CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-601

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Security+ (SY0-601) certification exam. 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**

This is equivalent to two years of hands-on experience working in a security/systems administrator job role.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at **examsecurity@comptia.org** to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on testing exam objectives. Please know that all related exam preparation materials will still be valid.

CompTIA.

TEST DETAILS

Required exam	SY0-601
Number of questions	Maximum of 90
Types of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	• At least 2 years of work experience in IT systems administration with a focus on security
	• Hands-on technical information security experience
	• Broad knowledge of security concepts
Passing score	750 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination
and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%
Total	**100%**

CompTIA.

1.0 Threats, Attacks, and Vulnerabilities

1.1 Compare and contrast different types of social engineering techniques.

- **Phishing**
- **Smishing**
- **Vishing**
- **Spam**
- **Spam over Internet messaging (SPIM)**
- **Spear phishing**
- **Dumpster diving**
- **Shoulder surfing**
- **Pharming**
- **Tailgating**
- **Eliciting information**
- **Whaling**

- **Prepending**
- **Identity fraud**
- **Invoice scams**
- **Credential harvesting**
- **Reconnaissance**
- **Hoax**
- **Impersonation**
- **Watering hole attack**
- **Typo squatting**
- **Pretexting**
- **Influence campaigns**
    - Hybrid warfare

    - Social media
- **Principles (reasons for effectiveness)**
    - Authority
    - Intimidation
    - Consensus
    - Scarcity
    - Familiarity
    - Trust
    - Urgency

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

- **Malware**
    - Ransomware
    - Trojans
    - Worms
    - Potentially unwanted programs (PUPs)
    - Fileless virus
    - Command and control
    - Bots
    - Cryptomalware
    - Logic bombs
    - Spyware
    - Keyloggers
    - Remote access Trojan (RAT)
    - Rootkit
    - Backdoor

- **Password attacks**
    - Spraying
    - Dictionary
    - Brute force
        - Offline
        - Online
    - Rainbow tables
    - Plaintext/unencrypted
- **Physical attacks**
    - Malicious universal serial bus (USB) cable
    - Malicious flash drive
    - Card cloning
    - Skimming

- **Adversarial artificial intelligence (AI)**
    - Tainted training data for machine learning (ML)
    - Security of machine learning algorithms
- **Supply-chain attacks**
- **Cloud-based vs. on-premises attacks**
- **Cryptographic attacks**
    - Birthday
    - Collision
    - Downgrade

CompTIA.

1.3 Given a scenario, analyze potential indicators associated with application attacks.

- **Privilege escalation**
- **Cross-site scripting**
- **Injections**
  - Structured query language (SQL)
  - Dynamic link library (DLL)
  - Lightweight directory access protocol (LDAP)
  - Extensible markup language (XML)
- **Pointer/object dereference**
- **Directory traversal**
- **Buffer overflows**

- **Race conditions**
  - Time of check/time of use
- **Error handling**
- **Improper input handling**
- **Replay attack**
  - Session replays
- **Integer overflow**
- **Request forgeries**
  - Server-side
  - Client-side
  - Cross-site

- **Application programming interface (API) attacks**
- **Resource exhaustion**
- **Memory leak**
- **Secure sockets layer (SSL) stripping**
- **Driver manipulation**
  - Shimming
  - Refactoring
- **Pass the hash**

1.4 Given a scenario, analyze potential indicators associated with network attacks.

- **Wireless**
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disassociation
  - Jamming
  - Radio frequency identifier (RFID)
  - Near-field communication (NFC)
  - Initialization vector (IV)
- **Man-in-the-middle**

- **Man-in-the-browser**
- **Layer 2 attacks**
  - Address resolution protocol (ARP) poisoning
  - Media access control (MAC) flooding
  - MAC cloning
- **Domain name system (DNS)**
  - Domain hijacking
  - DNS poisoning
  - Universal resource locator (URL) redirection

  - Domain reputation
- **Distributed denial-of-service (DDoS)**
  - Network
  - Application
  - Operational technology (OT)
- **Malicious code or script execution**
  - PowerShell
  - Python
  - Bash
  - Macros
  - Virtual Basic for Applications (VBA)

CompTIA.

1.5 Explain different threat actors, vectors, and intelligence sources.

- **Actors and threats**
  - Advanced persistent threat (APT)
  - Insider threats
  - State actors
  - Hacktivists
  - Script kiddies
  - Criminal syndicates
  - Hackers
    - White hat
    - Black hat
    - Gray hat
  - Shadow IT
  - Competitors
- **Attributes of actors**
  - Internal/external
  - Level of sophistication/capability
  - Resources/funding
  - Intent/motivation

- **Vectors**
  - Direct access
  - Wireless
  - Email
  - Supply chain
  - Social media
  - Removable media
  - Cloud
- **Threat intelligence sources**
  - Open source intelligence (OSINT)
  - Closed/proprietary
  - Vulnerability databases
  - Public/private information-sharing centers
  - Dark web
  - Indicators of compromise

- Automated indicator sharing (AIS)
  - Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII)
- Predictive analysis
- Threat maps
- File/code repositories
- **Research sources**
  - Vendor websites
  - Vulnerability feeds
  - Conferences
  - Academic journals
  - Request for comments (RFC)
  - Local industry groups
  - Social media
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTP)

