artifacts	Pgs. 549-550 Data Acquisition
On-premises vs. cloud	Pg. 550-551 Cloud Forensics
Right to audit clauses	
Regulatory/jurisdiction	
Data breach notification laws	
Integrity	Pg. 546 Capture the System Image
Hashing	Pgs. 546-547 Hash
Checksums	Pg. 547 Checksum
Provenance	Pg. 547 Digital Provenance
Preservation	Pgs. 545-546 Secure the Area
E-discovery	Pgs. 549-550 Data Acquisition
Data recovery	Pgs. 549-550 Data Acquisition
Nonrepudiation	Pg. 550 Forensics Report
Strategic intelligence/counterintelligence	Pg. 548-549 Forensics Procedure

Standard	Corresponding Page(s)
5.0: Governance, Risk, and Compliance	
5.1: Compare and contrast various types of controls.	
Category	Pg. 506 Strategies
Managerial	
Operational	
Technical	
Control type	Pgs. 153-154 Security Controls Pg. 506 Control Types
Preventive	
Detective	
Corrective	
Deterrent	
Compensating	
Physical	
5.2: Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	
Regulations, standards, and legislation	Pgs. 15-16 Regulatory Compliance
General Data Protection Regulation (GDPR)	
National, territory, or state laws	
Payment Card Industry Data Security Standard (PCI DSS)	Pgs. 8-9 Payment Card Industry Data Security Standard (PCI DSS)
Key frameworks	
Center for Internet Security (CIS)	Pg. 10 CIS Critical Security Controls
National Institute of Standards and Technology (NIST) RMF/CSF	Pg. 10-11 NIST Framework for Improving Critical Infrastructure Cybersecurity
International Organization for Standardization ISO) 27001/27002/27701/31000	Pgs. 9-10 ISO Standards
SSAE SOC2 Type II/III	Pg. 10 SSAE SOC2
Cloud Security alliance	Pg. 488 Cloud Security Controls
Cloud control matrix	
Reference architecture	
Benchmarks/secure configuration guides	Pgs. 6-7 Information Security Plan
Platform/vendor-specific guides	Pg. 15 System
Web server	
OS	
Application server	
Network infrastructure devices	
5.3: Explain the importance of policies to organization security.	
Personnel	
Acceptable use policy	Pg. 520 Acceptable Use Policy
Job rotation	Pg. 521-522 Job Rotation
Mandatory vacation	Pg. 521 Mandatory Vacation
Separation of duties	Pg. 524 Separation of Duties
Least privilege	Pg. 132 Least Privilege
Clean desk space	Pg. 523 Clean-Desk Policy
Background checks	Pg. 519 Background Checks

Standard	Corresponding Page(s)
Nondisclosure agreement (NDA)	Pg. 520 Employment Contracts
Social media analysis	Pg. 523 Social Media Analysis
Onboarding	Pg. 132 Employee Onboarding and Offboarding PG. 524 Onboarding
Offboarding	Pg. 132 Employee Onboarding and Offboarding Pgs. 524-525 Offboarding
User training	Pgs. 522-523 Employee User Training
Gamification	
Capture the flag	
Phishing campaigns	
Phishing simulations	Pgs. 522-523 Employee User Training
Computer-based training (CBT)	Pgs. 522-523 Employee User Training
Role-based training	Pg. 520-521 Role-Based Awareness Training
Diversity of training techniques	Pgs. 522-523 Employee User Training
Third-party risk management	Pgs. 525-526 Third-Party Risk Management
Vendors	
Supply chain	
Business partners	
Service level agreement (SLA)	
Memorandum of understanding (MOU)	
Measurement systems analysis (MSA)	
Business partnership agreement (BPA)	
End of life (EOL)	
End of service (EOS)	
NDA	
Data	
Classification	Pgs. 516-517 Data Clearance
Governance	Pgs. 506-507 Governance
Retention	Pg. 517 Data Retention
Credential policies	Pg. 507 Credential Policies
Personnel	
Third party	
Devices	
Service accounts	
Administrator/root accounts	
Organizational policies	
Change management	Pg. 508 Change Management
Change control	Pg. 508 Change Management
Asset management	Pg. 508 Asset Management
5.4: Summarize risk management processes and concepts.	
Risk types	
External	Pg. 510-511 Threat Assessment

