CompTIA Security+

Version 1.0

CompTIA Security+ Overview

- Who Is Eligible for This Course?
  - Freshers looking for basic cybersecurity knowledge
  - Working IT professionals looking for basic cybersecurity certification

- Course Duration
  - 1.25 Months (48 Hours)

- Course Syllabus
  - General Security Concepts
  - Threats, Vulnerabilities, and Mitigations
  - Security Architecture
  - Security Operations
  - Security Program Management and Oversight

- Why Training @CyberSPAIS?
  - Job Oriented Industry Relevant Curriculum
  - Based On Latest Cyber Security Topics & Trends
  - 100% Assistance for Placements & Internships
  - Industry Experienced & Certified Trainer
  - Concepts Explained with Industry Scenarios
  - Comprehensive Hands-on Sessions & Labs
  - Regular Module Wise Assessments & Evaluations
  - Cybersecurity Projects & Internships
  - Thorough Preparation – Job Interview & Soft Skills
  - Arrangement To Write Certification Exams
  - Among The Top Cybersecurity Institutes in Kerala

- Launch a successful cybersecurity career
  - Develop a core foundation of essential skills, paving the way for a fulfilling career.
  - More job roles use Security+ for baseline cybersecurity skills than any other certification in the industry.

- Assess on-the-job skills
  - Security+ is the most widely adopted ISO/ANSI-accredited early career cybersecurity certification on the market with hands-on, performance-based questions on the certification exam.
  - These practical questions assess your ability to effectively problem solve in real-life situations and demonstrate your expertise to potential employers immediately.

- Embrace the latest trends
  - Understand and use the most recent advancements in cybersecurity technology, terms, techniques, and tools.
  - By acquiring early career skills in the latest trends such as automation, zero trust, risk analysis, operational technology, and IoT, you will be well-equipped to excel in the ever-evolving cybersecurity landscape.

- About the exam
  - The new CompTIA Security+ (SY0-701) represents the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk – and more.
  - Once certified, you will understand the core skills needed to succeed on the job – and employers will notice too.
  - The Security+ exam verifies you have 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, Internet of Things (IoT), and operational technology.
    - Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
    - Identify, analyze, and respond to security events and incidents.
    - CompTIA Security+ is compliant with ISO 17024 standards and approved by the U.S. DoD to meet Directive 8140.03M requirements.
    - Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.
    - Over 3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

- What Skills Will You Learn?
  - General Security Concepts
    - Includes key cybersecurity terminology and concepts up front to provide a foundation for security controls discussed throughout the exam.
  - Threats, Vulnerabilities & Mitigations
    - Focuses on responding to common threats, cyberattacks, vulnerabilities, and security incidents and appropriate mitigation techniques to monitor and secure hybrid environments.
  - Security Architecture
    - Includes security implications of different architecture models, principles of securing enterprise infrastructure, and strategies to protect data.
  - Security Operations
    - Includes applying and enhancing security and vulnerability management techniques, as well as security implications of proper hardware, software, and data management.

- Security Program Management & Oversight
  - Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment, and security awareness.

- 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
    - 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
  - Testing Provider
    - Pearson VUE
  - Exam Fees
    - USD 404 + Taxes

- Certification Renewal
  - Keep your certification up to date with CompTIA's Continuing Education (CE) program. It's designed to be a continued validation of your expertise and a tool to expand your skillset. It's also the ace up your sleeve when you're ready to take the next step in your career.
  - Get the most out of your certification
    - Information technology is an incredibly dynamic field, creating new opportunities and challenges every day. Participating in our Continuing

Education program will enable you to stay current with new and evolving technologies and remain a sought-after IT and security expert.

- The CompTIA Continuing Education program
    - Your CompTIA Security+ certification is good for three years from the day of your exam.
    - The CE program allows you to extend your certification in three-year intervals through activities and training that relate to the content of your certification.
    - Like Security+ itself, CompTIA Security+ CE also carries globally-recognized ISO/ANSI accreditation status.
    -
- It's easy to renew
    - You can participate in a number of activities and training programs, including higher certifications, to renew your CompTIA Security+ certification.
    - Complete CertMaster CE, an online, self-paced CE course, or collect at least 50 Continuing Education Units (CEUs) in three years, upload them to your certification account and Security+ will automatically renew.

CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-701

Copyright © 2023 CompTIA, Inc. All rights reserved.

