

PEARSON IT
CERTIFICATION

Save 10%
on Exam
Voucher

See Inside



Practice
Tests



Flash
Cards



Review
Exercises



Study
Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Security+

SY0-601



OMAR SANTOS
RON TAYLOR
JOSEPH MLODZIANOWSKI

Special Offer

Save 80% on Premium Edition eBook and Practice Test

The *CompTIA Security+ SY0-601 Cert Guide Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.

CompTIA Security+ SY0-601 Cert Guide

Table of Contents

Cover

Half Title

Copyright Page

Contents at a Glance

Table of Contents

Introduction

Part I: Threats, Attacks, and Vulnerabilities

Chapter 1 Comparing and Contrasting Different Types of Social
Engineering Techniques

Do I Know This Already? Quiz

Foundation Topics

Social Engineering Fundamentals

Phishing and Spear Phishing

Smishing

Vishing

Spam and Spam over Internet Messaging (SPIM)

Dumpster Diving

Shoulder Surfing

Pharming

Piggybacking or Tailgating

Eliciting Information

Whaling

Prepending

Identity Fraud

Invoice Scams

Table of Contents

Credential Harvesting

Reconnaissance

Hoaxes

Impersonation or Pretexting

Eavesdropping

Baiting

Watering Hole Attack

Typo Squatting

Influence Campaigns, Principles of Social Engineering, and Reasons for Effectiveness

User Security Awareness Education

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 2 Analyzing Potential Indicators to Determine the Type of Attack

Do I Know This Already? Quiz

Foundation Topics

Malicious Software (Malware)

Ransomware and Cryptomalware

Trojans

Remote Access Trojans (RATs) and Rootkits

Worms

Fileless Virus

Command and Control, Bots, and Botnets

Logic Bombs

Potentially Unwanted Programs (PUPs) and Spyware

Keyloggers

Backdoors

Malware Delivery Mechanisms

You Can't Save Every Computer from Malware!

Password Attacks

Dictionary-based and Brute-force Attacks

Table of Contents

Password Spraying

Offline and Online Password Cracking

Rainbow Tables

Plaintext/Unencrypted

Physical Attacks

Malicious Flash Drives

Malicious Universal Serial Bus (USB) Cables

Card Cloning Attacks

Skimming

Adversarial Artificial Intelligence

Tainted Training Data for Machine Learning

Security of Machine Learning Algorithms

Supply-Chain Attacks

Cloud-based vs. On-premises Attacks

Cloud Security Threats

Cloud Computing Attacks

Cryptographic Attacks

Collision

Birthday

Downgrade

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 3 Analyzing Potential Indicators Associated with Application Attacks

Do I Know This Already? Quiz

Foundation Topics

Privilege Escalation

Cross-Site Scripting (XSS) Attacks

Injection Attacks

Structured Query Language (SQL) Injection Attacks

Table of Contents

SQL Injection Categories

Dynamic Link Library (DLL) Injection Attacks

Lightweight Directory Access Protocol (LDAP) Injection Attacks

Extensible Markup Language (XML) Injection Attacks

Pointer/Object Dereference

Directory Traversal

Buffer Overflows

Arbitrary Code Execution/Remote Code Execution

Race Conditions

Error Handling

Improper Input Handling

Compile-Time Errors vs. Runtime Errors

Replay Attacks

Request Forgeries

Application Programming Interface (API) Attacks

Resource Exhaustion

Memory Leaks

Secure Socket Layer (SSL) Stripping

Driver Manipulation

Pass the Hash

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 4 Analyzing Potential Indicators Associated with Network Attacks

Do I Know This Already? Quiz

Foundation Topics

Wireless Attacks

Evil Twin Attacks

Rogue Access Points

Table of Contents

Bluesnarfing Attacks

Bluejacking Attacks

Disassociation and Deauthentication Attacks

Jamming Attacks

Radio Frequency Identifier (RFID) Attacks

Near-Field Communication (NFC) Attacks

Initialization Vector (IV) Attacks

On-Path Attacks

Layer 2 Attacks

Address Resolution Protocol (ARP) Poisoning Attacks

Media Access Control (MAC) Flooding Attacks

MAC Cloning Attacks

Best Practices to Protect Against Layer 2 Attacks

Domain Name System (DNS) Attacks

Domain Hijacking Attacks

DNS Poisoning Attacks

Uniform Resource Locator (URL) Redirection Attacks

Domain Reputation

Distributed Denial-of-Service (DDoS) Attacks

Malicious Code or Script Execution Attacks

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 5 Understanding Different Threat Actors, Vectors, and Intelligence Sources