Standard	Corresponding Page(s)
Internal	Pg. 510-511 Threat Assessment
Legacy systems	Pg. 510-511 Threat Assessment
Multiparty	Pgs. 525-526 Third-Party Risk Management (TPRM)
IP theft	Pg. 515-516 Data Clearance
Software compliance/licensing	Pg. 520 Acceptable Use Policy
Risk management strategies	
Acceptance	Pg. 514 Risk Acceptance
Avoidance	Pg. 513 Risk Avoidance
Transference	Pg. 513 Risk Transfer
Cybersecurity insurance	Pg. 513 Risk Transfer
Mitigation	Pg. 514 Risk Mitigation
Risk analysis	
Risk register	Pg. 512-513 Risk Evaluation
Risk matrix/heat map	Pgs. 511-512 Risk Analysis
Risk control assessment	Pgs. 511-512 Risk Analysis
Risk control self-assessment	Pgs. 511-512 Risk Analysis
Risk awareness	Pg. 509 Risk Management
Inherent risk	Pg. 514 Risk Mitigation
Residual risk	Pg. 514 Risk Mitigation
Control risk	Pgs. 511-512 Risk Analysis
Risk appetite	Pgs. 511-512 Risk Analysis
Regulations that affect risk posture	Pg. 508 Asset Management
Risk assessment types	Pg. 512 Risk Impact
Qualitative	
Quantitative	
Likelihood of occurrence	Pg. 512 Risk Impact
Impact	Pg. 512 Risk Impact
Asset value	Pgs. 512-513 Risk Evaluation
Single loss expectancy (SLE)	Pgs. 512-513 Risk Evaluation
Annualized loss expectancy (ALE)	Pgs. 512-513 Risk Evaluation
Annualized rate of occurrence (ARO)	Pg. 512 Risk Impact
Disasters	Pg. 510-511 Threat Assessment
Environmental	
Man-made	
Internal vs. external	
Business impact analysis	
Recovery time objective (RTO)	Pgs. 562-563 High Availability
Recovery point objective (RPO)	Pgs. 562-563 High Availability
Mean time to repair (MTTR)	Pg. 565 MTTR
Mean time between failures (MTBF)	Pg. 565 MTBF
Functional recovery plans	Pg. 570 Disaster Recovery Plan (DRP)
Single point of failure	PG. 568 Multipathing
Disaster recovery plan (DRP)	Pg. 570 Disaster Recovery Plan (DRP)
Mission essential functions	Pgs. 562-563 Business Impact Analysis

Standard	Corresponding Page(s)
Identification of critical systems	Pgs. 562-563 Business Impact Analysis
Site risk assessment	Pg. 561 Business Continuity
5.5: Explain privacy and sensitive data concepts in relation to security.	
Organizational consequences of privacy breaches	Pgs. 516-517 Data Clearance
Reputation damage	
Identity theft	
Fines	
IP theft	
Notifications of breaches	Pgs. 516-517 Data Clearance
Escalation	
Public notifications and disclosures	
Data types	
Classifications	Pgs. 516-517 Data Clearance Figure 16-3
Public	
Private	
Sensitive	
Confidential	
Critical	
Proprietary	
Personally identifiable information (PII)	Pgs. 505-506 Governance
Health information	Pgs. 505-506 Governance
Financial information	Pgs. 505-506 Governance
Government data	Pgs. 505-506 Governance
Customer data	Pgs. 505-506 Governance
Privacy enhancing technologies	
Data minimization	Pg. 517 Data Minimization
Data masking	Pg. 518 Data Masking
Tokenization	Pg. 518 Tokenization
Anonymization	Pg. 518 Data Anonymization
Pseudo-anonymization	Pg. 519 Pseudoanonymization
Roles and responsibilities	Pgs. 505-506 Governance Pg. 508 Figure 16-1
Data owners	
Data controller	
Data processor	
Data custodian/steward	
Data privacy officer (DPO)	
Information life cycle	Pgs. 515-516 Data Life Cycle
Impact assessment	Pgs. 505-506 Governance
Terms of agreement	Pgs. 505-506 Governance
Privacy notice	Pgs. 505-506 Governance