

Appendix A

Mapping Course Content to CompTIA Security+

Achieving CompTIA Security+ certification requires candidates to pass Exam SY0-701. This table describes where the exam objectives for Exam SY0-701 are covered in this course.

1.0 General Security Concepts	
1.1 Compare and contrast various types of security controls.	Covered in
Categories	Lesson 1, Topic B
Technical	
Managerial	
Operational	
Physical	
Control types	Lesson 1, Topic B
Preventive	
Deterrent	
Detective	
Corrective	
Compensating	
Directive	
1.2 Summarize fundamental security concepts.	Covered in
Confidentiality, Integrity, and Availability (CIA)	Lesson 1, Topic A
Non-repudiation	Lesson 1, Topic A
Authentication, Authorization, and Accounting	Lesson 1, Topic A
Authenticating people	
Authenticating systems	
Authorization models	

1.2 Summarize fundamental security concepts.	Covered in
Gap analysis	Lesson 1, Topic A
Zero Trust	Lesson 6, Topic B
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	Lesson 7, Topic C
Bollards	
Access control vestibule	
Fencing	
Video surveillance	
Security guard	
Access badge	
Lighting	
Sensors	
Infrared	
Pressure	
Microwave	
Ultrasonic	
Deception and disruption technology	Lesson 7, Topic B
Honeypot	
Honeynet	
Honeyfile	
Honeytoken	
1.3 Explain the importance of change management processes and the impact to security.	Covered in
Business processes impacting security operation	Lesson 14, Topic B
Approval process	
Ownership	
Stakeholders	
Impact analysis	
Test results	
Backout plan	
Maintenance window	
Standard operating procedure	

1.3 Explain the importance of change management processes and the impact to security.	Covered in
Technical implications	Lesson 14, Topic B
Allow lists/deny lists	
Restricted activities	
Downtime	
Service restart	
Application restart	
Legacy applications	
Dependencies	
Documentation	Lesson 14, Topic B
Updating diagrams	
Updating policies/procedures	
Version control	Lesson 14, Topic B
1.4 Explain the importance of using appropriate cryptographic solutions.	Covered in
Public key infrastructure (PKI)	Lesson 3, Topic B
Public key	
Private key	
Key escrow	
Encryption	Lesson 3, Topic C
Level	
Full-disk	
Partition	
File	
Volume	
Database	
Record	
Transport/communication	
Asymmetric	Lesson 3, Topic A
Symmetric	
Key exchange	Lesson 3, Topic C
Algorithms	Lesson 3, Topic A
Key length	
Tools	Lesson 3, Topic B
Trusted Platform Module (TPM)	
Hardware security module (HSM)	
Key management system	
Secure enclave	
Obfuscation	Lesson 3, Topic C
Steganography	
Tokenization	
Data masking	

1.4 Explain the importance of using appropriate cryptographic solutions.	Covered in
Hashing	Lesson 3, Topic A
Salting	Lesson 3, Topic C
Digital signatures	Lesson 3, Topic A
Key stretching	Lesson 3, Topic C
Blockchain	Lesson 3, Topic C
Open public ledger	Lesson 3, Topic C
Certificates	Lesson 3, Topic B
Certificate authorities	
Certificate revocation lists (CRLs)	
Online Certificate Status Protocol (OCSP)	
Self-signed	
Third-party	
Root of trust	
Certificate signing request (CSR) generation	
Wildcard	
2.0 Threats, Vulnerabilities, and Mitigations	
2.1 Compare and contrast common threat actors and motivations.	Covered in
Threat actors	Lesson 2, Topic A
Nation-state	
Unskilled attacker	
Hacktivist	
Insider threat	
Organized crime	
Shadow IT	
Attributes of actors	Lesson 2, Topic A
Internal/external	
Resources/funding	
Level of sophistication/capability	
Motivations	Lesson 2, Topic A
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.	Covered in
Message-based	Lesson 2, Topic B
Email	
Short Message Service (SMS)	
Instant messaging (IM)	
Image-based	Lesson 2, Topic B
File-based	Lesson 2, Topic B
Voice call	Lesson 2, Topic B
Removable device	Lesson 2, Topic B
Vulnerable software	Lesson 2, Topic B
Client-based vs. agentless	
Unsupported systems and applications	Lesson 2, Topic B
Unsecure networks	Lesson 2, Topic B
Wireless	
Wired	
Bluetooth	
Open service ports	Lesson 2, Topic B
Default credentials	Lesson 2, Topic B
Supply chain	Lesson 2, Topic B
Managed service providers (MSPs)	
Vendors	
Suppliers	
Human vectors/social engineering	Lesson 2, Topic C
Phishing	
Vishing	
Smishing	
Misinformation/disinformation	
Impersonation	
Business email compromise	
Pretexting	
Watering hole	
Brand impersonation	
Typosquatting	
2.3 Explain various types of vulnerabilities	Covered in
Application	Lesson 8, Topic B
Memory injection	
Buffer overflow	
Race conditions	
Time-of-check (TOC)	
Time-of-use (TOU)	
Malicious update	

