CyberSpoke's CompTIA Security+ SY0-701 Master Cheat Sheet Guide

Exam Objectives & Domains

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 General Security Concepts	12%
2.0 Threats, Vulnerabilities, and Mitigations	22%
3.0 Security Architecture	18%
4.0 Security Operations	28%
5.0 Security Program Management and Oversight	20%

Exam Details

Exam Code	SY0-701
Launch Date	November 7, 2023
Exam Description	The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents
Number of Questions	A maximum of 90 questions

Type of Questions	Multiple-choice and performance-based
Length of Test	90 minutes
Passing Score	750 (on a scale of 100-900)
Recommended Experience	CompTIA Network+ and two years of experience working in a security/ systems administrator job role
Languages	English, with Japanese, Portuguese and Spanish to follow
Retirement	TBD – Usually three years after launch
DoD 8140 Approved Work Roles	To view approved work roles click here. For more information on 8140, click here.
Testing Provider	Pearson VUE • Testing Centers • Online Testing
Price	View price in cart (See all pricing)

Resource List

Study Guide	This Document
Practice Tests	CompTIA Security+ SY-701 Practice T...
Acronyms	CompTIA Security+ SY0-701 Acronyms
Pocket Prep Practice Questions/Tests	Mobile Test Prep App
CompTIA Provided Practice Tests	Practice Tests
Practice Exams (Jason Dion)(Paid)	Jason Dion Practice Tests
Professor Messer Security+ Training	Professor Messer Videos
Stationx: CompTIA PBQ (Performance-Based Questions)	PBQ Help
Youtube PBQ Help	PBQ Youtube Videos

1.0 General Security Concepts

1.1 Compare and contrast various types of security controls.

Categories

1. Technical
2. Managerial
3. Operational
4. Physical

Control Types

1. Preventive
2. Deterrent
3. Detective
4. Corrective
5. Compensating
6. Directive

1.2 Summarize fundamental security concepts.

Core Security Concepts

- Confidentiality, Integrity, and Availability (CIA)
- Non-repudiation

Access Control & Identity Management

- Authentication, Authorization, and Accounting (AAA)
    - Authenticating people
    - Authenticating systems
    - Authorization models

Security Assessments & Frameworks

- Gap Analysis

Zero Trust Architecture

- Control Plane
    - Adaptive identity
    - Threat scope reduction
    - Policy-driven access control
    - Policy Administrator
    - Policy Engine
- Data Plane
    - Implicit trust zones
    - Subject/System
    - Policy Enforcement Point

Physical Security

- Perimeter & Access Control
    - Bollards
    - Access control vestibule
    - Fencing
- Surveillance & Monitoring
    - Video surveillance
    - Security guard
    - Access badge
    - Lighting
- Detection Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic

Deception & Disruption Technology

- Honeypot
- Honeynet
- Honeyfile
- Honeytoken

1.3 Explain the importance of change management processes and the impact to security.

Business Processes Impacting Security Operations

- Approval process
- Ownership
- Stakeholders
- Impact analysis
- Test results
- Backout plan
- Maintenance window
- Standard operating procedure

Technical Implications

- Allow lists / Deny lists
- Restricted activities
- Downtime
- Service restart
- Application restart
- Legacy applications
- Dependencies

Documentation

- Updating diagrams
- Updating policies/procedures

1.4 Explain the importance of using appropriate cryptographic solutions.

Public Key Infrastructure (PKI)

- Public key
- Private key
- Key escrow

Encryption

- Levels:
    - Full-disk
    - Partition

        - File
        - Volume
        - Database
        - Record
- Transport/Communication Encryption
- Types:
    - Asymmetric
    - Symmetric
- Key Management:
    - Key exchange
    - Algorithms
    - Key length

Encryption Tools

- Trusted Platform Module (TPM)
- Hardware Security Module (HSM)
- Key Management System
- Secure Enclave

