IT DOJO

EXAM STUDY GUIDE

Security+

COMPTIA SECURITY+ (SY0-701)

A domain-by-domain field guide to CompTIA Security+ — the foundational, vendor-neutral security certification. Aligned to the current SY0-701 objectives. DoD 8140/8570 IAT Level II approved.

5 Domains • Concepts, tables & math • Mnemonics & exam tips

Trusted IT & Cybersecurity Training Since 2003 • Virginia Beach, VA

ABOUT THIS GUIDE — This is an exam-preparation aid built around the official, publicly available exam objectives. It is designed to reinforce and condense your study — not to replace hands-on experience, official courseware, or a complete study plan. Certification exams are updated periodically, so always confirm the current objectives with the certifying body before you test. We work hard to keep this accurate but make no warranty that it is complete or error-free, and IT Dojo is not affiliated with the certification bodies named. Use it as one tool among several on your way to passing.

Security+ at a Glance

Security+ validates the core skills to assess security posture, secure hybrid environments, and respond to incidents. It is broad and practical, and includes performance-based questions (PBQs) that put you in a hands-on scenario.

EXAM CODE
SY0-701 (V7)

QUESTIONS
Max 90 (MC + PBQs)

LENGTH
90 minutes

PASSING SCORE
750 (scale 100–900)

RECOMMENDED
Network+ & 2 yrs experience

RENEWAL
Valid 3 years (CEUs)

DOMAINS & EXAM WEIGHTING

#	Domain	Weight	Relative
1	General Security Concepts	**12%**	
2	Threats, Vulnerabilities & Mitigations	**22%**	
3	Security Architecture	**18%**	
4	Security Operations	**28%**	
5	Security Program Management & Oversight	**20%**	

HOW TO USE THIS GUIDE

Each section below gives the core ideas you must know, a short list of high-yield terms, an exam tip, and a self-check against the official outline. Use it as a primer and a final-week refresher — not as your only resource.

1 General Security Concepts

Controls, fundamentals, change management, and cryptography

12%

CORE CONCEPTS

- **Security controls** are described two ways: by **category** (technical, managerial, operational, physical) and by **type/function** (preventive, deterrent, detective, corrective, compensating, directive). A single control can be more than one — a fence is physical and both deterrent and preventive.
- **Fundamentals** — the CIA triad, **AAA** (authentication, authorization, accounting), non-repudiation, and gap analysis. These frame every later domain.
- **Zero Trust** separates the **control plane** (the policy engine and policy administrator that make decisions) from the **data plane** (the policy enforcement point that acts on them). The model assumes breach and verifies every request.
- **Deception & disruption** — honeypots, honeynets, honeyfiles, and honeytokens lure attackers and generate high-fidelity alerts, since no legitimate user should ever touch them.
- **Change management** matters for security: approval, ownership, test/backout plans, and maintenance windows reduce the risk that a change itself becomes the incident.
- **Cryptographic building blocks** — PKI, symmetric vs. asymmetric encryption, key exchange, certificates, digital signatures, hashing, salting, and blockchain. Salting defeats precomputed (rainbow-table) attacks.

CONTROL TYPES (FUNCTION)

Type	What It Does
Preventive	Stops an action before it happens (firewall rule, MFA).
Deterrent	Discourages an attempt (warning banner, visible cameras).
Detective	Identifies an event during/after (logs, IDS, alarms).
Corrective	Restores after an event (backups, patching).
Compensating	Substitutes when the primary control isn’t feasible.
Directive	Instructs/mandates behavior (policy, signage).

HIGH-YIELD TERMS

control category vs. type, CIA, AAA, non-repudiation, zero trust, control plane vs. data plane, PEP/PDP, honeytoken, PKI, salting, digital signature.

EXAM TIP

Know control **categories vs. types** cold — it is one of the most-tested distinctions. A **compensating** control is the fallback you use when the primary control is not feasible.

MEMORY AID

Control **categories** = "**T-MOP**": **T**echnical, **M**anagerial, **O**perational, **P**hysical. Zero Trust: the **PE** (Policy **E**ngine) **decides**, the **PEP** (enforcement point) **does**.