2.3 Explain various types of vulnerabilities	Covered in
Operating system (OS)-based	Lesson 8, Topic A
Web-based	Lesson 8, Topic B
Structured Query Language injection (SQLi)	
Cross-site scripting (XSS)	
Hardware	Lesson 8, Topic A
Firmware	
End-of-life	
Legacy	
Virtualization	Lesson 8, Topic A
Virtual machine (VM) escape	
Resource reuse	
Cloud-specific	Lesson 8, Topic B
Supply chain	Lesson 8, Topic B
Service provider	
Hardware provider	
Software provider	
Cryptographic	Lesson 8, Topic A
Misconfiguration	Lesson 8, Topic A
Mobile device	Lesson 8, Topic A
Side loading	
Jailbreaking	
Zero-day	Lesson 8, Topic A
2.4 Given a scenario, analyze indicators of malicious activity.	Covered in
Malware attacks	Lesson 13, Topic A
Ransomware	
Trojan	
Worm	
Spyware	
Bloatware	
Virus	
Keylogger	
Logic bomb	
Rootkit	
Physical attacks	Lesson 13, Topic B
Brute force	
Radio frequency identification (RFID) cloning	
Environmental	

2.4 Given a scenario, analyze indicators of malicious activity.	Covered in
Network attacks Distributed denial-of-service (DDoS) Amplified Reflected Domain Name System (DNS) attacks Wireless On-path Credential replay Malicious code	Lesson 13, Topic B
Application attacks Injection Buffer overflow Replay Privilege escalation Forgery Directory traversal	Lesson 13, Topic C
Cryptographic attacks Downgrade Collision Birthday	Lesson 13, Topic B
Password attacks Spraying Brute force	Lesson 13, Topic B
Indicators Account lockout Concurrent session usage Blocked content Impossible travel Resource consumption Resource inaccessibility Out-of-cycle logging Published/documented Missing logs	Lesson 13, Topic A
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	Covered in
Segmentation	Lesson 10, Topic A
Access control Access control list (ACL) Permissions	Lesson 10, Topic A
Application allow list	Lesson 10, Topic A
Isolation	Lesson 10, Topic A
Patching	Lesson 10, Topic A

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	Covered in
Encryption	Lesson 10, Topic A
Monitoring	Lesson 10, Topic A
Least privilege	Lesson 10, Topic A
Configuration enforcement	Lesson 10, Topic A
Decommissioning	Lesson 10, Topic A
Hardening techniques	Lesson 10, Topic A
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.	Covered in
Architecture and infrastructure concepts	Lesson 5, Topic A
Cloud	Lesson 6, Topic A
Responsibility matrix	
Hybrid considerations	
Third-party vendors	
Infrastructure as code (IaC)	
Serverless	
Microservices	
Network infrastructure	
Physical isolation	Lesson 5, Topic A
Air-gapped	
Logical segmentation	
Software-defined networking (SDN)	Lesson 6, Topic A
On-premises	Lesson 5, Topic A
Centralized vs. decentralized	Lesson 6, Topic A
Containerization	
Virtualization	
IoT	Lesson 6, Topic B
Industrial control systems (ICS)/supervisory control and data acquisition (SCADA)	
Real-time operating system (RTOS)	
Embedded systems	
High availability	Lesson 6, Topic A

3.1 Compare and contrast security implications of different architecture models.	Covered in
--	------------

Considerations	Lesson 6, Topic A
Availability	
Resilience	
Cost	
Responsiveness	
Scalability	
Ease of deployment	
Risk transference	Lesson 5, Topic A
Ease of recovery	Lesson 6, Topic A
Patch availability	
Inability to patch	
Power	
Compute	