Obfuscation

- Steganography
- Tokenization
- Data masking

Cryptographic Concepts

- Hashing
- Salting
- Digital signatures
- Key stretching
- Blockchain
- Open public ledger

Certificates & Trust Models

- Certificate Authorities (CAs)
- Certificate Revocation & Validation:
    - Certificate Revocation Lists (CRLs)
    - Online Certificate Status Protocol (OCSP)

- Types of Certificates:
    - Self-signed
    - Third-party
    - Root of trust
    - Wildcard
- Certificate Management:
    - Certificate Signing Request (CSR) generation

2.0 Threats, Vulnerabilities, and Mitigations

2.1 Compare and contrast common threat actors and motivations.

Threat Actors

- Nation-state
- Unskilled attacker
- Hacktivist
- Insider threat
- Organized crime
- Shadow IT

Attributes of Threat Actors

- Internal / External
- Resources / Funding
- Level of sophistication / Capability

Motivations

- Data exfiltration
- Espionage
- Service disruption
- Blackmail
- Financial gain
- Philosophical / Political beliefs

- Ethical
- Revenge
- Disruption / Chaos
- War

2.2 Explain common threat vectors and attack surfaces.

Communication-Based Attack Vectors

- Message-Based
    - Email
    - Short Message Service (SMS)
    - Instant Messaging (IM)
- Image-Based
- File-Based
- Voice Call
- Removable Device

Software & System Vulnerabilities

- Vulnerable Software
    - Client-based vs. Agentless
- Unsupported Systems & Applications

Network Security Risks

- Unsecure Networks
    - Wireless
    - Wired
    - Bluetooth
- Open Service Ports
- Default Credentials

Supply Chain Risks

- Third-Party Dependencies
    - Managed Service Providers (MSPs)
    - Vendors

    - Suppliers

Human Vectors & Social Engineering

- Phishing
- Vishing
- Smishing
- Misinformation / Disinformation
- Impersonation
- Business Email Compromise
- Pretexting
- Watering Hole Attack
- Brand Impersonation
- Typosquatting

2.3 Explain various types of vulnerabilities.

Application Security Risks

- Memory Injection
- Buffer Overflow
- Race Conditions
    - Time-of-Check (TOC)
    - Time-of-Use (TOU)
- Malicious Update

Operating System (OS)-Based Vulnerabilities

Web-Based Vulnerabilities

- Structured Query Language Injection (SQLi)
- Cross-Site Scripting (XSS)

Hardware Security Risks

- Firmware
- End-of-Life (EOL)
- Legacy Systems

Virtualization Security Risks

- Virtual Machine (VM) Escape
- Resource Reuse

Cloud-Specific Security Risks

Supply Chain Risks

- Service Provider
- Hardware Provider
- Software Provider

Cryptographic Vulnerabilities

Misconfiguration Risks

Mobile Device Security Risks

- Side Loading
- Jailbreaking

Zero-Day Vulnerabilities

2.4 Given a scenario, analyze indicators of malicious activity.

Malware Attacks

- Ransomware
- Trojan
- Worm
- Spyware
- Bloatware
- Virus
- Keylogger
- Logic Bomb
- Rootkit

Physical Attacks

- Brute Force
- Radio Frequency Identification (RFID) Cloning
- Environmental

Network Attacks

- Distributed Denial-of-Service (DDoS)
    - Amplified
    - Reflected
- Domain Name System (DNS) Attacks
- Wireless Attacks
- On-Path Attacks
- Credential Replay
- Malicious Code Injection

Application Attacks

- Injection
- Buffer Overflow
- Replay
- Privilege Escalation
- Forgery
- Directory Traversal

Cryptographic Attacks

- Downgrade
- Collision
- Birthday Attack

Password Attacks

- Spraying
- Brute Force

Indicators of Attack / Compromise

- Account Lockout
- Concurrent Session Usage
- Blocked Content
- Impossible Travel
- Resource Consumption