Do I Know This Already? Quiz

Foundation Topics

Actors and Threats

Attributes of Threat Actors

Attack Vectors

Table of Contents

Threat Intelligence and Threat Intelligence Sources

Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of
Indicator Information (TAXII)

Research Sources

The MITRE ATT&CK Framework

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 6 Understanding the Security Concerns Associated with Various Types of Vulnerabilities

Do I Know This Already? Quiz

Foundation Topics

Cloud-based vs. On-premises Vulnerabilities

Other Cloud-based Concerns

Server Defense

File Servers

Network Controllers

Email Servers

Web Servers

FTP Server

Zero-day Vulnerabilities

Weak Configurations

Third-party Risks

Improper or Weak Patch Management

Patches and Hotfixes

Patch Management

Legacy Platforms

The Impact of Cybersecurity Attacks and Breaches

Chapter Review Activities

Review Key Topics

Table of Contents

Define Key Terms

Review Questions

Chapter 7 Summarizing the Techniques Used in Security Assessments

Do I Know This Already? Quiz

Foundation Topics

Threat Hunting

Security Advisories and Bulletins

Vulnerability Scans

Credentialed vs. Noncredentialed

Intrusive vs. Nonintrusive

Common Vulnerability Scoring System (CVSS)

Logs and Security Information and Event Management (SIEM)

Security Orchestration, Automation, and Response (SOAR)

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 8 Understanding the Techniques Used in Penetration Testing

Do I Know This Already? Quiz

Foundation Topics

Penetration Testing

Bug Bounties vs. Penetration Testing

Passive and Active Reconnaissance

Exercise Types

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Part II: Architecture and Design

Table of Contents

Chapter 9 Understanding the Importance of Security Concepts in an Enterprise Environment

Do I Know This Already? Quiz

Foundation Topics

Configuration Management

Data Sovereignty and Data Protection

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Inspection

- API Considerations

- Data Masking and Obfuscation

- Encryption at Rest, in Transit/Motion, and in Processing

- Hashing

- Rights Management

- Geographical Considerations

- Data Breach Response and Recovery Controls

Site Resiliency

Deception and Disruption

- Fake Telemetry

- DNS Sinkhole

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 10 Summarizing Virtualization and Cloud Computing Concepts

Do I Know This Already? Quiz

Foundation Topics

Cloud Models

- Public, Private, Hybrid, and Community Clouds

Cloud Service Providers

Cloud Architecture Components

- Fog and Edge Computing

- Thin Clients

Table of Contents

Containers

Microservices and APIs

Infrastructure as Code

Serverless Architecture

Services Integration

Resource Policies

Transit Gateway

Virtual Machine (VM) Sprawl Avoidance and VM Escape Protection

Understanding and Avoiding VM Sprawl

Protecting Against VM Escape Attacks

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 11 Summarizing Secure Application Development, Deployment, and Automation Concepts

Do I Know This Already? Quiz

Foundation Topics

Software Development Environments and Methodologies

Application Provisioning and Deprovisioning

Software Integrity Measurement

Secure Coding Techniques

Core SDLC and DevOps Principles

Programming Testing Methods

Compile-Time Errors vs. Runtime Errors

Input Validation

Static and Dynamic Code Analysis

Fuzz Testing

Programming Vulnerabilities and Attacks

Testing for Backdoors

Memory/Buffer Vulnerabilities

XSS and XSRF

Table of Contents

More Code Injection Examples

Directory Traversal

Zero-Day Attack

Open Web Application Security Project (OWASP)

Software Diversity

Automation/Scripting

Elasticity and Scalability

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 12 Summarizing Authentication and Authorization Design Concepts

Do I Know This Already? Quiz

Foundation Topics

Authentication Methods

Directory Services

Federations

Attestation

Authentication Methods and Technologies

Time-Based One-Time Password (TOTP)

HMAC-Based One-Time Password (HOTP)

Short Message Service (SMS)

Token Key

Static Codes

Authentication Applications

Push Notifications

Phone Call Authentication

Smart Card Authentication

Biometrics

Fingerprints

Table of Contents

Retina

Iris

Facial

Voice

Vein

Gait Analysis

Efficacy Rates

False Acceptance

False Rejection

Crossover Error Rate

Multifactor Authentication (MFA) Factors and Attributes

Authentication, Authorization, and Accounting (AAA)