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

Infrastructure considerations	Lesson 5, Topic A
Device placement	Lesson 5, Topic B
Security zones	Lesson 5, Topic A
Attack surface	
Connectivity	
Failure modes	Lesson 5, Topic B
Fail-open	
Fail-closed	
Device attribute	
Active vs. passive	
Inline vs. tap/monitor	
Network appliances	Lesson 5, Topic A
Jump server	Lesson 5, Topic C
Proxy server	Lesson 5, Topic B
Intrusion prevention system (IPS)/intrusion detection system (IDS)	
Load balancer	
Sensors	
Port security	Lesson 5, Topic A
802.1X	
Extensible Authentication Protocol (EAP)	
Firewall types	Lesson 5, Topic B
Web application firewall (WAF)	
Unified threat management (UTM)	
Next-generation firewall (NGFW)	
Layer 4/Layer 7	

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	Covered in
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)	Lesson 5, Topic C
Selection of effective controls	Lesson 5, Topic B
3.3 Compare and contrast concepts and strategies to protect data.	Covered in
Data types Regulated Trade secret Intellectual property Legal information Financial information Human- and non-human-readable	Lesson 16, Topic A
Data classifications Sensitive Confidential Public Restricted Private Critical	Lesson 16, Topic A
General data considerations Data states Data at rest Data in transit Data in use Data sovereignty Geolocation	Lesson 16, Topic A
Methods to secure data Geographic restrictions Encryption Hashing Masking Tokenization Obfuscation Segmentation Permission restrictions	Lesson 16, Topic A

3.4 Explain the importance of resilience and recovery in security architecture.	Covered in
High availability	Lesson 7, Topic B
Load balancing vs. clustering	
Site considerations	Lesson 7, Topic B
Hot	
Cold	
Warm	
Geographic dispersion	
Platform diversity	Lesson 7, Topic B
Multi-cloud systems	Lesson 7, Topic B
Continuity of operations	Lesson 7, Topic B
Capacity planning	Lesson 7, Topic B
People	
Technology	
Infrastructure	
Testing	Lesson 7, Topic B
Tabletop exercises	
Fail over	
Simulation	
Parallel processing	
Backups	Lesson 7, Topic B
Onsite/offsite	Lesson 7, Topic A
Frequency	
Encryption	
Snapshots	
Recovery	
Replication	
Journaling	
Power	Lesson 7, Topic B
Generators	
Uninterruptible power supply (UPS)	

4.0 Security Operations	
4.1 Given a scenario, apply common security techniques to computing resources.	Covered in
Secure baselines	Lesson 9, Topic A
Establish	
Deploy	
Maintain	

4.1 Given a scenario, apply common security techniques to computing resources.	Covered in
Hardening targets	Lesson 9, Topic A Lesson 10, Topic A
Mobile devices	
Workstations	Lesson 9, Topic A
Switches	
Routers	
Cloud infrastructure	
Servers	Lesson 11, Topic B
ICS/SCADA	Lesson 10, Topic A
Embedded systems	
RTOS	
IoT devices	
Wireless devices	Lesson 9, Topic A
Installation considerations	
Site surveys	
Heat maps	Lesson 10, Topic B
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	Lesson 9, Topic A
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	Lesson 11, Topic B
Input validation	
Secure cookies	
Static code analysis	
Code signing	
Sandboxing	Lesson 11, Topic B
Monitoring	

4.2 Explain the security implications of proper hardware, software, and data asset management.	Covered inw
Acquisition/procurement process	Lesson 7, Topic A
Assignment/accounting	Lesson 7, Topic A
Ownership	
Classification	
Monitoring/asset tracking	Lesson 7, Topic A
Inventory	
Enumeration	
Disposal/decommissioning	Lesson 7, Topic A
Sanitization	
Destruction	
Certification	
Data retention	

4.3 Explain various activities associated with vulnerability management.	Covered in
Identification methods	Lesson 8, Topic C
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	Lesson 8, Topic D
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	