About the Exam

The CompTIA Security+ certification exam will certify 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 Internet of Things (IoT).
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

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 existing exam objectives. Please know that all related exam preparation materials will still be valid.

Copyright © 2023 CompTIA, Inc. All rights reserved.

TEST DETAILS

Required exam	SY0-701
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	A minimum of 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts

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	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%
Total		**100%**

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.0 General Security Concepts

1.1 Compare and contrast various types of security controls.

- **Categories**
  - Technical
  - Managerial
  - Operational
  - Physical
- **Control types**
  - Preventive
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive

1.2 Summarize fundamental security concepts.

- **Confidentiality, Integrity, and Availability (CIA)**
- **Non-repudiation**
- **Authentication, Authorization, and Accounting (AAA)**
  - Authenticating people
  - Authenticating systems
  - Authorization models
- **Gap analysis**
- **Zero Trust**
  - 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**
  - Bollards
  - Access control vestibule
  - Fencing
  - Video surveillance
  - Security guard
  - Access badge
  - Lighting
  - Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic
- **Deception and disruption technology**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

Copyright © 2023 CompTIA, Inc. All rights reserved.

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

- **Business processes impacting security operation**
  - 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
- **Version control**

1.4 Explain the importance of using appropriate cryptographic solutions.

- **Public key infrastructure (PKI)**
  - Public key
  - Private key
  - Key escrow
- **Encryption**
  - Level
    - Full-disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  - Transport/communication
  - Asymmetric
  - Symmetric
  - Key exchange
  - Algorithms
  - Key length
- **Tools**
  - Trusted Platform Module (TPM)
  - Hardware security module (HSM)
  - Key management system
  - Secure enclave
- **Obfuscation**
  - Steganography
  - Tokenization
  - Data masking
- **Hashing**
- **Salting**
- **Digital signatures**
- **Key stretching**
- **Blockchain**
- **Open public ledger**
- **Certificates**
  - Certificate authorities
  - Certificate revocation lists (CRLs)
  - Online Certificate Status Protocol (OCSP)
  - Self-signed
  - Third-party
  - Root of trust
  - Certificate signing request (CSR) generation
  - Wildcard

Copyright © 2023 CompTIA, Inc. All rights reserved.

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 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.

- **Message-based**
  - Email
  - Short Message Service (SMS)
  - Instant messaging (IM)
- **Image-based**
- **File-based**
- **Voice call**
- **Removable device**
- **Vulnerable software**
  - Client-based vs. agentless
- **Unsupported systems and applications**
- **Unsecure networks**
  - Wireless
  - Wired
  - Bluetooth
- **Open service ports**
- **Default credentials**
- **Supply chain**
  - Managed service providers (MSPs)
  - Vendors
  - Suppliers
- **Human vectors/social engineering**
  - Phishing
  - Vishing
  - Smishing
  - Misinformation/disinformation
  - Impersonation
  - Business email compromise
  - Pretexting
  - Watering hole
  - Brand impersonation
  - Typosquatting

Copyright © 2023 CompTIA, Inc. All rights reserved.

2.3 Explain various types of vulnerabilities.

- **Application**
  - Memory injection
  - Buffer overflow
  - Race conditions
    - Time-of-check (TOC)
    - Time-of-use (TOU)
  - Malicious update
- **Operating system (OS)-based**
- **Web-based**
  - Structured Query Language injection (SQLi)
  - Cross-site scripting (XSS)
- **Hardware**
  - Firmware
  - End-of-life
  - Legacy
- **Virtualization**
  - Virtual machine (VM) escape
  - Resource reuse
- **Cloud-specific**
- **Supply chain**
  - Service provider
  - Hardware provider
  - Software provider
- **Cryptographic**
- **Misconfiguration**
- **Mobile device**
  - Side loading
  - Jailbreaking
- **Zero-day**

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
  - On-path
  - Credential replay
  - Malicious code
- **Application attacks**
  - Injection
  - Buffer overflow
  - Replay
  - Privilege escalation
  - Forgery
  - Directory traversal
- **Cryptographic attacks**
  - Downgrade
  - Collision
  - Birthday
- **Password attacks**
  - Spraying
  - Brute force
- **Indicators**
  - Account lockout
  - Concurrent session usage
  - Blocked content
  - Impossible travel
  - Resource consumption
  - Resource inaccessibility
  - Out-of-cycle logging
  - Published/documented
  - Missing logs

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

- **Segmentation**
- **Access control**
  - Access control list (ACL)
  - Permissions
- **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

Copyright © 2023 CompTIA, Inc. All rights reserved.