OUTLINE COVERAGE — SELF-CHECK

- [ ] Security controls (categories & types)
- [ ] Fundamental concepts
- [ ] Change management
- [ ] Cryptographic solutions

2 Threats, Vulnerabilities & Mitigations

Actors, vectors, vulnerabilities, attacks, and defenses

22%

CORE CONCEPTS

- **Threat actors** differ by attributes (resources, sophistication, internal vs. external) and motivation. A nation-state (APT) is well-resourced and stealthy; an unskilled attacker ("script kiddie") reuses tools; insiders and shadow IT bypass perimeter defenses entirely.
- **Threat vectors & attack surfaces** — message-based (phishing email/SMS), files, removable media, vulnerable or unsupported software, and the supply chain. Reducing the attack surface is itself a control.
- **Vulnerabilities** span application (buffer overflow, race condition/TOCTOU), web (SQLi, XSS), hardware (firmware, end-of-life), virtualization (VM escape), cloud, mobile, and the dreaded **zero-day** (no patch yet exists).
- **Recognizing attacks** — malware families (ransomware, trojan, worm, rootkit, logic bomb), network attacks (DDoS, DNS, on-path/MITM), application attacks (injection, privilege escalation, replay), and password attacks (spraying, brute force). The exam tests you on **indicators** that distinguish them.
- **Mitigations** — segmentation, least privilege, patching, encryption, monitoring, and host hardening (disabling unused ports/services, host firewall, EDR). Match the defense to the specific weakness.

COMMON MALWARE TYPES

Type	Behavior
Ransomware	Encrypts data and demands payment for the key.
Trojan	Disguised as legitimate software; opens a backdoor.
Worm	Self-replicates across networks with no user action.
Rootkit	Hides at a privileged level to evade detection.
Spyware	Covertly collects user data and activity.
Logic bomb	Dormant code that triggers on a condition or date.

HIGH-YIELD TERMS

APT, script kiddie, insider/shadow IT, TOCTOU, VM escape, zero-day, on-path (MITM), privilege escalation, IoC, segmentation, hardening, least privilege.

EXAM TIP

Map each **attack to its best mitigation**. "Least privilege" and "segmentation" are frequent best-answers; let the described **indicators** point you to which attack is happening.

MEMORY AID

Password attacks: **spraying** = one password against **many** users (avoids lockout); **brute force** = many passwords against **one** user. **Worm** spreads on its own; a **virus** needs you to run it.

OUTLINE COVERAGE — SELF-CHECK

- [ ] Threat actors & motivations
- [ ] Threat vectors & attack surfaces
- [ ] Vulnerability types
- [ ] Indicators of malicious activity
- [ ] Mitigation techniques

3 Security Architecture

Secure design across cloud, network, data, and resilience

18%

CORE CONCEPTS

- **Architecture models** — cloud (with a shared-responsibility matrix), IaC, serverless, microservices, containers, virtualization, IoT, ICS/SCADA, and embedded systems. Each is a trade-off among availability, resilience, cost, and patchability.
- **Enterprise infrastructure** — device placement and security zones, plus a key design choice: **fail-open** (favor availability) vs. **fail-closed** (favor security), and whether a device is **inline** (can block) or a **tap/monitor** (observe only).
- **Firewalls & access** — from packet filters to stateful to proxy to NGFW and WAF; secure remote access via VPN tunneling (TLS, IPSec), SD-WAN, and SASE.
- **Data protection** — classify data, protect it in all three states (at rest, in transit, in use), and apply encryption, hashing, masking, tokenization, or obfuscation as fits the use case. Sovereignty dictates where data may legally reside.
- **Resilience** — high availability (load balancing, clustering), site types (hot/warm/cold), geographic dispersion, backups, and power protection (UPS, generators), validated by regular testing.

RECOVERY SITE TYPES

Site	Whats Ready	Speed	Cost
Cold	Space & power only	Slowest	Lowest
Warm	Some hardware; restore data	Moderate	Medium
Hot	Fully equipped, near-real-time data	Fast	High

HIGH-YIELD TERMS

shared responsibility, IaC, fail-open/closed, inline vs. tap, NGFW, WAF, SASE, SD-WAN, data states, tokenization, geographic dispersion.

EXAM TIP

Fail-closed favors security; fail-open favors availability. Know which appliance is inline (can block traffic) versus a passive tap (monitor only) — PBQs test this.

MEMORY AID

Tokenization swaps data for a meaningless token (reversible via a vault); **masking** just hides characters (****1234); **hashing** is one-way. Cloud: **SaaS** = provider owns most; **IaaS** = you own most.