- Resource Inaccessibility
- Out-of-Cycle Logging
- Published / Documented Attacks
- Missing Logs

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

Security Controls & Best Practices

Access Control & Segmentation

- Segmentation
- Access Control
    - Access Control List (ACL)
    - Permissions

Application & System Security

- Application Allow List
- Isolation
- Patching
- Encryption
- Monitoring
- Least Privilege
- Configuration Enforcement
- Decommissioning

Hardening Techniques

- Encryption
- Installation of Endpoint Protection
- Host-Based Firewall
- Host-Based Intrusion Prevention System (HIPS)
- Disabling Ports / Protocols
- Default Password Changes
- Removal of Unnecessary Software

3.0 Security Architecture

3.1 Compare and contrast security implications of different architecture models.

Architecture & Infrastructure Concepts

Cloud Infrastructure

- Responsibility Matrix
- Hybrid Considerations
- Third-Party Vendors

Infrastructure as Code (IaC)

Compute & Deployment Models

- Serverless
- Microservices

Network Infrastructure

- Physical Isolation
    - Air-Gapped
- Logical Segmentation
- Software-Defined Networking (SDN)

Deployment Environments

- On-Premises
- Centralized vs. Decentralized

Containerization & Virtualization

- Containerization
- Virtualization

Specialized Systems

- Internet of Things (IoT)

- Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)
- Real-Time Operating System (RTOS)
- Embedded Systems

High Availability Considerations

Key Infrastructure Considerations

- Availability
- Resilience
- Cost
- Responsiveness
- Scalability
- Ease of Deployment
- Risk Transference
- Ease of Recovery
- Patch Availability
- Inability to Patch
- Power
- Compute

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

Infrastructure Considerations

Network & Device Security

- Device Placement
- Security Zones
- Attack Surface
- Connectivity

Failure Modes

- Fail-Open

- Fail-Closed

Device Attributes

- Active vs. Passive
- Inline vs. Tap/Monitor

Network Appliances

- Jump Server
- Proxy Server
- Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)
- Load Balancer
- Sensors

Port Security

- 802.1X
- Extensible Authentication Protocol (EAP)

Firewall Types

- Web Application Firewall (WAF)
- Unified Threat Management (UTM)
- Next-Generation Firewall (NGFW)
- Layer 4 / Layer 7 Firewalls

Secure Communication & Access

- Virtual Private Network (VPN)
- Remote Access
- Tunneling Protocols
    - Transport Layer Security (TLS)
    - Internet Protocol Security (IPSec)
- Software-Defined Wide Area Network (SD-WAN)
- Secure Access Service Edge (SASE)

Selection of Effective Controls

3.3 Compare and contrast concepts and strategies to protect data.

Data Security & Management

Data Types

- Regulated
- Trade Secret
- Intellectual Property
- Legal Information
- Financial Information
- Human- and Non-Human Readable

Data Classifications

- Sensitive
- Confidential
- Public
- Restricted
- Private
- Critical

General Data Considerations

- Data States
    - Data at Rest
    - Data in Transit
    - Data in Use
- Data Sovereignty
- Geolocation

Methods to Secure Data

- Geographic Restrictions
- Encryption
- Hashing
- Masking
- Tokenization
- Obfuscation
- Segmentation

- Permission Restrictions

3.4 Explain the importance of resilience and recovery in security architecture.

High Availability & Continuity Planning

High Availability

- Load Balancing vs. Clustering

Site Considerations

- Hot Site
- Cold Site
- Warm Site
- Geographic Dispersion

Platform & Infrastructure

- Platform Diversity
- Multi-Cloud Systems
- Continuity of Operations

Capacity Planning

- People
- Technology
- Infrastructure

Testing Methods

- Tabletop Exercises
- Failover Testing
- Simulation
- Parallel Processing

Backup Strategies

- Onsite / Offsite
- Frequency
- Encryption
- Snapshots
- Recovery
- Replication
- Journaling