1.6 Explain the security concerns associated with various types of vulnerabilities.

- **Cloud-based vs. on-premises vulnerabilities**
- **Zero-day**
- **Weak configurations**
  - Open permissions
  - Unsecure root accounts
  - Errors
  - Weak encryption
  - Unsecure protocols
  - Default settings
  - Open ports and services

- **Third-party risks**
  - Vendor management
    - System integration
    - Lack of vendor support
  - Supply chain
  - Outsourced code development
  - Data storage
- **Improper or weak patch management**
  - Firmware
  - Operating system (OS)
  - Applications

- **Legacy platforms**
- **Impacts**
  - Data loss
  - Data breaches
  - Data exfiltration
  - Identity theft
  - Financial
  - Reputation
  - Availability loss

CompTIA

1.7 Summarize the techniques used in security assessments.

- **Threat hunting**
  - Intelligence fusion
  - Threat feeds
  - Advisories and bulletins
  - Maneuver
- **Vulnerability scans**
  - False positives
  - False negatives
  - Log reviews
  - Credentialed vs. non-credentialed
  - Intrusive vs. non-intrusive
  - Application
  - Web application
  - Network
  - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)
  - Configuration review

- **Syslog/Security information and event management (SIEM)**
  - Review reports
  - Packet capture
  - Data inputs
  - User behavior analysis
  - Sentiment analysis
  - Security monitoring
  - Log aggregation
  - Log collectors
- **Security orchestration, automation, and response (SOAR)**

1.8 Explain the techniques used in penetration testing.

- **Penetration testing**
  - White-box
  - Black-box
  - Gray-box
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting

- **Passive and active reconnaissance**
  - Drones/unmanned aerial vehicle (UAV)
  - War flying
  - War driving
  - Footprinting
  - OSINT
- **Exercise types**
  - Red-team
  - Blue-team
  - White-team
  - Purple-team

CompTIA.

2.0 Architecture and Design

2.1 Explain the importance of security concepts in an enterprise environment.

- **Configuration management**
  - Diagrams
  - Baseline configuration
  - Standard naming conventions
  - Internet protocol (IP) schema
- **Data sovereignty**
- **Data protection**
  - Data loss prevention (DLP)
  - Masking
  - Encryption
  - At rest
  - In transit/motion
  - In processing
  - Tokenization
  - Rights management

- **Hardware security module (HSM)**
- **Geographical considerations**
- **Cloud access security broker (CASB)**
- **Response and recovery controls**
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection**
- **Hashing**
- **API considerations**
- **Site resiliency**
  - Hot site
  - Cold site
  - Warm site

- **Deception and disruption**
  - Honeypots
  - Honeyfiles
  - Honeynets
  - Fake telemetry
  - DNS sinkhole

2.2 Summarize virtualization and cloud computing concepts.

- **Cloud models**
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
  - Anything as a service (XaaS)
  - Public
  - Community
  - Private
  - Hybrid
- **Cloud service providers**

- **Managed service provider (MSP)/ managed security service provider (MSSP)**
- **On-premises vs. off-premises**
- **Fog computing**
- **Edge computing**
- **Thin client**
- **Containers**
- **Microservices/API**

- **Infrastructure as code**
  - Software-defined networking (SDN)
  - Software-defined visibility (SDV)
- **Serverless architecture**
- **Services integration**
- **Resource policies**
- **Transit gateway**
- **Virtualization**
  - Virtual machine (VM) sprawl avoidance
  - VM escape protection

CompTIA.

2.3 Summarize secure application development, deployment, and automation concepts.

- **Environment**
  - Development
  - Test
  - Staging
  - Production
  - Quality assurance (QA)
- **Provisioning and deprovisioning**
- **Integrity measurement**
- **Secure coding techniques**
  - Normalization
  - Stored procedures
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and software development kits (SDKs)
  - Data exposure
- **Open Web Application Security Project (OWASP)**
- **Software diversity**
  - Compiler
  - Binary
- **Automation/scripting**
  - Automated courses of action
  - Continuous monitoring
  - Continuous validation
  - Continuous integration
  - Continuous delivery
  - Continuous deployment
- **Elasticity**
- **Scalability**
- **Version control**

2.4 Summarize authentication and authorization design concepts.

- **Authentication methods**
  - Directory services
  - Federation
  - Attestation
  - 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
  - Smart card authentication
- **Biometrics**
  - Fingerprint
  - Retina
  - Iris
  - Facial
  - Voice
  - Vein
  - Gait analysis
  - Efficacy rates
  - False acceptance
  - False rejection
  - Crossover error rate
- **Multifactor authentication (MFA) factors and attributes**
  - 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)**
- **Cloud vs. on-premises requirements**

CompTIA.