OUTLINE COVERAGE — SELF-CHECK

- [ ] Architecture models & trade-offs
- [ ] Enterprise infrastructure principles
- [ ] Data protection strategies
- [ ] Resilience & recovery

4 Security Operations

Hardening, monitoring, IAM, automation, and incident response

28%

CORE CONCEPTS

- **Securing resources** — secure baselines and hardening across mobile, servers, ICS/SCADA, and IoT; wireless security (WPA3, RADIUS); mobile management (MDM with BYOD/COPE/CYOD); and application security (input validation, sandboxing).
- **Vulnerability management** — scan, then prioritize with **CVSS** scores and **CVE** identifiers, then remediate, validate, and report. Confirm findings to rule out false positives before acting.
- **Monitoring & alerting** — aggregate logs into a **SIEM**, then tune alerts to cut noise; supporting tools include SCAP, NetFlow, DLP, and SNMP traps.
- **Hardening the enterprise** — firewall and IPS rules, web/DNS filtering, file integrity monitoring, NAC, EDR/XDR, and email authentication. The **SPF → DKIM → DMARC** trio together defeats spoofing.
- **IAM** — provisioning/deprovisioning, federation and SSO (LDAP, SAML, OAuth), access models, MFA factor types, and privileged access management (just-in-time, vaulting).
- **Automation & incident response** — SOAR automates repetitive response; the IR lifecycle runs **preparation → detection → analysis → containment → eradication → recovery → lessons learned**, supported by forensics and chain of custody.

EMAIL AUTHENTICATION TRIO

Record	Purpose
SPF	Lists which mail servers are authorized to send for the domain.
DKIM	Adds a cryptographic signature proving the message wasn't altered.
DMARC	Tells receivers how to handle SPF/DKIM failures and where to report.

HIGH-YIELD TERMS

baseline/hardening, WPA3, MDM (BYOD/COPE/CYOD), CVSS/CVE, SIEM, SCAP, SPF/DKIM/DMARC, NAC, EDR/XDR, SOAR, IR lifecycle, PAM.

EXAM TIP

This is the **heaviest domain (28%)** — invest here. Memorize the **IR lifecycle order** and the email-authentication trio **SPF, DKIM, DMARC** (PBQ favorites).

MEMORY AID

Email auth: **SPF** says **who can send**, **DKIM signs** the message, **DMARC** says **what to do** if they fail. IR order: "**P-DAC-ERL**" — Prep, Detect, Analyze, Contain, Eradicate, Recover, Lessons.

OUTLINE COVERAGE — SELF-CHECK

- [ ] Apply security to resources
- [ ] Asset management
- [ ] Vulnerability management
- [ ] Monitoring & alerting
- [ ] Enhance enterprise security
- [ ] Identity & access management
- [ ] Automation & orchestration
- [ ] Incident response
- [ ] Investigate data sources

5 Security Program Management & Oversight

Governance, risk, third-party, compliance, and awareness

20%

CORE CONCEPTS

- **Security governance** — policies (AUP, BC/DR, incident response, SDLC), standards, procedures, and playbooks, plus the roles of owner, controller, processor, and custodian. Governance gives the program its authority.
- **Risk management** — identify, assess (qualitative or quantitative with **SLE/ALE/ARO**), and track in a risk register with owners and thresholds. Choose a response — transfer, accept, avoid, or mitigate — consistent with risk appetite.
- **Business impact analysis** quantifies disruption with **RTO, RPO, MTTR, and MTBF** — the metrics that drive continuity and recovery investment.
- **Third-party risk** — vendor assessments, right-to-audit clauses, and supply-chain analysis, formalized in agreements: SLA, MOU, MSA, SOW, BPA, and NDA. Know what each agreement does.
- **Compliance & awareness** — reporting and the consequences of non-compliance (fines, reputational, contractual), privacy concepts (data subject, controller vs. processor, right to be forgotten), and security-awareness programs including phishing simulations.

COMMON VENDOR AGREEMENTS

Agreement	Purpose
SLA	Defines measurable service/performance targets.
MSA	Master terms governing the overall relationship.
SOW	The specific scope, deliverables, and timeline of work.
MOU/MOA	A (often non-binding) statement of intent to cooperate.
BPA	Business partnership terms (roles, profit/loss, responsibilities).
NDA	Protects confidential information shared between parties.