Power & Redundancy

- Generators
- Uninterruptible Power Supply (UPS)

4.0 Security Operations

4.1 Given a scenario, apply common security techniques to computing resources.

System Security & Hardening

Secure Baselines

- Establish
- Deploy
- Maintain

Hardening Targets

- Mobile Devices
- Workstations
- Switches
- Routers
- Cloud Infrastructure
- Servers
- ICS/SCADA
- Embedded Systems

- RTOS
- IoT Devices

Wireless Devices

- Installation Considerations
    - Site Surveys
    - Heat Maps

Mobile Solutions

- Mobile Device Management (MDM)
- Deployment Models
    - Bring Your Own Device (BYOD)
    - Corporate-Owned, Personally Enabled (COPE)
    - Choose Your Own Device (CYOD)
- Connection Methods
    - Cellular
    - Wi-Fi
    - Bluetooth

Wireless Security Settings

- Wi-Fi Protected Access 3 (WPA3)
- AAA/Remote Authentication Dial-In User Service (RADIUS)
- Cryptographic Protocols
- Authentication Protocols

Application Security

- Input Validation
- Secure Cookies
- Static Code Analysis
- Code Signing

Additional Security Measures

- Sandboxing
- Monitoring

4.2 Explain the security implications of proper hardware, software, and data asset management.

Asset Management Lifecycle

Acquisition & Procurement

- Acquisition/Procurement Process

Assignment & Accounting

- Ownership
- Classification

Monitoring & Asset Tracking

- Inventory
- Enumeration

Disposal & Decommissioning

- Sanitization
- Destruction
- Certification
- Data Retention

4.3 Explain various activities associated with vulnerability management.

Vulnerability Management

Identification Methods

- Vulnerability Scan
- Application Security
    - Static Analysis

    - Dynamic Analysis
    - Package Monitoring
- Threat Feeds
    - Open-Source Intelligence (OSINT)
    - Proprietary/Third-Party
    - Information-Sharing Organization
    - Dark Web
- Penetration Testing
- Responsible Disclosure Program
    - Bug Bounty Program
- System/Process Audit

Analysis

- Confirmation
    - False Positive
    - False Negative
- Prioritization
- Common Vulnerability Scoring System (CVSS)
- Common Vulnerability Enumeration (CVE)
- Vulnerability Classification
- Exposure Factor
- Environmental Variables
- Industry/Organizational Impact
- Risk Tolerance

Vulnerability Response & Remediation

- Patching
- Insurance
- Segmentation
- Compensating Controls
- Exceptions and Exemptions

Validation of Remediation

- Rescanning
- Audit
- Verification

Reporting

4.4 Explain security alerting and monitoring concepts and tools.

Monitoring & Security Operations

Monitoring Computing Resources

- Systems
- Applications
- Infrastructure

Monitoring Activities

- Log Aggregation
- Alerting
- Scanning
- Reporting
- Archiving
- Alert Response & Remediation/Validation
    - Quarantine
    - Alert Tuning

Monitoring & Security Tools

- Security Content Automation Protocol (SCAP)
- Benchmarks
- Agents/Agentless Monitoring
- Security Information and Event Management (SIEM)
- Antivirus
- Data Loss Prevention (DLP)
- Simple Network Management Protocol (SNMP) Traps
- NetFlow
- Vulnerability Scanners

4.5 Given a scenario, modify enterprise capabilities to enhance security.

Network & Endpoint Security

Firewall Security

- Rules
- Access Lists
- Ports/Protocols
- Screened Subnets

Intrusion Detection/Prevention Systems (IDS/IPS)

- Trend Analysis
- Signature-Based Detection

Web Filtering

- Agent-Based Filtering
- Centralized Proxy
- URL Scanning
- Content Categorization
- Block Rules
- Reputation-Based Filtering