2.5 Given a scenario, implement cybersecurity resilience.

- **Redundancy**
  - Geographic dispersal
  - Disk
    - Redundant array of inexpensive disks (RAID) levels
    - Multipath
  - Network
    - Load balancers
    - Network interface card (NIC) teaming
  - Power
    - Uninterruptible power supply (UPS)
    - Generator
    - Dual supply
    - Managed power distribution units (PDUs)

- **Replication**
  - Storage area network
  - VM
- **On-premises vs. cloud**
- **Backup types**
  - Full
  - Incremental
  - Snapshot
  - Differential
  - Tape
  - Disk
  - Copy
  - Network-attached storage (NAS)
  - Storage area network
  - Cloud
  - Image
  - Online vs. offline

  - Offsite storage
    - Distance considerations
- **Non-persistence**
  - Revert to known state
  - Last known-good configuration
  - Live boot media
- **High availability**
  - Scalability
- **Restoration order**
- **Diversity**
  - Technologies
  - Vendors
  - Crypto
  - Controls

2.6 Explain the security implications of embedded and specialized systems.

- **Embedded systems**
  - Raspberry Pi
  - Field-programmable gate array (FPGA)
  - Arduino
- **Supervisory control and data acquisition (SCADA)/industrial control system (ICS)**
  - Facilities
  - Industrial
  - Manufacturing
  - Energy
  - Logistics
- **Internet of Things (IoT)**
  - Sensors
  - Smart devices
  - Wearables
  - Facility automation
  - Weak defaults

- **Specialized**
  - Medical systems
  - Vehicles
  - Aircraft
  - Smart meters
- **Voice over IP (VoIP)**
- **Heating, ventilation, air conditioning (HVAC)**
- **Drones/AVs**
- **Multifunction printer (MFP)**
- **Real-time operating system (RTOS)**
- **Surveillance systems**
- **System on chip (SoC)**
- **Communication considerations**
  - 5G
  - Narrow-band
  - Baseband radio

  - Subscriber identity module (SIM) cards
  - Zigbee
- **Constraints**
  - Power
  - Compute
  - Network
  - Crypto
  - Inability to patch
  - Authentication
  - Range
  - Cost
  - Implied trust

2.7 Explain the importance of physical security controls.

- **Bollards/barricades**
- **Mantraps**
- **Badges**
- **Alarms**
- **Signage**
- **Cameras**
  - Motion recognition
  - Object detection
- **Closed-circuit television (CCTV)**
- **Industrial camouflage**
- **Personnel**
  - Guards
  - Robot sentries
  - Reception
  - Two-person integrity/control
- **Locks**
  - Biometrics

- Electronic
- Physical
- Cable locks
- **USB data blocker**
- **Lighting**
- **Fencing**
- **Fire suppression**
- **Sensors**
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards
  - Temperature
- **Drones/UAV**
- **Visitor logs**
- **Faraday cages**

- **Air gap**
- **Demilitarized zone (DMZ)**
- **Protected cable distribution**
- **Secure areas**
  - Air gap
  - Vault
  - Safe
  - Hot aisle
  - Cold aisle
- **Secure data destruction**
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Third-party solutions

2.8 Summarize the basics of cryptographic concepts.

- **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**
  - Authenticated
  - Unauthenticated
  - Counter

- **Blockchain**
  - Public ledgers
- **Cipher suites**
  - Stream
  - Block
- **Symmetric vs. asymmetric**
- **Lightweight cryptography**
- **Steganography**
  - Audio
  - Video
  - Image
- **Homomorphic encryption**
- **Common use cases**
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality

- Supporting integrity
- Supporting obfuscation
- Supporting authentication
- Supporting non-repudiation
- Resource vs. security constraints
- **Limitations**
  - Speed
  - Size
  - Weak keys
  - Time
  - Longevity
  - Predictability
  - Reuse
  - Entropy
  - Computational overheads
  - Resource vs. security constraints

3.0 Implementation

3.1 Given a scenario, implement secure protocols.

- **Protocols**
  - Domain Name System Security Extension (DNSSEC)
  - SSH
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-time Protocol (SRTP)
  - Lightweight Directory Access Protocol Over SSL (LDAPS)
  - File Transfer Protocol, Secure (FTPS)
  - SSH File Transfer Protocol (SFTP)
  - Simple Network Management Protocol, version 3 (SNMPv3)
  - Hypertext transfer protocol over SSL/TLS (HTTPS)
  - IPSec
    - Authentication header (AH)/ Encapsulating Security Payloads (ESP)
    - Tunnel/transport
  - Secure Post Office Protocol (POP)/ Internet Message Access Protocol (IMAP)
- **Use cases**
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

3.2 Given a scenario, implement host or application security solutions.

- **Endpoint protection**
  - Antivirus
  - Anti-malware
  - Endpoint detection and response (EDR)
  - DLP
  - Next-generation firewall (NGFW)
  - Host-based intrusion prevention system (HIPS)
  - Host-based intrusion detection system (HIDS)
  - Host-based firewall
- **Boot integrity**
  - Boot security/Unified Extensible Firmware Interface (UEFI)
  - Measured boot
  - Boot attestation
- **Database**
  - Tokenization
  - Salting
  - Hashing
- **Application security**
  - Input validations
  - Secure cookies
  - Hypertext Transfer Protocol (HTTP) headers
  - Code signing
  - Whitelisting
  - Blacklisting
  - Secure coding practices
  - Static code analysis
    - Manual code review
  - Dynamic code analysis
  - Fuzzing
- **Hardening**
  - Open ports and services
  - Registry
  - Disk encryption
  - OS
  - Patch management
    - Third-party updates
    - Auto-update
- **Self-encrypting drive (SED)/ full-disk encryption (FDE)**
  - Opal
- **Hardware root of trust**
- **Trusted Platform Module (TPM)**
- **Sandboxing**

CompTIA.