3.0 Security Architecture

3.1 Compare and contrast security implications of different architecture models.

- **Architecture and infrastructure concepts**
  - Cloud
    - Responsibility matrix
    - Hybrid considerations
    - Third-party vendors
  - Infrastructure as code (IaC)
  - Serverless
  - Microservices
  - Network infrastructure
    - Physical isolation
      - Air-gapped
    - Logical segmentation
    - Software-defined networking (SDN)
  - On-premises
  - Centralized vs. decentralized
  - Containerization
  - Virtualization
  - IoT
  - Industrial control systems (ICS)/supervisory control and data acquisition (SCADA)
  - Real-time operating system (RTOS)
  - Embedded systems
  - High availability
- **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**
  - Device placement
  - Security zones
  - Attack surface
  - Connectivity
  - Failure modes
    - Fail-open
    - Fail-closed
  - Device attribute
    - 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
- **Secure communication/access**
  - Virtual private network (VPN)
  - Remote access
  - Tunneling
    - 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 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**
  - Load balancing vs. clustering
- **Site considerations**
  - Hot
  - Cold
  - Warm
  - Geographic dispersion
- **Platform diversity**
- **Multi-cloud systems**
- **Continuity of operations**
- **Capacity planning**
  - People
  - Technology
  - Infrastructure
- **Testing**
  - Tabletop exercises
  - Fail over
  - Simulation
  - Parallel processing
- **Backups**
  - Onsite/offsite
  - Frequency
  - Encryption
  - Snapshots
  - Recovery
  - Replication
  - Journaling
- **Power**
  - Generators
  - Uninterruptible power supply (UPS)

4.0 Security Operations

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

- **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
- **Sandboxing**
- **Monitoring**

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

- **Acquisition/procurement process**
- **Assignment/accounting**
  - Ownership
  - Classification
- **Monitoring/asset tracking**
  - Inventory
  - Enumeration
- **Disposal/decommissioning**
  - Sanitization
  - Destruction
  - Certification
  - Data retention

Copyright © 2023 CompTIA, Inc. All rights reserved.

4.3 Explain various activities associated with vulnerability management.

- **Identification methods**
  - Vulnerability scan
  - Application security
    - Static analysis
    - Dynamic analysis
    - Package monitoring
  - Threat feed
    - 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
  - Prioritize
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerability Enumeration (CVE)
  - Vulnerability classification
  - Exposure factor
  - Environmental variables
  - Industry/organizational impact
  - Risk tolerance
- **Vulnerability response and 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 computing resources**
  - Systems
  - Applications
  - Infrastructure
- **Activities**
  - Log aggregation
  - Alerting
  - Scanning
  - Reporting
  - Archiving
  - Alert response and remediation/validation
    - Quarantine
    - Alert tuning
- **Tools**
  - Security Content Automation Protocol (SCAP)
  - Benchmarks
  - Agents/agentless
  - Security information and event management (SIEM)
  - Antivirus
  - Data loss prevention (DLP)
  - Simple Network Management Protocol (SNMP) traps
  - NetFlow
  - Vulnerability scanners

Copyright © 2023 CompTIA, Inc. All rights reserved.

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

- **Firewall**
  - Rules
  - Access lists
  - Ports/protocols
  - Screened subnets
- **IDS/IPS**
  - Trends
  - Signatures
- **Web filter**
  - Agent-based
  - Centralized proxy
  - Universal Resource Locator (URL) scanning
  - Content categorization
  - Block rules
  - Reputation
- **Operating system security**
  - Group Policy
  - SELinux
- **Implementation of secure protocols**
  - Protocol selection
  - Port selection
  - Transport method
- **DNS filtering**
- **Email security**
  - Domain-based Message Authentication Reporting and Conformance (DMARC)
  - DomainKeys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Gateway
- **File integrity monitoring**
- **DLP**
- **Network access control (NAC)**
- **Endpoint detection and response (EDR)/extended detection and response (XDR)**
- **User behavior analytics**

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

- **Provisioning/de-provisioning user accounts**
- **Permission assignments and 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
  - Discretionary
  - Role-based
  - Rule-based
  - Attribute-based
  - Time-of-day restrictions
  - Least privilege
- **Multifactor authentication**
  - Implementations
    - □ Biometrics
    - □ Hard/soft authentication tokens
    - □ Security keys
  - Factors
    - □ Something you know
    - □ Something you have
    - □ Something you are
    - □ Somewhere you are
- **Password concepts**
  - Password best practices
    - □ Length
    - □ Complexity
    - □ Reuse
    - □ Expiration
    - □ Age
  - Password managers
  - Passwordless
- **Privileged access management tools**
  - Just-in-time permissions
  - Password vaulting
  - Ephemeral credentials

Copyright © 2023 CompTIA, Inc. All rights reserved.