Operating System Security

- Group Policy
- Security-Enhanced Linux (SELinux)

Secure Protocol Implementation

- Protocol Selection
- Port Selection
- Transport Method

Additional Network & Endpoint Security Controls

- DNS Filtering
- Email Security

    - DMARC (Domain-based Message Authentication Reporting & Conformance)
    - DKIM (DomainKeys Identified Mail)
    - SPF (Sender Policy Framework)
    - Secure Email Gateway
- File Integrity Monitoring (FIM)
- Data Loss Prevention (DLP)
- Network Access Control (NAC)
- Endpoint Detection & Response (EDR) / Extended Detection & Response (XDR)
- User Behavior Analytics (UBA)

4.6 Given a scenario, implement and maintain identity and access management.

Identity & Access Management (IAM)

User Account Lifecycle Management

- Provisioning & De-provisioning
- Permission Assignments & Implications
- Identity Proofing

Federation & Single Sign-On (SSO)

- Lightweight Directory Access Protocol (LDAP)
- Open Authorization (OAuth)
- Security Assertions Markup Language (SAML)
- Interoperability & Attestation

Access Controls

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-Based Access Control (RBAC)
- Rule-Based Access Control
- Attribute-Based Access Control (ABAC)
- Time-of-Day Restrictions
- Least Privilege Principle

Multifactor Authentication (MFA)

Implementations:

- Biometrics (Fingerprint, Face Recognition)
- Hard/Soft Authentication Tokens
- Security Keys

Authentication Factors:

- Something You Know (Password, PIN)
- Something You Have (Smart Card, Token)
- Something You Are (Biometric Data)
- Somewhere You Are (Geo-Location)

Password Security & Management

- Best Practices:
    - Length & Complexity
    - Avoiding Reuse
    - Expiration & Age Policies
- Password Managers
- Passwordless Authentication

Privileged Access Management (PAM)

- Just-in-Time (JIT) Permissions
- Password Vaulting
- Ephemeral Credentials

4.7 Explain the importance of automation and orchestration related to secure operations

Automation & Scripting

Use Cases

- User & Resource Provisioning – Automating account creation, access management, and resource allocation.
- Security & Compliance – Implementing guardrails, security group enforcement, and continuous security testing.
- Incident Response – Automating ticket creation, escalation, and service enabling/disabling.
- DevSecOps – Integrating security into CI/CD pipelines and enforcing standardized configurations.

Benefits

- Efficiency & Time Savings
- Enforced Baselines & Security
- Scalability
- Faster Incident Response
- Workforce Optimization

Considerations

- Complexity & Maintenance
- Cost & Resource Allocation
- Single Points of Failure (SPOF)
- Technical Debt & Ongoing Support

4.8 Explain appropriate incident response activities.

Incident Response & Digital Forensics

Incident Response Process

1. Preparation – Policies, tools, and training readiness.
2. Detection – Identifying security incidents.
3. Analysis – Assessing impact and scope.
4. Containment – Isolating affected systems.
5. Eradication – Removing threats.
6. Recovery – Restoring normal operations.
7. Lessons Learned – Reviewing and improving response strategies.

Training & Testing

- Tabletop Exercises – Discussion-based scenario planning.
- Simulations – Hands-on testing of response capabilities.

Root Cause Analysis

- Identifying weaknesses and vulnerabilities that led to the incident.

Threat Hunting

- Proactively searching for hidden threats within an environment.

Digital Forensics

- Legal Hold & Chain of Custody – Preserving evidence integrity.
- Acquisition & Preservation – Collecting and securing data.
- Analysis & Reporting – Investigating and documenting findings.
- E-Discovery – Retrieving electronic evidence for legal use.