3.3 Given a scenario, implement secure network designs.

- **Load balancing**
  - Active/active
  - Active/passive
  - Scheduling
  - Virtual IP
  - Persistence
- **Network segmentation**
  - Virtual local area network (VLAN)
  - DMZ
  - East-west traffic
  - Extranet
  - Intranet
  - Zero Trust
- **Virtual private network (VPN)**
  - Always-on
  - Split tunnel vs. full tunnel
  - Remote access vs. site-to-site
  - IPSec
  - SSL/TLS
  - HTML5
  - Layer 2 tunneling protocol (L2TP)
- **DNS**
- **Network access control (NAC)**
  - Agent and agentless

- **Out-of-band management**
- **Port security**
  - Broadcast storm prevention
  - Bridge Protocol Data Unit (BPDU) guard
  - Loop prevention
  - Dynamic Host Configuration Protocol (DHCP) snooping
  - Media access control (MAC) filtering
- **Network appliances**
  - Jump servers
  - Proxy servers
    - Forward
    - Reverse
  - Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS)
    - Signature-based
    - Heuristic/behavior
    - Anomaly
    - Inline vs. passive
  - HSM
  - Sensors

  - Collectors
  - Aggregators
  - Firewalls
    - Web application firewall (WAF)
    - NGFW
    - Stateful
    - Stateless
    - Unified threat management (UTM)
    - Network address translation (NAT) gateway
    - Content/URL filter
    - Open-source vs. proprietary
    - Hardware vs. software
    - Appliance vs. host-based vs. virtual
- **Access control list (ACL)**
- **Route security**
- **Quality of service (QoS)**
- **Implications of IPv6**
- **Port spanning/port mirroring**
  - Port taps
- **Monitoring services**
- **File integrity monitors**

3.4 Given a scenario, install and configure wireless security settings.

- **Cryptographic protocols**
  - WiFi protected access II (WPA2)
  - WiFi protected access III (WPA3)
  - Counter-mode/CBC-MAC protocol (CCMP)
  - Simultaneous Authentication of Equals (SAE)
- **Authentication protocols**
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Application Protocol (PEAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS

  - IEEE 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) Federation
- **Methods**
  - Pre-shared key (PSK) vs. Enterprise vs. Open
  - WiFi Protected Setup (WPS)
  - Captive portals
- **Installation considerations**
  - Site surveys
  - Heat maps
  - WiFi analyzers
  - Channel overlays
  - Wireless access point (WAP) placement

  - Controller and access point security

CompTIA

3.5 Given a scenario, implement secure mobile solutions.

- **Connection methods and receivers**
  - Cellular
  - WiFi
  - Bluetooth
  - NFC
  - Infrared
  - USB
  - Point-to-point
  - Point-to-multipoint
  - Global Positioning System (GPS)
  - RFID
- **Mobile device management (MDM)**
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notifications
  - Passwords and pins

  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption
- **Mobile devices**
  - MicroSD HSM
  - MDM/Unified Endpoint Management (UEM)
  - Mobile application management (MAM)
  - SEAndroid
- **Enforcement and monitoring of:**
  - Third-party application stores
  - Rooting/jailbreaking
  - Sideloading
  - Custom firmware
  - Carrier unlocking
  - Firmware over-the-air (OTA) updates
  - Camera use

  - SMS/Multimedia Messaging Service (MMS)/Rich communication services (RCS)
  - External media
  - USB On-The-Go (USB OTG)
  - Recording microphone
  - GPS tagging
  - WiFi direct/ad hoc
  - Tethering
  - Hotspot
  - Payment methods
- **Deployment models**
  - 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
  - Resource policies
  - Secrets management
  - Integration and auditing
  - 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 (VPC) endpoint
    - Container security

- **Solutions**
  - CASB
  - Application security
  - Next-generation Secure Web Gateway (SWG)
  - Firewall considerations in a cloud environment
    - Cost
    - Need for segmentation
    - Open Systems Interconnection (OSI) layers
- **Cloud native controls vs. third-party solutions**

CompTIA

3.7 Given a scenario, implement identity and account management controls.

- **Identity**
  - Identity provider (IdP)
  - Attributes
  - Certificates
  - Tokens
  - SSH keys
  - Smart cards
- **Account types**
  - User account
  - Shared and generic accounts/credentials

- Guest accounts
- Service accounts
- **Account policies**
  - Password complexity
  - Password history
  - Password reuse
  - Time of day
  - Network location
  - Geofencing
  - Geotagging
  - Geolocation

- Time-based logins
- Access policies
- Account permissions
- Account audits
- Impossible travel time/risky login
- Lockout
- Disablement

3.8 Given a scenario, implement authentication and authorization solutions.

- **Authentication management**
  - Password keys
  - Password vaults
  - TPM
  - HSM
  - Knowledge-based authentication
- **Authentication**
  - EAP
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)

- 802.1X
- RADIUS
- Single sign-on (SSO)
- Security Assertions Markup Language (SAML)
- Terminal Access Controller Access Control System Plus (TACACS+)
- OAuth
- OpenID
- Kerberos
- **Access control schemes**
  - Attribute-based access control (ABAC)

