CompTIA Security+ SY0-701 30-Day Study Plan

secplusmastery.com

A printable day-by-day checklist across all five domains. A free study resource.

A focused 30-day plan to prepare for the CompTIA Security+ SY0-701 exam (up to 90 questions, 90 minutes, 750 of 900 to pass). Each day covers a defined topic, with built-in review and practice days. Adjust the pace to your schedule, but keep the order: it follows the five domains by exam weight.

Week 1: Foundations and Domain 1 (General Security Concepts)

[ ] **Day 1** **Orientation.** Learn the exam format (up to 90 questions, 90 minutes, 750 of 900 to pass, including performance-based questions) and the five domains and their weights. Skim the acronyms glossary and the ports cheat sheet.

[ ] **Day 2** **Security controls.** Study control categories (technical, managerial, operational, physical) and control types (preventive, deterrent, detective, corrective, compensating, directive).

[ ] **Day 3** **Core concepts.** Review the CIA triad, non-repudiation, AAA, Zero Trust, physical security, and deception techniques such as honeypots.

[ ] **Day 4** **Cryptography.** Study symmetric vs asymmetric encryption, hashing, digital signatures, PKI, and certificates. Use the cryptography cheat sheet.

[ ] **Day 5** **Change management and review.** Review change management processes, then take the Domain 1 practice questions and note weak spots.

[ ] **Day 6** **Threats begin.** Start Domain 2: threat actors and their motivations, plus threat vectors and attack surfaces.

[ ] **Day 7** **Week 1 review.** Light day. Re-quiz Domain 1, build flashcards for anything shaky, and rest.

Week 2: Threats and Architecture (Domains 2 and 3)

[ ] **Day 8** **Vulnerabilities.** Study vulnerability types: application, operating system, web, hardware, cloud, supply chain, and misconfiguration.

[ ] **Day 9** **Malicious activity.** Learn malware types and social engineering techniques. Use the common attacks cheat sheet.

[ ] **Day 10** **Mitigations.** Study mitigation techniques: segmentation, hardening, least privilege, patching, and isolation. Take the Domain 2 practice questions.

[ ] **Day 11** **Architecture models.** Start Domain 3: cloud, serverless, microservices, virtualization, infrastructure as code, and Zero Trust models.

[ ] **Day 12** **Secure infrastructure.** Study firewalls, IDS and IPS, and ports and protocols. Use the ports cheat sheet and the IDS vs IPS guide.

[ ] **Day 13** **Data and resilience.** Review data classification, DLP, encryption states, backups, RAID, and high availability.

[ ] **Day 14** **Week 2 review.** Take the full 30-question practice test and record which domains are weakest.

Week 3: Security Operations (Domain 4, the largest domain)

[ ] **Day 15** **Secure resources.** Study secure baselines, hardening, mobile device security, and endpoint protection such as EDR.

[ ] **Day 16** **Asset and vulnerability management.** Review asset inventory and disposal, vulnerability scanning, CVSS scoring, and remediation.

[ ] **Day 17** **Monitoring and alerting.** Study SIEM, SNMP, NetFlow, log aggregation, and alerting concepts.

[ ] **Day 18** **Enterprise capabilities.** Review firewall rules, web and DNS filtering, email security, NAC, and DLP.

[ ] **Day 19** **Identity and access.** Study IAM, provisioning, SSO, MFA, federation, and PAM. Use the MAC vs DAC vs RBAC and authentication vs authorization guides.

[ ] **Day 20** **Automation and incident response.** Review SOAR, the incident response phases, digital forensics, and log data sources.

[ ] **Day 21** **Domain 4 review.** Take the Domain 4 practice questions and review every item you miss.

Week 4: Program Management and final prep (Domain 5 plus review)

[ ] **Day 22** **Governance.** Start Domain 5: policies, standards, procedures, guidelines, and roles and responsibilities.

[ ] **Day 23** **Risk management.** Study risk assessment, SLE, ARO, and ALE, the risk register, and the four risk responses: accept, avoid, transfer, mitigate.

[ ] **Day 24** **Third-party risk.** Review vendor assessment, due diligence, and agreements such as SLA, MOU, NDA, and BPA.

[ ] **Day 25** **Compliance and privacy.** Study key regulations (HIPAA, GDPR, PCI DSS), data roles, and privacy concepts.

[ ] **Day 26** **Audits and awareness.** Review internal and external audits, penetration testing, attestation, and security awareness training. Take the Domain 5 practice questions.

[ ] **Day 27** **Full review.** Take the full practice test again and concentrate on your weakest domains.

[ ] Day 28 **Targeted review.** Redo the per-domain practice for your two weakest domains and re-read the ports, cryptography, attacks, and acronyms cheat sheets.

[ ] Day 29 **Light review and logistics.** Skim all cheat sheets and flashcards. Confirm your exam appointment, ID, and testing rules. Do not cram new material.

[ ] Day 30 **Exam day.** Do a brief warm-up with the cheat sheets, arrive early, read each question carefully, flag and return to hard ones, and manage your time. You are ready.