HIGH-YIELD TERMS

AUP, risk register, risk appetite, ALE/SLE/ARO, RTO/RPO/MTTR/MTBF, SLA/MOU/MSA/SOW/BPA, due diligence, right to be forgotten.

WORKED EXAMPLE — QUANTITATIVE RISK

An asset worth **$500,000** faces a threat that would destroy an estimated 30% of it, occurring roughly once every 10 years.

`EF = 30%`	Exposure Factor — portion of the asset lost per event
`SLE = AV × EF`	$500,000 × 0.30 = **$150,000** (Single Loss Expectancy)
`ARO = 0.1`	Annualized Rate of Occurrence — once per 10 years
`ALE = SLE × ARO`	$150,000 × 0.10 = **$15,000 / year** (Annualized Loss Expectancy)

Decision rule: a safeguard is cost-justified only if it costs **less than the $15,000/year ALE** it reduces.

EXAM TIP

A lighter "manager mindset": **governance, policy, and risk before technology**. Distinguish the agreements — **MSA** sets overall terms, **SOW** defines the specific work, **SLA** sets performance targets.

MEMORY AID

MTBF = time **Between** failures (reliability); **MTTR** = time **To Repair** (recovery). **RTO** = how fast you recover; **RPO** = how much data you can lose.

OUTLINE COVERAGE — SELF-CHECK

- ☐ Security governance
- ☐ Risk management
- ☐ Third-party risk
- ☐ Compliance
- ☐ Audits & assessments
- ☐ Security awareness

Acronym & Term Quick-Reference

Security+ is acronym-dense. These appear across multiple domains — know them on sight.

CIA — Confidentiality, Integrity, Availability

AAA — Authentication, Authorization, Accounting

MFA — Multi-Factor Authentication

PKI — Public Key Infrastructure

IoC — Indicator of Compromise

APT — Advanced Persistent Threat

CVSS — Common Vulnerability Scoring System

CVE — Common Vulnerabilities & Exposures

SIEM — Security Info & Event Management

SOAR — Security Orchestration, Automation & Response

EDR/XDR — Endpoint / Extended Detection & Response

DLP — Data Loss Prevention

NAC — Network Access Control

MDM — Mobile Device Management

SPF/DKIM/DMARC — Email authentication trio

WPA3 — Wi-Fi Protected Access 3

SASE — Secure Access Service Edge

SD-WAN — Software-Defined WAN

WAF — Web Application Firewall

NGFW — Next-Generation Firewall

RTO/RPO — Recovery Time / Point Objective

MTTR/MTBF — Mean Time To Repair / Between Failures

ALE/SLE/ARO — Loss-expectancy risk formulas

SLA/MSA/SOW — Common vendor agreements

SUGGESTED STUDY PLAN

Timeframe	Focus
Weeks 1–2	Domains 1 & 5 — build the controls, governance, and risk foundation (and the risk math).
Week 3	Domain 2 (Threats, Vulnerabilities & Mitigations) — the largest threat content; drill attack-to-mitigation mapping.
Week 4	Domain 3 (Architecture) — cloud, network design, and data protection.
Weeks 5–6	Domain 4 (Security Operations, 28%) — the heaviest domain; practice PBQs on logs, firewall rules, and IAM.
Week 7	Full-length practice exams and PBQ drills; review weak areas and re-read every Memory Aid.

EXAM-DAY STRATEGY

Security+ rewards **practical judgment**. On PBQs, read the whole scenario before acting. When two answers seem right, pick the one that addresses the **immediate risk with the least disruption**. Flag hard items and return — every question is worth the same.

Rote-Fact Reference

The pure-memorization facts this exam expects you to know cold. Drill these until recall is automatic.

COMMON PORTS & PROTOCOLS

Port	Protocol	Notes
20 / 21	FTP (data / control)	Unencrypted file transfer.
22	SSH / SCP / SFTP	Secure remote access & transfer.
23	Telnet	Remote access — unencrypted (insecure).
25	SMTP	Email sending.
53	DNS	Name resolution (TCP & UDP).
67 / 68	DHCP	Dynamic IP assignment.
69	TFTP	Trivial FTP (UDP).
80	HTTP	Web (unencrypted).
88	Kerberos	Authentication.
110 / 995	POP3 / POP3S	Email retrieval / over TLS.
123	NTP	Time synchronization.
137–139	NetBIOS	Legacy Windows networking.
143 / 993	IMAP / IMAPS	Email retrieval / over TLS.
161 / 162	SNMP	Network management / traps.
389 / 636	LDAP / LDAPS	Directory services / over TLS.
443	HTTPS	Web over TLS.
445	SMB	Windows file sharing.
514	Syslog	Log collection.
3306	MySQL	MySQL database.
3389	RDP	Remote Desktop.