- Role-based access control
- Rule-based access control
- MAC
- Discretionary access control (DAC)
- Conditional access
- Privilege access management
- Filesystem permissions

3.9 Given a scenario, implement public key infrastructure.

- **Public key infrastructure (PKI)**
  - Key management
  - Certificate authority (CA)
  - Intermediate CA
  - Registration authority (RA)
  - Certificate revocation list (CRL)
  - Certificate attributes
  - Online Certificate Status Protocol (OCSP)
  - Certificate signing request (CSR)
  - CN
  - Subject alternative name
  - Expiration

- **Types of certificates**
  - Wildcard
  - Subject alternative name
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User
  - Root
  - Domain validation
  - Extended validation
- **Certificate formats**
  - Distinguished encoding rules (DER)

- Privacy enhanced mail (PEM)
- Personal information exchange (PFX)
- .cer
- P12
- P7B
- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining

CompTIA.

4.0 Operations and Incident Response

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- **Network reconnaissance and discovery**
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - IP scanners
  - arp
  - route
  - curl
  - the harvester
  - sn1per
  - scanless
  - dnsenum
  - Nessus
  - Cuckoo
- **File manipulation**
  - head
  - tail
  - cat
  - grep
  - 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**

4.2 Summarize the importance of policies, processes, and procedures for incident response.

- **Incident response plans**
- **Incident response process**
  - Preparation
  - 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**

CompTIA.

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- **Vulnerability scan output**
- **SIEM dashboards**
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation
- **Log files**
  - Network
  - System
  - Application
    - Security
    - Web
    - DNS
    - Authentication
    - Dump files
    - VoIP and call managers
    - Session Initiation Protocol (SIP) traffic
- **syslog/rsyslog/syslog-ng**
- **journalctl**
- **nxlog**
- **Retention**
- **Bandwidth monitors**
- **Metadata**
  - Email
  - Mobile
  - Web
  - File
- **Netflow/sflow**
  - Echo
  - IPfix
- **Protocol analyzer output**

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- **Reconfigure endpoint security solutions**
  - Application whitelisting
  - Application blacklisting
  - Quarantine
- **Configuration changes**
  - Firewall rules
  - MDM
  - DLP
  - Content filter/URL filter
  - Update or revoke certificates
- **Isolation**
- **Containment**
- **Segmentation**
- **SOAR**
  - Runbooks
  - Playbooks

4.5 Explain the key aspects of digital forensics.

- **Documentation/evidence**
  - Legal hold
  - Video
  - Admissibility
  - Chain of custody
  - Timelines of sequence of events
    - Time stamps
    - Time offset
  - Tags
  - Reports
  - Event logs
  - Interviews
- **Acquisition**
  - Order of volatility
  - Disk
  - Random-access memory (RAM)
  - Swap/pagefile
  - OS
  - 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**
- **Non-repudiation**
- **Strategic intelligence/ counterintelligence**

CompTIA

5.0 Governance, Risk, and Compliance

5.1 Compare and contrast various types of controls.

- **Category**
  - Managerial
  - Operational
  - Technical
- **Control type**
  - Preventative
  - 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**
  - General Data Protection Regulation (GDPR)
  - National, territory, or state laws
  - Payment Card Industry Data Security Standard (PCI DSS)
- **Key frameworks**
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST) RMF/CSF
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance
    - Cloud control matrix
  - Reference architecture
- **Benchmarks /secure configuration guides**
  - Platform/vendor-specific guides
    - Web server
    - OS
    - Application server
    - Network infrastructure devices

5.3 Explain the importance of policies to organizational security.

- **Personnel**
  - Acceptable use policy
  - Job rotation
  - Mandatory vacation
  - Separation of duties
  - Least privilege
  - Clean desk space
  - Background checks
  - Non-disclosure agreement (NDA)
  - Social media analysis
  - Onboarding
  - Offboarding
  - User training
    - Gamification
    - Capture the flag
    - Phishing campaigns
      - Phishing simulations
    - Computer-based training (CBT)
    - Role-based training
- **Diversity of training techniques**
- **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
  - Governance
  - Retention
- **Credential policies**
  - Personnel
  - Third-party
  - Devices
  - Service accounts
  - Administrator/root accounts
- **Organizational policies**
  - Change management
  - Change control
  - Asset management

CompTIA.

5.4 Summarize risk management processes and concepts.

- **Risk types**
  - External
  - Internal
  - Legacy systems
  - Multiparty
  - IP theft
  - Software compliance/licensing
- **Risk management strategies**
  - Acceptance
  - Avoidance
  - Transference
    - Cybersecurity insurance
  - Mitigation
- **Risk analysis**
  - Risk register
  - Risk matrix/heat map
  - Risk control assessment

- Risk control self-assessment
- Risk awareness
- Inherent risk
- Residual risk
- Control risk
- Risk appetite
- Regulations that affect risk posture
- Risk assessment types
  - Qualitative
  - Quantitative
- Likelihood of occurrence
- Impact
- Asset value
- Single loss expectancy (SLE)
- Annualized loss expectancy (ALE)
- Annualized rate of occurrence (ARO)