Cloud vs. On-premises Requirements

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 13 Implementing Cybersecurity Resilience

Do I Know This Already? Quiz

Foundation Topics

Redundancy

Geographic Dispersal

Disk Redundancy

Redundant Array of Inexpensive Disks

Multipath

Network Resilience

Load Balancers

Network Interface Card (NIC) Teaming

Power Resilience

Uninterruptible Power Supply (UPS)

Generators

Dual Supply

Table of Contents

Managed Power Distribution Units (PDUs)

Replication

Storage Area Network

Virtual Machines

On-premises vs. Cloud

Backup Types

Full Backup

Differential Backup

Incremental Backup

Non-persistence

High Availability

Restoration Order

Diversity

Technologies

Vendors

Crypto

Controls

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 14 Understanding the Security Implications of Embedded and Specialized Systems

Do I Know This Already? Quiz

Foundation Topics

Embedded Systems

Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)

Internet of Things (IoT)

Specialized Systems

Medical Systems

Table of Contents

Vehicles

Aircraft

Smart Meters

Voice over IP (VoIP)

Heating, Ventilation, and Air Conditioning (HVAC)

Drones

Multifunction Printers (MFP)

Real-Time Operating Systems (RTOS)

Surveillance Systems

System on a Chip (SoC)

Communication Considerations

5G

NarrowBand

Baseband Radio

Subscriber Identity Module (SIM) Cards

Zigbee

Embedded System Constraints

Power

Compute

Network

Crypto

Inability to Patch

Authentication

Range

Cost

Implied Trust

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 15 Understanding the Importance of Physical Security

Table of Contents

Controls

Do I Know This Already? Quiz

Foundation Topics

Bollards/Barricades

Access Control Vestibules

Badges

Alarms

Signage

Cameras

Closed-Circuit Television (CCTV)

Industrial Camouflage

Personnel

Locks

USB Data Blockers

Lighting

Fencing

Fire Suppression

Sensors

Drones

Visitor Logs

Faraday Cages

Air Gap

Screened Subnet (Previously Known as Demilitarized Zone [DMZ])

Protected Cable Distribution

Secure Areas

Secure Data Destruction

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Table of Contents

Chapter 16 Summarizing the Basics of Cryptographic Concepts

Do I Know This Already? Quiz

Foundation Topics

Digital Signatures

Key Length

Key Stretching

Salting

Hashing

Key Exchange

Elliptic-Curve Cryptography

Perfect Forward Secrecy

Quantum

Communications

Computing

Post-Quantum

Ephemeral

Modes of Operation

Electronic Code Book Mode

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Blockchain

Cipher Suites

Symmetric vs. Asymmetric Encryption

Lightweight Cryptography

Steganography

Audio Steganography

Video Steganography

Image Steganography

Homomorphic Encryption

Table of Contents

Common Use Cases

Limitations

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Part III: Implementation

Chapter 17 Implementing Secure Protocols

Do I Know This Already? Quiz

Foundation Topics

Protocols

- Domain Name System Security Extensions

- SSH

- Secure/Multipurpose Internet Mail Extensions

- Secure Real-Time Transport Protocol

- Lightweight Directory Access Protocol over SSL

- File Transfer Protocol, Secure

- Secure (or SSH) File Transfer Protocol

- Simple Network Management Protocol Version 3

- Hypertext Transfer Protocol over SSL/TLS

- IPsec

- Authentication Header/Encapsulating Security Payloads

- Tunnel/Transport

- Post Office Protocol/Internet Message Access Protocol

Use Cases

- Voice and Video

- Time Synchronization

- Email and Web

- File Transfer

- Directory Services

- Remote Access

- Domain Name Resolution

Table of Contents

- Routing and Switching
- Network Address Allocation
- Subscription Services

Chapter Review Activities

- Review Key Topics

- Define Key Terms

- Review Questions

Chapter 18 Implementing Host or Application Security Solutions

- Do I Know This Already? Quiz

- Foundation Topics

- Endpoint Protection

 - Antivirus

- Antimalware

 - Endpoint Detection and Response

 - Data Loss Prevention

- Next-Generation Firewall

- Host-based Intrusion Prevention System

- Host-based Intrusion Detection System

- Host-based Firewall

- Boot Integrity

 - Boot Security/Unified Extensible Firmware Interface

 - Measured Boot

 - Boot Attestation

- Database

 - Tokenization

 - Salting

 - Hashing

- Application Security

 - Input Validations

 - Secure Cookies

 - Hypertext Transfer Protocol Headers

Table of Contents

- End-to-End Headers
- Hop-by-Hop Headers
- Code Signing
- Allow List
- Block List/Deny List
- Secure Coding Practices
- Static Code Analysis
- Manual Code Review
- Dynamic Code Analysis
- Fuzzing