4.3 Explain various activities associated with vulnerability management.	Covered in
Vulnerability response and remediation Patching Insurance Segmentation Compensating controls Exceptions and exemptions Validation of remediation Rescanning Audit Verification	Lesson 8, Topic D Lesson 8, Topic D
Reporting	Lesson 8, Topic D
4.4 Explain security alerting and monitoring concepts and tools.	Covered in
Monitoring computing resources Systems Applications Infrastructure	Lesson 12, Topic D
Activities Log aggregation Alerting Scanning Reporting Archiving Alert response and remediation/validation Quarantine Alert tuning	Lesson 12, Topic D
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	Lesson 12, Topic D

4.5 Given a scenario, modify enterprise capabilities to enhance security.	Covered in
Firewall	Lesson 9, Topic B
Rules	
Access lists	
Ports/protocols	
Screened subnets	
IDS/IPS	Lesson 9, Topic B
Trends	
Signatures	
Web filter	Lesson 9, Topic B
Agent-based	
Centralized proxy	
Universal Resource Locator (URL) scanning	
Content categorization	
Block rules	
Reputation	
Operating system security	Lesson 10, Topic A
Group Policy	
SELinux	
Implementation of secure protocols	Lesson 11, Topic A
Protocol selection	
Port selection	
Transport method	
DNS filtering	Lesson 11, Topic A
Email security	Lesson 11, Topic A
Domain-based Message Authentication Reporting and Conformance (DMARC)	
DomainKeys Identified Mail (DKIM)	
Sender Policy Framework (SPF)	
Gateway	
File integrity monitoring	Lesson 10, Topic A
DLP	Lesson 11, Topic A
Network access control (NAC)	Lesson 9, Topic A
Endpoint detection and response (EDR)/extended detection and response (XDR)	Lesson 10, Topic A
User behavior analytics	Lesson 10, Topic A
4.6 Given a scenario, implement and maintain identity and access management.	Covered in
Provisioning/de-provisioning user accounts	Lesson 4, Topic B
Permission assignments and implications	Lesson 4, Topic B
Identity proofing	Lesson 4, Topic B
Federation	Lesson 4, Topic C

4.6 Given a scenario, implement and maintain identity and access management.	Covered in
Single sign-on (SSO)	Lesson 4, Topic C
Lightweight Directory Access Protocol (LDAP)	
Open authorization (OAuth)	
Security Assertions Markup Language (SAML)	
Interoperability	Lesson 4, Topic C
Attestation	Lesson 4, Topic A
Access controls	Lesson 4, Topic B
Mandatory	
Discretionary	
Role-based	
Rule-based	
Attribute-based	
Time-of-day restrictions	
Least privilege	
Multifactor authentication	Lesson 4, Topic A
Implementations	
Biometrics	
Hard/soft authentication tokens	
Security keys	
Factors	
Something you know	
Something you have	
Something you are	
Somewhere you are	
Password concepts	Lesson 4, Topic A
Password best practices	
Length	
Complexity	
Reuse	
Expiration	
Age	
Password managers	
Passwordless	
Privileged access management tools	Lesson 4, Topic B
Just-in-time permissions	
Password vaulting	
Ephemeral credentials	

4.7 Explain the importance of automation and orchestration related to secure operations.	Covered in
Use cases of automation and scripting	Lesson 14, Topic C
- 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	Lesson 14, Topic C
- Efficiency/time saving - Enforcing baselines - Standard infrastructure configurations - Scaling in a secure manner - Employee retention - Reaction time - Workforce multiplier	
Other considerations	Lesson 14, Topic C
- Complexity - Cost - Single point of failure - Technical debt - Ongoing supportability	
4.8 Explain appropriate incident response activities.	Covered in
Process	Lesson 12, Topic A
- Preparation - Detection - Analysis - Containment - Eradication - Recovery - Lessons learned	
Training	Lesson 12, Topic A
Testing	Lesson 12, Topic A
- Tabletop exercise - Simulation	
Root cause analysis	Lesson 12, Topic A
Threat hunting	Lesson 12, Topic A