- **Disasters**
  - Environmental
  - Person-made
  - Internal vs. external
- **Business impact analysis**
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Functional recovery plans
  - Single point of failure
  - Disaster recovery plan (DRP)
  - Mission essential functions
  - Identification of critical systems
  - Site risk assessment

5.5 Explain privacy and sensitive data concepts in relation to security.

- **Organizational consequences of privacy breaches**
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft
- **Notifications of breaches**
  - Escalation
  - Public notifications and disclosures
- **Data types**
  - Classifications
    - Public
    - Private
    - Sensitive
    - Confidential
    - Critical
    - Proprietary

- Personally identifiable information (PII)
- Health information
- Financial information
- Government data
- Customer data
- **Privacy enhancing technologies**
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- **Roles and responsibilities**
  - Data owners
  - Data controller
  - Data processor
  - Data custodian/steward
  - Data protection officer (DPO)

- **Information life cycle**
- **Impact assessment**
- **Terms of agreement**
- **Privacy notice**

CompTIA.

Security+ (SY0-601) Acronym List

The following is a list of acronyms that appear on the CompTIA Security+ 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.

ACRONYM	DEFINITION	ACRONYM	DEFINITION
3DES	Triple Digital Encryption Algorithm	CAR	Corrective Action Report
AAA	Authentication, Authorization, and Accounting	CASB	Cloud Access Security Broker
ABAC	Attribute-based Access Control	CBC	Cipher Block Chaining
ACL	Access Control List	CBT	Computer-based Training
AD	Active Directory	CCMP	Counter-Mode/CBC-MAC Protocol
AES	Advanced Encryption Standard	CCTV	Closed-Circuit Television
AES256	Advanced Encryption Standards 256bit	CERT	Computer Emergency Response Team
AH	Authentication Header	CFB	Cipher Feedback
AI	Artificial Intelligence	CHAP	Challenge-Handshake Authentication Protocol
AIS	Automated Indicator Sharing	CIO	Chief Information Officer
ALE	Annualized Loss Expectancy	CIRT	Computer Incident Response Team
AP	Access Point	CIS	Center for Internet Security
API	Application Programming Interface	CMS	Content Management System
APT	Advanced Persistent Threat	CN	Common Name
ARO	Annualized Rate of Occurrence	COOP	Continuity of Operations Planning
ARP	Address Resolution Protocol	COPE	Corporate-owned Personally Enabled
ASLR	Address Space Layout Randomization	CP	Contingency Planning
ASP	Active Server Pages	CRC	Cyclic Redundancy Check
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	CRL	Certificate Revocation List
		CSA	Cloud Security Alliance
AUP	Acceptable Use Policy	CSIRT	Computer Security Incident Response Team
AV	Antivirus	CSO	Chief Security Officer
BASH	Bourne Again Shell	CSP	Cloud Service Provider
BCP	Business Continuity Planning	CSR	Certificate Signing Request
BGP	Border Gateway Protocol	CSRF	Cross-Site Request Forgery
BIA	Business Impact Analysis	CSU	Channel Service Unit
BIOS	Basic Input/Output System	CTM	Counter-Mode
BPA	Business Partnership Agreement	CTO	Chief Technology Officer
BPDU	Bridge Protocol Data Unit	CVE	Common Vulnerabilities and Exposures
BSSID	Basic Service Set Identifier	CVSS	Common Vulnerability Scoring System
BYOD	Bring Your Own Device	CYOD	Choose Your Own Device
CA	Certificate Authority	DAC	Discretionary Access Control
CAC	Common Access Card	DBA	Database Administrator
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart	DDoS	Distributed Denial-of-Service
		DEP	Data Execution Prevention

CompTIA.