4.9 Given a scenario, use data sources to support an investigation.

Log Data & Data Sources

Log Data Types

- Firewall Logs – Tracks inbound/outbound traffic, blocked requests.
- Application Logs – Records app activity, errors, and authentication events.
- Endpoint Logs – Captures activity from user devices.
- OS Security Logs – System-level security events (e.g., Windows Event Logs, Linux syslog).
- IPS/IDS Logs – Intrusion detection/prevention alerts.
- Network Logs – Captures traffic patterns, connections, and anomalies.
- Metadata – Additional context for log correlation and analysis.

Data Sources

- Vulnerability Scans – Identifies weaknesses in systems and applications.

- Automated Reports – Security insights generated from log analysis tools.
- Dashboards – Real-time visualization of security events.
- Packet Captures – Detailed network traffic analysis for threat detection.

5.0 Security Program Management and Oversight

5.1 Summarize elements of effective security governance.

Governance, Policies, and Compliance

Guidelines & Policies

- Acceptable Use Policy (AUP) – Defines proper use of company resources.
- Information Security Policies – Outlines security best practices and expectations.
- Business Continuity & Disaster Recovery – Ensures operational resilience during disruptions.
- Incident Response – Framework for responding to security incidents.
- Software Development Lifecycle (SDLC) – Secure development and deployment standards.
- Change Management – Processes for handling system modifications.

Standards

- Password Management – Enforces complexity, rotation, and storage guidelines.
- Access Control – Defines authentication and authorization mechanisms.
- Physical Security – Establishes perimeter and asset protection measures.
- Encryption Standards – Ensures data confidentiality through encryption protocols.

Procedures

- Change Management – Steps for approving and implementing system changes.
- Onboarding/Offboarding – Managing user access during hiring and termination.
- Playbooks – Defined actions for responding to specific security scenarios.

External Considerations

- Regulatory & Legal – Compliance with industry and governmental regulations.
- Industry Standards – Adherence to frameworks like NIST, ISO 27001, and CIS.
- Local/National/Global Compliance – Ensures alignment with jurisdictional laws.

Monitoring & Governance Structures

- Boards & Committees – Oversee security policies and risk management.
- Government Entities – Regulatory bodies enforcing compliance.
- Centralized vs. Decentralized Models – Defines security control distribution.

Roles & Responsibilities

- Owners – Accountable for data and system security.
- Controllers – Manage data processing activities.
- Processors – Handle data based on controller instructions.
- Custodians/Stewards – Maintain and protect data integrity.

5.2 Explain elements of the risk management process.

Risk Management & Business Impact Analysis

Risk Identification & Assessment

- Risk Identification – Recognizing potential threats and vulnerabilities.
- Risk Assessment Types
    - *Ad hoc* – Performed as needed.
    - *Recurring* – Scheduled assessments at regular intervals.
    - *One-time* – Conducted for specific projects or events.
    - *Continuous* – Ongoing evaluation for real-time risk monitoring.

Risk Analysis

- Qualitative Analysis – Subjective evaluation of risk impact and likelihood.
- Quantitative Analysis – Data-driven assessment using metrics.
    - *Single Loss Expectancy (SLE)* – Expected monetary loss per incident.
    - *Annualized Loss Expectancy (ALE)* – Projected yearly financial loss.

    - *Annualized Rate of Occurrence (ARO)* – Estimated frequency of an event.
    - *Probability & Likelihood* – Measurement of risk occurrence chances.
    - *Exposure Factor* – Percentage of asset loss due to a risk event.
    - *Impact* – Consequences of a realized risk.

Risk Register

- Key Risk Indicators (KRIs) – Metrics for tracking emerging risks.
- Risk Owners – Individuals accountable for specific risks.
- Risk Threshold – Acceptable level of risk before action is required.

Risk Tolerance & Appetite

- Risk Tolerance – Organization's capacity to handle risk.
- Risk Appetite – Strategic approach to risk-taking:
    - *Expansionary* – Willing to take more risks for growth.
    - *Conservative* – Prefers minimal risk exposure.
    - *Neutral* – Balanced approach between risk-taking and caution.