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

- **Use cases of automation and scripting**
  - User provisioning
  - Resource provisioning
  - Guard rails
  - Security groups
  - Ticket creation
  - Escalation
  - Enabling/disabling services and access
  - Continuous integration and testing
  - Integrations and Application programming interfaces (APIs)
- **Benefits**
  - Efficiency/time saving
  - Enforcing baselines
  - Standard infrastructure configurations
  - Scaling in a secure manner
  - Employee retention
  - Reaction time
  - Workforce multiplier
- **Other considerations**
  - Complexity
  - Cost
  - Single point of failure
  - Technical debt
  - Ongoing supportability

4.8 Explain appropriate incident response activities.

- **Process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- **Training**
- **Testing**
  - Tabletop exercise
  - Simulation
- **Root cause analysis**
- **Threat hunting**
- **Digital forensics**
  - Legal hold
  - Chain of custody
  - Acquisition
  - Reporting
  - Preservation
  - E-discovery

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

- **Log data**
  - Firewall logs
  - Application logs
  - Endpoint logs
  - OS-specific security logs
  - IPS/IDS logs
  - Network logs
  - Metadata
- **Data sources**
  - Vulnerability scans
  - Automated reports
  - Dashboards
  - Packet captures

Copyright © 2023 CompTIA, Inc. All rights reserved.

5.0 Security Program Management and Oversight

5.1 Summarize elements of effective security governance.

- **Guidelines**
- **Policies**
  - Acceptable use policy (AUP)
  - Information security policies
  - Business continuity
  - Disaster recovery
  - Incident response
  - Software development lifecycle (SDLC)
  - Change management
- **Standards**
  - Password
  - Access control
  - Physical security
  - Encryption
- **Procedures**
  - Change management
  - Onboarding/offboarding
  - Playbooks
- **External considerations**
  - Regulatory
  - Legal
  - Industry
  - Local/regional
  - National
  - Global
- **Monitoring and revision**
- **Types of governance structures**
  - Boards
  - Committees
  - Government entities
  - Centralized/decentralized
- **Roles and responsibilities for systems and data**
  - Owners
  - Controllers
  - Processors
  - Custodians/stewards

5.2 Explain elements of the risk management process.

- **Risk identification**
- **Risk assessment**
  - Ad hoc
  - Recurring
  - One-time
  - Continuous
- **Risk analysis**
  - Qualitative
  - Quantitative
  - Single loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Probability
  - Likelihood
  - Exposure factor
  - Impact
- **Risk register**
  - Key risk indicators
  - Risk owners
  - Risk threshold
- **Risk tolerance**
- **Risk appetite**
  - Expansionary
  - Conservative
  - Neutral
- **Risk management strategies**
  - Transfer
  - Accept
    - ▫ Exemption
    - ▫ Exception
  - Avoid
  - Mitigate
- **Risk reporting**
- **Business impact analysis**
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)

Copyright © 2023 CompTIA, Inc. All rights reserved.

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

- **Vendor assessment**
  - Penetration testing
  - Right-to-audit clause
  - Evidence of internal audits
  - Independent assessments
  - Supply chain analysis
- **Vendor selection**
  - Due diligence
  - Conflict of interest
- **Agreement types**
  - Service-level agreement (SLA)
  - Memorandum of agreement (MOA)
  - Memorandum of understanding (MOU)
  - Master service agreement (MSA)
  - Work order (WO)/statement of work (SOW)
  - Non-disclosure agreement (NDA)
  - Business partners agreement (BPA)
- **Vendor monitoring**
- **Questionnaires**
- **Rules of engagement**

5.4 Summarize elements of effective security compliance.

- **Compliance reporting**
  - Internal
  - External
- **Consequences of non-compliance**
  - Fines
  - Sanctions
  - Reputational damage
  - Loss of license
  - Contractual impacts
- **Compliance monitoring**
  - Due diligence/care
  - Attestation and acknowledgement
  - Internal and external
  - Automation
- **Privacy**
  - Legal implications
    - Local/regional
    - National
    - Global
  - Data subject
  - Controller vs. processor
  - Ownership
  - Data inventory and retention
  - Right to be forgotten