ACRONYM	DEFINITION	ACRONYM	DEFINITION
DER	Distinguished Encoding Rules	HOTP	HMAC-based One-time Password
DES	Data Encryption Standard	HSM	Hardware Security Module
DHCP	Dynamic Host Configuration Protocol	HSMaaS	Hardware Security Module as a Service
DHE	Diffie-Hellman Ephemeral	HTML	Hypertext Markup Language
DKIM	Domain Keys Identified Mail	HTTP	Hypertext Transfer Protocol
DLL	Dynamic Link Library	HTTPS	Hypertext Transfer Protocol Secure
DLP	Data Loss Prevention	HVAC	Heating, Ventilation, Air Conditioning
DMARC	Domain Message Authentication Reporting and Conformance	IaaS	Infrastructure as a Service
DMZ	Demilitarized Zone	IAM	Identity and Access Management
DNAT	Destination Network Address Transaction	ICMP	Internet Control Message Protocol
DNS	Domain Name System	ICS	Industrial Control Systems
DNSSEC	Domain Name System Security Extensions	IDEA	International Data Encryption Algorithm
DoS	Denial-of-Service	IDF	Intermediate Distribution Frame
DPO	Data Protection Officer	IdP	Identity Provider
DRP	Disaster Recovery Plan	IDS	Intrusion Detection System
DSA	Digital Signature Algorithm	IEEE	Institute of Electrical and Electronics Engineers
DSL	Digital Subscriber Line	IKE	Internet Key Exchange
EAP	Extensible Authentication Protocol	IM	Instant Messaging
ECB	Electronic Code Book	IMAP4	Internet Message Access Protocol v4
ECC	Elliptic-curve Cryptography	IoC	Indicators of Compromise
ECDHE	Elliptic-curve Diffie-Hellman Ephemeral	IoT	Internet of Things
ECDSA	Elliptic-curve Digital Signature Algorithm	IP	Internet Protocol
EDR	Endpoint Detection and Response	IPS	Intrusion Prevention System
EFS	Encrypted File System	IPSec	Internet Protocol Security
EIP	Extended Instruction Pointer	IR	Incident Response
EOL	End of Life	IRC	Internet Relay Chat
EOS	End of Service	IRP	Incident Response Plan
ERP	Enterprise Resource Planning	ISA	Interconnection Security Agreement
ESN	Electronic Serial Number	ISFW	Internal Segmentation Firewall
ESP	Encapsulating Security Payload	ISO	International Organization for Standardization
ESSID	Extended Service Set Identifier	ISP	Internet Service Provider
FACL	File System Access Control List	ISSO	Information Systems Security Officer
FDE	Full Disk Encryption	ITCP	IT Contingency Plan
FIM	File Integrity Monitoring	IV	Initialization Vector
FPGA	Field Programmable Gate Array	KDC	Key Distribution Center
FRR	False Rejection Rate	KEK	Key Encryption Key
FTP	File Transfer Protocol	L2TP	Layer 2 Tunneling Protocol
FTPS	Secured File Transfer Protocol	LAN	Local Area Network
GCM	Galois/Counter Mode	LDAP	Lightweight Directory Access Protocol
GDPR	General Data Protection Regulation	LEAP	Lightweight Extensible Authentication Protocol
GPG	GNU Privacy Guard	MaaS	Monitoring as a Service
GPO	Group Policy Object	MAC	Media Access Control
GPS	Global Positioning System	MAM	Mobile Application Management
GPU	Graphics Processing Unit	MAN	Metropolitan Area Network
GRE	Generic Routing Encapsulation	MBR	Master Boot Record
HA	High Availability	MD5	Message Digest 5
HDD	Hard Disk Drive	MDF	Main Distribution Frame
HIDS	Host-based Intrusion Detection System	MDM	Mobile Device Management
HIPS	Host-based Intrusion Prevention System	MFA	Multifactor Authentication
HMAC	Hash-based Message Authentication Code	MFD	Multifunction Device
		MFP	Multifunction Printer

CompTIA.

ACRONYM	DEFINITION	ACRONYM	DEFINITION
MITM	Man-in-the-Middle	PBKDF2	Password-based Key Derivation Function 2
ML	Machine Learning	PBX	Private Branch Exchange
MMS	Multimedia Message Service	PCAP	Packet Capture
MOA	Memorandum of Agreement	PCI DSS	Payment Card Industry Data Security Standard
MOU	Memorandum of Understanding	PDU	Power Distribution Unit
MPLS	Multiprotocol Label Switching	PE	Portable Executable
MSA	Measurement Systems Analysis	PEAP	Protected Extensible Authentication Protocol
MSCHAP	Microsoft Challenge Handshake Authentication Protocol	PED	Portable Electronic Device
		PEM	Privacy Enhanced Mail
MSP	Managed Service Provider	PFS	Perfect Forward Secrecy
MSSP	Managed Security Service Provider	PGP	Pretty Good Privacy
MTBF	Mean Time Between Failures	PHI	Personal Health Information
MTTF	Mean Time to Failure	PII	Personally Identifiable Information
MTTR	Mean Time to Repair	PIN	Personal Identification Number
MTU	Maximum Transmission Unit	PIV	Personal Identity Verification
NAC	Network Access Control	PKCS	Public Key Cryptography Standards
NAS	Network-attached Storage	PKI	Public Key Infrastructure
NAT	Network Address Translation	PoC	Proof of Concept
NDA	Non-disclosure Agreement	POP	Post Office Protocol
NFC	Near-field Communication	POTS	Plain Old Telephone Service
NFV	Network Function Virtualization	PPP	Point-to-Point Protocol
NGFW	Next-generation Firewall	PPTP	Point-to-Point Tunneling Protocol
NG-SWG	Next-generation Secure Web Gateway	PSK	Pre-shared Key
NIC	Network Interface Card	PTZ	Pan-Tilt-Zoom
NIDS	Network-based Intrusion Detection System	PUP	Potentially Unwanted Program
NIPS	Network-based Intrusion Prevention System	QA	Quality Assurance
NIST	National Institute of Standards & Technology	QoS	Quality of Service
NOC	Network Operations Center	PUP	Potentially Unwanted Program
NTFS	New Technology File System	RA	Registration Authority
NTLM	New Technology LAN Manager	RAD	Rapid Application Development
NTP	Network Time Protocol	RADIUS	Remote Authentication Dial-in User Service
OAUTH	Open Authentication	RAID	Redundant Array of Inexpensive Disks
OCSP	Online Certificate Status Protocol	RAM	Random Access Memory
OID	Object Identifier	RAS	Remote Access Server
OS	Operating System	RAT	Remote Access Trojan
OSI	Open Systems Interconnection	RC4	Rivest Cipher version 4
OSINT	Open-source Intelligence	RCS	Rich Communication Services
OSPF	Open Shortest Path First	RFC	Request for Comments
OT	Operational Technology	RFID	Radio Frequency Identifier
OTA	Over-The-Air	RIPEMD	RACE Integrity Primitives Evaluation Message Digest
OTG	On-The-Go		
OVAL	Open Vulnerability and Assessment Language	ROI	Return on Investment
OWASP	Open Web Application Security Project	RPO	Recovery Point Objective
P12	PKCS #12	RSA	Rivest, Shamir, & Adleman
P2P	Peer-to-Peer	RTBH	Remotely Triggered Black Hole
PaaS	Platform as a Service	RTO	Recovery Time Objective
PAC	Proxy Auto Configuration	RTOS	Real-time Operating System
PAM	Privileged Access Management	RTP	Real-time Transport Protocol
PAM	Pluggable Authentication Modules	S/MIME	Secure/Multipurpose Internet Mail Extensions
PAP	Password Authentication Protocol	SaaS	Software as a Service
PAT	Port Address Translation	SAE	Simultaneous Authentication of Equals