Hardening

- Open Ports and Services
- Registry
- Disk Encryption
- Operating System
- Patch Management

Self-Encrypting Drive/Full-Disk Encryption

- OPAL

Hardware Root of Trust

Trusted Platform Module

Sandboxing

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 19 Implementing Secure Network Designs

Do I Know This Already? Quiz

Foundation Topics

Load Balancing

- Active/Active
- Active/Passive
- Scheduling

Table of Contents

Virtual IP

Persistence

Network Segmentation

Application-Based Segmentation and Microsegmentation

Virtual Local Area Network

Screened Subnet

East-West Traffic

Intranets and Extranets

Zero Trust

Virtual Private Network

Remote Access vs. Site-to-Site

IPsec

IKEv1 Phase 1

IKEv1 Phase 2

IKEv2

SSL/TLS

HTML5

Layer 2 Tunneling Protocol

DNS

Network Access Control

Out-of-Band Management

Port Security

Broadcast Storm Prevention

Bridge Protocol Data Unit Guard

Loop Prevention

Dynamic Host Configuration Protocol Snooping

Media Access Control Filtering

Network Appliances

Jump Servers

Proxy Servers

Network-Based Intrusion Detection System/Network-Based Intrusion Prevention System

NIDS

NIPS

Table of Contents

Summary of NIDS vs. NIPS

Signature-Based

Heuristic/Behavior

Anomaly

Inline vs. Passive

HSM

Sensors

Collectors

Aggregators

Firewalls

Hardware vs. Software

Appliance vs. Host-based vs. Virtual

Access Control List

Route Security

Quality of Service

Implications of IPv6

Port Spanning/Port Mirroring

Monitoring Services

Performance Baselineing

File Integrity Monitors

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 20 Installing and Configuring Wireless Security Settings

Do I Know This Already? Quiz

Foundation Topics

Cryptographic Protocols

Wi-Fi Protected Access 2 (WPA2)

Wi-Fi Protected Access 3 (WPA3)

Counter-mode/CBC-MAC Protocol (CCMP)

Table of Contents

Simultaneous Authentication of Equals

Wireless Cryptographic Protocol Summary

Authentication Protocols

802.1X and EAP

IEEE 802.1x

Remote Authentication Dial-In User Service (RADIUS) Federation

Methods

Wi-Fi Protected Setup

Captive Portals

Installation Considerations

Controller and Access Point Security

Wireless Access Point Vulnerabilities

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 21 Implementing Secure Mobile Solutions

Do I Know This Already? Quiz

Foundation Topics

Connection Methods and Receivers

RFID and NFC

More Wireless Connection Methods and Receivers

Secure Implementation Best Practices

Mobile Device Management

MDM Security Feature Concerns: Application and Content Management

MDM Security Feature Concerns: Remote Wipe, Geofencing, Geolocation, Screen Locks,
Passwords and PINs, Full Device Encryption

Mobile Device Management Enforcement and Monitoring

Mobile Devices

MDM/Unified Endpoint Management

SEAndroid

Deployment Models

Table of Contents

Secure Implementation of BYOD, CYOD, and COPE

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 22 Applying Cybersecurity Solutions to the Cloud

Do I Know This Already? Quiz

Foundation Topics

Cloud Security Controls

Security Assessment in the Cloud

Understanding the Different Cloud Security Threats

Cloud Computing Attacks

High Availability Across Zones

Resource Policies

Integration and Auditing

Secrets Management

Storage

Permissions

Encryption

Replication

High Availability

Network

Virtual Networks

Public and Private Subnets

Segmentation

API Inspection and Integration

Compute

Security Groups

Dynamic Resource Allocation

Instance Awareness

Virtual Private Cloud Endpoint

Container Security

Table of Contents

Summary of Cloud Security Controls

Solutions

CASB

Application Security

Next-Generation Secure Web Gateway

Firewall Considerations in a Cloud Environment

Cost

Need for Segmentation

Open Systems Interconnection Layers

Summary of Cybersecurity Solutions to the Cloud

Cloud Native Controls vs. Third-Party Solutions

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 23 Implementing Identity and Account Management Controls