4.8 Explain appropriate incident response activities.	Covered in
Digital forensics Legal hold Chain of custody Acquisition Reporting Preservation E-discovery	Lesson 12, Topic B
4.9 Given a scenario, use data sources to support an investigation.	Covered in
Log data Firewall logs Application logs Endpoint logs OS-specific security logs IPS/IDS logs Network logs Metadata	Lesson 12, Topic C
Data sources Vulnerability scans Automated reports Dashboards Packet captures	Lesson 12, Topic C
5.0 Security Program Management and Oversight	
5.1 Summarize elements of effective security governance.	Covered in
Guidelines	Lesson 14, Topic A
Policies Acceptable use policy (AUP) Information security policies Business continuity Disaster recovery Incident response Software development lifecycle (SDLC) Change management	Lesson 14, Topic A
Standards Password Access control Physical security Encryption	Lesson 14, Topic A

5.1 Summarize elements of effective security governance.	Covered in
Procedures	Lesson 14, Topic A
Change management	
Onboarding/offboarding	
Playbooks	
External considerations	Lesson 14, Topic A
Regulatory	
Legal	
Industry	
Local/regional	
National	
Global	
Monitoring and revision	Lesson 14, Topic A
Types of governance structures	Lesson 14, Topic A
Boards	
Committees	
Government entities	
Centralized/decentralized	
Roles and responsibilities for systems and data	Lesson 14, Topic A
Owners	
Controllers	
Processors	
Custodians/stewards	
5.2 Explain elements of the risk management process.	Covered in
Risk identification	Lesson 15, Topic A
Risk assessment	Lesson 15, Topic A
Ad hoc	
Recurring	
One-time	
Continuous	
Risk analysis	Lesson 15, Topic A
Qualitative	
Quantitative	
Single loss expectancy (SLE)	
Annualized loss expectancy (ALE)	
Annualized rate of occurrence (ARO)	
Probability	
Likelihood	
Exposure factor	
Impact	
Risk register	Lesson 15, Topic A
Key risk indicators	
Risk owners	
Risk threshold	

5.2 Explain elements of the risk management process.	Covered in
Risk tolerance	Lesson 15, Topic A
Risk appetite	Lesson 15, Topic A
Expansionary	
Conservative	
Neutral	
Risk management strategies	Lesson 15, Topic A
Transfer	
Accept	
Exemption	
Exception	
Avoid	
Mitigate	
Risk reporting	Lesson 15, Topic A
Business impact analysis	Lesson 15, Topic A
Recovery time objective (RTO)	
Recovery point objective (RPO)	
Mean time to repair (MTTR)	
Mean time between failures (MTBF)	
5.3 Explain the processes associated with third-party risk assessment and management.	Covered in
Vendor assessment	Lesson 15, Topic B
Penetration testing	
Right-to-audit clause	
Evidence of internal audits	
Independent assessments	
Supply chain analysis	
Vendor selection	Lesson 15, Topic B
Due diligence	
Conflict of interest	
Agreement types	Lesson 15, Topic B
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	Lesson 15, Topic B
Questionnaires	Lesson 15, Topic B
Rules of engagement	Lesson 15, Topic B

5.4 Summarize elements of effective security compliance.	Covered in
Compliance reporting	Lesson 16, Topic A
Internal	
External	
Consequences of non-compliance	Lesson 16, Topic A
Fines	
Sanctions	
Reputational damage	
Loss of license	
Contractual impacts	
Compliance monitoring	Lesson 16, Topic A
Due diligence/care	
Attestation and acknowledgement	
Internal and external	
Automation	
Privacy	Lesson 16, Topic A
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.	Covered in
Attestation	Lesson 15, Topic C
Internal	Lesson 15, Topic C
Compliance	
Audit committee	
Self-assessments	
External	Lesson 15, Topic C
Regulatory	
Examinations	
Assessment	
Independent third-party audit	

5.5 Explain types and purposes of audits and assessments.	Covered in
Penetration testing Physical Offensive Defensive Integrated Known environment Partially known environment Unknown environment Reconnaissance Passive Active	Lesson 15, Topic C
5.6 Given a scenario, implement security awareness practices.	Covered in
Phishing Campaigns Recognizing a phishing attempt Responding to reported suspicious messages	Lesson 16, Topic B
Anomalous behavior recognition Risky Unexpected Unintentional	Lesson 16, Topic B
User guidance and training Policy/handbooks Situational awareness Insider threat Password management Removable media and cables Social engineering Operational security Hybrid/remote work environments	Lesson 16, Topic B
Reporting and monitoring Initial Recurring	Lesson 16, Topic B
Development	Lesson 16, Topic B
Execution	Lesson 16, Topic B