CompTIA.

ACRONYM	DEFINITION	ACRONYM	DEFINITION
SAML	Security Assertions Markup Language	TOTP	Time-based One Time Password
SCADA	Supervisory Control and Data Acquisition	TPM	Trusted Platform Module
SCAP	Security Content Automation Protocol	TSIG	Transaction Signature
SCEP	Simple Certificate Enrollment Protocol	TTP	Tactics, Techniques, and Procedures
SDK	Software Development Kit	UAT	User Acceptance Testing
SDLC	Software Development Life Cycle	UAV	Unmanned Aerial Vehicle
SDLM	Software Development Life-cycle Methodology	UDP	User Datagram Protocol
SDN	Software-defined Networking	UEBA	User and Entity Behavior Analytics
SDP	Service Delivery Platform	UEFI	Unified Extensible Firmware Interface
SDV	Software-defined Visibility	UEM	Unified Endpoint Management
SED	Self-Encrypting Drives	UPS	Uninterruptable Power Supply
SEH	Structured Exception Handling	URI	Uniform Resource Identifier
SFTP	SSH File Transfer Protocol	URL	Universal Resource Locator
SHA	Secure Hashing Algorithm	USB	Universal Serial Bus
S-HTTP	Secure Hypertext Transfer Protocol	USB OTG	USB On-The-Go
SIEM	Security Information and Event Management	UTM	Unified Threat Management
SIM	Subscriber Identity Module	UTP	Unshielded Twisted Pair
SIP	Session Initiation Protocol	VBA	Visual Basic
SLA	Service-level Agreement	VDE	Virtual Desktop Environment
SLE	Single Loss Expectancy	VDI	Virtual Desktop Infrastructure
SMB	Server Message Block	VLAN	Virtual Local Area Network
S/MIME	Secure/Multipurpose Internet Mail Extensions	VLSM	Variable-length Subnet Masking
SMS	Short Message Service	VM	Virtual Machine
SMTP	Simple Mail Transfer Protocol	VoIP	Voice over IP
SMTPS	Simple Mail Transfer Protocol Secure	VPC	Virtual Private Cloud
SNMP	Simple Network Management Protocol	VPN	Virtual Private Network
SOAP	Simple Object Access Protocol	VTC	Video Teleconferencing
SOAR	Security Orchestration, Automation, Response	WAF	Web Application Firewall
SoC	System on Chip	WAP	Wireless Access Point
SOC	Security Operations Center	WEP	Wired Equivalent Privacy
SPF	Sender Policy Framework	WIDS	Wireless Intrusion Detection System
SPIM	Spam over Internet Messaging	WIPS	Wireless Intrusion Prevention System
SQL	Structured Query Language	WORM	Write Once Read Many
SQLi	SQL Injection	WPA	WiFi Protected Access
SRTP	Secure Real-time Transport Protocol	WPS	WiFi Protected Setup
SSD	Solid State Drive	WTLS	Wireless TLS
SSH	Secure Shell	XaaS	Anything as a Service
SSID	Service Set Identifier	XML	Extensible Markup Language
SSL	Secure Sockets Layer	XOR	Exclusive Or
SSO	Single Sign-on	XSRF	Cross-site Request Forgery
STIX	Structured Threat Information eXpression	XSS	Cross-site Scripting
STP	Shielded Twisted Pair		
SWG	Secure Web Gateway		
TACACS+	Terminal Access Controller Access Control System		
TAXII	Trusted Automated eXchange of Indicator Information		
TCP/IP	Transmission Control Protocol/Internet Protocol		
TGT	Ticket Granting Ticket		
TKIP	Temporal Key Integrity Protocol		
TLS	Transport Layer Security		

CompTIA.

Security+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Security+ exam. This list may also be helpful for training companies that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

HARDWARE
- Laptop with Internet access
- Separate wireless NIC
- WAP
- Firewall
- UTM
- Mobile device
- Server/cloud server
- IoT devices

SOFTWARE
- Virtualization software
- Penetration testing OS/distributions (e.g., Kali Linux, ParrotOS)
- SIEM
- Wireshark
- Metasploit
- tcpdump

OTHER
- Access to a CSP