Risk Management Strategies

- Transfer – Shifting risk to third parties (e.g., insurance).
- Accept – Acknowledging and tolerating risk.
    - *Exemption* – Officially approved risk deviation.
    - *Exception* – Temporary risk acceptance.
- Avoid – Eliminating risk by discontinuing risky activities.
- Mitigate – Reducing risk through controls and safeguards.

Risk Reporting

- Documenting and communicating risk findings to stakeholders.

Business Impact Analysis (BIA)

- Recovery Time Objective (RTO) – Maximum time to restore services.
- Recovery Point Objective (RPO) – Maximum data loss acceptable.
- Mean Time to Repair (MTTR) – Average time to fix a failure.
- Mean Time Between Failures (MTBF) – Average uptime between failures.

5.3 Explain the processes associated with third-party risk assessment and management.

Vendor Assessment

- Penetration Testing – Evaluating vendor security posture through ethical hacking.
- Right-to-Audit Clause – Contractual right to assess vendor security controls.
- Evidence of Internal Audits – Reviewing vendor self-assessments and reports.
- Independent Assessments – Third-party security evaluations (e.g., SOC 2, ISO 27001).
- Supply Chain Analysis – Assessing risks in vendor dependencies and partnerships.

Vendor Selection

- Due Diligence – Verifying vendor credibility, compliance, and security posture.
- Conflict of Interest – Ensuring no unethical or biased selection process.

Agreement Types

- Service-Level Agreement (SLA) – Defines performance expectations and penalties.
- Memorandum of Agreement (MOA) – Legally binding contract outlining responsibilities.
- Memorandum of Understanding (MOU) – Non-binding agreement on mutual goals.
- Master Service Agreement (MSA) – Governs overall vendor relationship terms.
- Work Order (WO) / Statement of Work (SOW) – Defines specific deliverables and scope.
- Non-Disclosure Agreement (NDA) – Protects sensitive data shared between parties.
- Business Partners Agreement (BPA) – Outlines responsibilities between business entities.

Vendor Monitoring

- Continuous evaluation of vendor compliance, security, and performance.

Questionnaires

- Standardized vendor security and compliance assessment forms.

Rules of Engagement

- Defines boundaries and methodologies for vendor security assessments.

5.4 Summarize elements of effective security compliance.

Compliance & Privacy Management

Compliance Reporting

- Internal – Regular audits, reports, and security assessments within the organization.
- External – Compliance reports for regulatory bodies, third-party auditors, and stakeholders.

Consequences of Non-Compliance

- Fines – Monetary penalties for failing to meet regulatory standards.
- Sanctions – Restrictions on business operations imposed by authorities.
- Reputational Damage – Loss of customer trust and brand credibility.
- Loss of License – Revocation of certifications, permits, or business licenses.
- Contractual Impacts – Termination of vendor agreements or loss of partnerships.

Compliance Monitoring

- Due Diligence/Care – Ensuring security and regulatory requirements are met.
- Attestation & Acknowledgment – Formal confirmation of compliance adherence.
- Internal & External Audits – Ongoing assessments to maintain regulatory alignment.
- Automation – Using tools and platforms for continuous compliance tracking.

Privacy Considerations

- Legal Implications
    - Local/Regional – Compliance with state or municipal regulations.
    - National – Adhering to country-specific data protection laws.
    - Global – Meeting international privacy frameworks (e.g., GDPR, CCPA).

- Data Subject – Individuals whose personal data is collected and processed.
- Controller vs. Processor
    - Controller – Entity that determines the purpose and means of processing personal data.
    - Processor – Entity that processes data on behalf of the controller.
- Ownership – Defining responsibility over data and accountability for protection.
- Data Inventory & Retention – Maintaining records of data collected and stored.
- Right to Be Forgotten – Compliance with requests to delete personal data.

5.5 Explain types and purposes of audits and assessments.

Attestation & Security Assessments

Attestation

- Formal verification that security controls, compliance requirements, and policies are being met.