Do I Know This Already? Quiz

Foundation Topics

Identity

Identity Provider (IdP)

Authentication

Authentication by Knowledge

Authentication by Ownership

Authentication by Characteristic Attributes

Certificates

Tokens

SSH Keys

Smart Cards

Account Types

Account Policies

Introduction to Identity and Access Management

Phases of the Identity and Access Lifecycle

Table of Contents

- Registration and Identity Validation
- Privileges Provisioning
- Access Review
- Access Revocation
- Password Management
- Password Creation
- Attribute-Based Access Control (ABAC)
- Rights, Permissions, and Policies
- Users, Groups, and Account Permissions
- Permission Inheritance and Propagation

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 24 Implementing Authentication and Authorization Solutions

Do I Know This Already? Quiz

Foundation Topics

Authentication Management

- Password Keys
- Password Vaults
- Trusted Platform Module
- Hardware Security Modules
- Knowledge-Based Authentication

Authentication/Authorization

- Security Assertion Markup Language
- OAuth
- OpenID and OpenID Connect
- 802.1X and EAP
- LDAP
- Kerberos and Mutual Authentication
- Remote Authentication Technologies
- Remote Access Service

Table of Contents

RADIUS versus TACACS+

Access Control Schemes

Discretionary Access Control

Mandatory Access Control

Role-Based Access Control

Attribute-Based Access Control

Rule-Based Access Control

Conditional Access

Privileged Access Management

Summary of Access Control Models

Access Control Wise Practices

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 25 Implementing Public Key Infrastructure

Do I Know This Already? Quiz

Foundation Topics

Public Key Infrastructure

Key Management

Certificate Authorities

Certificate Attributes

Subject Alternative Name

Expiration

Types of Certificates

SSL Certificate Types

Certificate Chaining

Certificate Formats

PKI Concepts

Trust Model

Certificate Pinning

Stapling, Key Escrow, Certificate Chaining, Online vs. Offline CA

Table of Contents

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Part IV: Operations and Incident Response

Chapter 26 Using the Appropriate Tool to Assess Organizational Security

Do I Know This Already? Quiz

Foundation Topics

Network Reconnaissance and Discovery

tracert/traceroute

nslookup/dig

ipconfig/ifconfig

nmap

ping/pathping

hping

netstat

netcat

IP Scanners

arp

route

curl

theHarvester

sn1per

scanless

dnsenum

Nessus

Cuckoo

File Manipulation

head

tail

cat

grep

Table of Contents

chmod

Logger

Shell and Script Environments

SSH

PowerShell

Python

OpenSSL

Packet Capture and Replay

Tcpreplay

Tcpdump

Wireshark

Forensics

dd

Memdump

WinHex

FTK Imager

Autopsy

Exploitation Frameworks

Password Crackers

Data Sanitization

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 27 Summarizing the Importance of Policies, Processes, and Procedures for Incident Response

Do I Know This Already? Quiz

Foundation Topics

Incident Response Plans

Incident Response Process

Preparation

Table of Contents

Identification

Containment

Eradication

Recovery

Lessons Learned

Exercises

Tabletop

Walkthroughs

Simulations

Attack Frameworks

MITRE ATT&CK

The Diamond Model of Intrusion Analysis

Cyber Kill Chain

Stakeholder Management

Communication Plan

Disaster Recovery Plan

Business Continuity Plan

Continuity of Operations Planning (COOP)

Incident Response Team

Retention Policies

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 28 Using Appropriate Data Sources to Support an Investigation