5.5 Explain types and purposes of audits and assessments.

- **Attestation**
- **Internal**
  - Compliance
  - Audit committee
  - Self-assessments
- **External**
  - Regulatory
  - Examinations
  - Assessment
  - Independent third-party audit
- **Penetration testing**
  - Physical
  - Offensive
  - Defensive
  - Integrated
  - Known environment
  - Partially known environment
  - Unknown environment
  - Reconnaissance
    - Passive
    - Active

Copyright © 2023 CompTIA, Inc. All rights reserved.

5.6 Given a scenario, implement security awareness practices.

- **Phishing**
  - Campaigns
  - Recognizing a phishing attempt
  - Responding to reported suspicious messages
- **Anomalous behavior recognition**
  - Risky
  - Unexpected
  - Unintentional
- **User guidance and training**
  - Policy/handbooks
  - Situational awareness
  - Insider threat
  - Password management
  - Removable media and cables
  - Social engineering
  - Operational security
  - Hybrid/remote work environments
- **Reporting and monitoring**
  - Initial
  - Recurring
- **Development**
- **Execution**

Copyright © 2023 CompTIA, Inc. All rights reserved.

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.

Acronym	Spelled Out
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AES-256	Advanced Encryption Standards 256-bit
AH	Authentication Header
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
AV	Antivirus
BASH	Bourne Again Shell
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partners Agreement
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR	Corrective Action Report
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCMP	Counter Mode/CBC-MAC Protocol
CCTV	Closed-circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operation Planning
COPE	Corporate Owned, Personally Enabled
CP	Contingency Planning
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Cloud Service Provider
CSR	Certificate Signing Request
CSRF	Cross-site Request Forgery
CSU	Channel Service Unit
CTM	Counter Mode
CTO	Chief Technology Officer
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	DomainKeys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Translation
DNS	Domain Name System
DoS	Denial of Service
DPO	Data Privacy Officer

Copyright © 2023 CompTIA, Inc. All rights reserved.

Acronym	Spelled Out
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EFS	Encrypted File System
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Management
FPGA	Field Programmable Gate Array
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	Secured File Transfer Protocol
GCM	Galois Counter Mode
GDPR	General Data Protection Regulation
GPG	Gnu Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
HA	High Availability
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-time Password
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation Air Conditioning
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System

Acronym	Spelled Out
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISO	International Standards Organization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MaaS	Monitoring as a Service
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol Label Switching
MSA	Master Service Agreement
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure

Copyright © 2023 CompTIA, Inc. All rights reserved.

Acronym	Spelled Out
MTTR	Mean Time to Recover
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGFW	Next-generation Firewall
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over the Air
OVAL	Open Vulnerability Assessment Language
P12	PKCS #12
P2P	Peer to Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
PAM	Privileged Access Management
PAM	Pluggable Authentication Modules
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards

Acronym	Spelled Out
PKI	Public Key Infrastructure
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
PTZ	Pan-tilt-zoom
PUP	Potentially Unwanted Program
RA	Recovery Agent
RA	Registration Authority
RACE	Research and Development in Advanced Communications Technologies in Europe
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol
RFID	Radio Frequency Identifier
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAN	Subject Alternative Name
SASE	Secure Access Service Edge
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SD-WAN	Software-defined Wide Area Network
SDK	Software Development Kit
SDLC	Software Development Lifecycle
SDLM	Software Development Lifecycle Methodology

Acronym	Spelled Out
SDN	Software-defined Networking
SE Linux	Security-enhanced Linux
SED	Self-encrypting Drives
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, Response
SoC	System on Chip
SOC	Security Operations Center
SOW	Statement of Work
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXchange
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
TOC	Time-of-check
TOTP	Time-based One-time Password
TOU	Time-of-use
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
TSIG	Transaction Signature
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On the Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VBA	Visual Basic
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WO	Work Order
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WTLS	Wireless TLS
XDR	Extended Detection and Response
XML	Extensible Markup Language
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

CompTIA Security+ SY0-701 Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Security+ SY0-701 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

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

CompTIA.

© 2023 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA, Inc. CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners. Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. Printed in the U.S. 10179-Jan2023