Internal Assessments

- Compliance – Ensuring internal security controls align with industry standards and regulations.
- Audit Committee – Dedicated group responsible for overseeing compliance and security audits.
- Self-Assessments – Internal evaluations of security policies, procedures, and risks.

External Assessments

- Regulatory – Assessments conducted by government agencies or industry regulators.
- Examinations – Formal inspections to verify adherence to security and compliance frameworks.
- Independent Third-Party Audit – External auditors assessing security controls, risk management, and compliance.

Penetration Testing

- Physical – Testing access to physical security controls (e.g., doors, locks, badges).
- Offensive – Actively simulating cyberattacks to identify vulnerabilities.
- Defensive – Assessing security posture by defending against simulated attacks.
- Integrated – Combining offensive and defensive testing strategies.

Testing Environments

- Known Environment – Testers have full knowledge of the system and security controls.
- Partially Known Environment – Limited information is provided to testers.
- Unknown Environment – No prior knowledge; simulates a real-world attack scenario.

Reconnaissance (Information Gathering)

- Passive – Collecting publicly available data without directly interacting with the target.
- Active – Engaging with the target system to gather information (e.g., scanning, probing).

5.6 Given a scenario, implement security awareness practices.

Security Awareness & Training

Phishing Awareness

- Campaigns – Simulated phishing exercises to test and educate users.
- Recognizing Phishing Attempts – Identifying suspicious emails, links, attachments, and requests.
- Responding to Phishing – Reporting suspicious messages and following organizational response procedures.

Anomalous Behavior Recognition

- Risky Behavior – Actions that increase exposure to threats (e.g., sharing credentials).
- Unexpected Behavior – Deviations from normal usage patterns.

- Unintentional Behavior – Accidental security risks (e.g., misconfigurations, accidental data sharing).

User Guidance & Training

- Policies & Handbooks – Clearly documented security policies and best practices.
- Situational Awareness – Educating employees on potential threats in their work environment.
- Insider Threat Awareness – Recognizing risks posed by internal personnel.
- Password Management – Encouraging strong, unique passwords and use of password managers.
- Removable Media & Cables – Safe handling of USB drives and external storage devices.
- Social Engineering – Training on manipulation tactics used to extract sensitive information.
- Operational Security (OPSEC) – Protecting sensitive information from inadvertent disclosure.
- Hybrid/Remote Work Security – Securing home networks, VPN use, and safe remote access practices.

Reporting & Monitoring

- Initial Reporting – Procedures for users to report security incidents or anomalies.
- Recurring Monitoring – Continuous assessment of user behavior and security risks.

Training Program Development & Execution

- Development – Creating tailored security awareness programs based on organizational needs.
- Execution – Implementing training sessions, workshops, and simulated attack scenarios.

CompTIA Security+ SY0-701 Acronym List

The following is a list of acronyms that appears on the CompTIA Security+ SY0-701 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

CompTIA Security+ SY0-701 Acronyms

Hardware & Software List

Equipment

- Tablet
- Laptop
- Web server
- Firewall
- Router
- Switch
- IDS
- IPS
- Wireless access point
- Virtual machines
- Email system
- Internet access
- DNS server
- IoT devices
- Hardware tokens
- Smartphone

Spare Hardware

- NICs
- Power supplies
- GBICs
- SFPs
- Managed Switch
- Wireless access point
- UPS

Tools

- Wi-Fi analyzer
- Network mapper

- NetFlow analyzer

Software

- Windows OS
- Linux OS
- Kali Linux
- Packet capture software
- Pen testing software
- Static and dynamic analysis tools
- Vulnerability scanner
- Network emulators
- Sample code
- Code editor
- SIEM
- Keyloggers
- MDM software
- VPN
- DHCP service
- DNS service

Other

- Access to cloud environments
- Sample network documentation/diagrams
- Sample logs