Do I Know This Already? Quiz

Foundation Topics

Vulnerability Scan Output

SIEM Dashboards

Sensors

Table of Contents

Sensitivity

Trends

Alerts

Correlation

Log Files

Network

CVBSystem

Application

Security

Web

DNS

Authentication

Dump Files

VoIP and Call Managers

Session Initiation Protocol Traffic

syslog/rsyslog/syslog-ng

journalctl

NXLog

Bandwidth Monitors

Metadata

Email

Mobile

Web

File

NetFlow/sFlow

NetFlow

sFlow

IPFIX

Protocol Analyzer Output

Chapter Review Activities

Review Key Topics

Define Key Terms

Table of Contents

Review Questions

Chapter 29 Applying Mitigation Techniques or Controls to Secure an Environment

Do I Know This Already? Quiz

Foundation Topics

Reconfigure Endpoint Security Solutions

- Application Approved Lists

- Application Block List/Deny List

- Quarantine

Configuration Changes

- Firewall Rules

- MDM

- Data Loss Prevention

- Content Filter/URL Filter

- Update or Revoke Certificates

Isolation

Containment

Segmentation

SOAR

- Runbooks

- Playbooks

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 30 Understanding the Key Aspects of Digital Forensics

Do I Know This Already? Quiz

Foundation Topics

Documentation/Evidence

- Legal Hold

- Video

Table of Contents

- Admissibility
- Chain of Custody
- Timelines of Sequence of Events
- Timestamps
- Time Offset
- Tags
- Reports
- Event Logs
- Interviews

Acquisition

- Order of Volatility
- Disk
- Random-Access Memory
- Swap/Pagefile
- Operating System
- Device
- Firmware
- Snapshot
- Cache
- Network
- Artifacts

On-premises vs. Cloud

- Right-to-Audit Clauses
- Regulatory/Jurisdiction
- Data Breach Notification Laws

Integrity

- Hashing
- Checksums
- Provenance

Preservation

E-discovery

Data Recovery

Nonrepudiation

Table of Contents

Strategic Intelligence/Counterintelligence

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Part V: Governance, Risk, and Compliance

Chapter 31 Comparing and Contrasting the Various Types of Controls

Do I Know This Already? Quiz

Foundation Topics

Control Category

Managerial Controls

Operational Controls

Technical Controls

Summary of Control Categories

Control Types

Preventative Controls

Detective Controls

Corrective Controls

Deterrent Controls

Compensating Controls

Physical Controls

Summary of Control Types

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 32 Understanding the Importance of Applicable Regulations, Standards, or Frameworks That Impact Organizational Security Posture

Do I Know This Already? Quiz

Table of Contents

Foundation Topics

Regulations, Standards, and Legislation

General Data Protection Regulation

National, Territory, or State Laws

Payment Card Industry Data Security Standard (PCI DSS)

Key Frameworks

Benchmarks and Secure Configuration Guides

Security Content Automation Protocol

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 33 Understanding the Importance of Policies to Organizational Security

Do I Know This Already? Quiz

Foundation Topics

Personnel Policies

Privacy Policies

Acceptable Use

Separation of Duties/Job Rotation

Mandatory Vacations

Onboarding and Offboarding

Personnel Security Policies

Diversity of Training Techniques

User Education and Awareness Training

Third-Party Risk Management

Data Concepts

Understanding Classification and Governance

Data Retention

Credential Policies

Organizational Policies

Table of Contents

Change Management and Change Control

Asset Management

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 34 Summarizing Risk Management Processes and Concepts

Do I Know This Already? Quiz

Foundation Topics

Risk Types

Risk Management Strategies

Risk Analysis

Qualitative Risk Assessment

Quantitative Risk Assessment

Disaster Analysis

Business Impact Analysis

Disaster Recovery Planning

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Chapter 35 Understanding Privacy and Sensitive Data Concepts in Relation to Security

Do I Know This Already? Quiz

Foundation Topics

Organizational Consequences of Privacy and Data Breaches

Notifications of Breaches

Data Types and Asset Classification

Personally Identifiable Information and Protected Health Information

PII

Table of Contents

PHI

Privacy Enhancing Technologies

Roles and Responsibilities

Information Lifecycle

Impact Assessment

Terms of Agreement

Privacy Notice

Chapter Review Activities

Review Key Topics

Define Key Terms

Review Questions

Part VI: Final Preparation

Chapter 36 Final Preparation

Hands-on Activities

Suggested Plan for Final Review and Study

Summary

Glossary of Key Terms

A

B

C

D

E

F

G

H

I

J-K

L

Table of Contents

M

N

O

P

Q

R

S

T

U

V

W

X-Z

Appendix A: Answers to the Do I Know This Already?

Quizzes and Review Questions

Appendix B: CompTIA Security+ (SY0-601) Cert Guide Exam

Updates

Index

APPENDIX C: Study Planner