CONTROL FUNCTIONS

Type	Purpose
Preventive	Stops it before it happens.
Deterrent	Discourages the attempt.
Detective	Identifies during/after.
Corrective	Restores after.
Compensating	Substitute for an infeasible control.
Directive	Mandates behavior.

CRYPTOGRAPHY CHEAT SHEET

Type	Algorithms & Key Facts
Symmetric	AES (128/192/256), 3DES, ChaCha20. Fast; shared secret key; key count = n(n-1)/2.
Asymmetric	RSA (2048+), ECC (small, efficient), Diffie-Hellman (key exchange). Solves key distribution; slower.
Hashing	SHA-256/512 (current), SHA-1 & MD5 (broken). One-way; provides integrity, not secrecy.
Signatures	Sign with PRIVATE key, verify with PUBLIC key — provides integrity + non-repudiation.
Encryption	Encrypt with the recipient's PUBLIC key; they decrypt with their PRIVATE key.

EMAIL AUTHENTICATION

Record	Purpose
SPF	Lists authorized sending servers.
DKIM	Cryptographically signs the message.
DMARC	Policy for SPF/DKIM failures + reporting.

Flashcards — Cover & Recall

Cover the right column, answer each prompt aloud, then check. Repeat over several days — retrieving the answer (not re-reading it) is what moves it into long-term memory.

Prompt	Answer
Two ways to describe a control	By category (technical/managerial/operational/physical) and by function (preventive, etc.).
A compensating control is…	A substitute used when the primary control isn't feasible.
Zero Trust: who decides vs. who enforces?	Policy Engine decides; Policy Enforcement Point (PEP) enforces.
Password spraying vs. brute force	Spraying = one password vs. many users; brute force = many passwords vs. one user.
Worm vs. virus	Worm self-replicates; a virus needs the user to run it.
SPF / DKIM / DMARC roles	SPF = who can send; DKIM = signs message; DMARC = what to do on failure.
Fail-open vs. fail-closed	Fail-open favors availability; fail-closed favors security.
Inline device vs. tap	Inline can block traffic; a tap only monitors.
Tokenization vs. masking	Tokenization swaps data for a vault-mapped token; masking just hides characters.
IR lifecycle order	Prepare, detect, analyze, contain, eradicate, recover, lessons learned.
CVSS vs. CVE	CVSS = severity score (0–10); CVE = the specific vulnerability ID.
SIEM vs. SOAR	SIEM correlates & alerts on logs; SOAR automates the response.
Ports: HTTP / HTTPS	80 / 443.
Ports: SSH / RDP	22 / 3389.
Ports: DNS / DHCP	53 / 67–68.
Ports: LDAP / LDAPS	389 / 636.
RTO vs. RPO	RTO = time to recover; RPO = acceptable data loss.
MTBF vs. MTTR	MTBF = time between failures (reliability); MTTR = time to repair (recovery).
MSA vs. SOW	MSA = master/overall terms; SOW = the specific work, scope, and timeline.

SLE / ALE formulas	SLE = AV × EF; ALE = SLE × ARO.
WPA3 replaced…	WPA2 — stronger wireless encryption and key exchange.
Recovery sites cheapest to fastest	Cold (cheap/slow), warm, hot (costly/fast).
NAC does what?	Controls device admission to the network based on posture/identity.
EDR vs. DLP	EDR = endpoint detection & response; DLP = prevents data exfiltration.

Exam Cram Sheet

Security+ distilled to the must-memorize essentials — your final-review sheet. If you can recall every line here from memory, you are ready.

CONTROL CATEGORIES

- Technical, Managerial,
- Operational, Physical

CONTROL FUNCTIONS

- Preventive, Deterrent, Detective,
- Corrective, Compensating, Directive

PORTS: LOW

- 20/21 FTP, 22 SSH, 23 Telnet
- 25 SMTP, 53 DNS, 67/68 DHCP
- 69 TFTP, 80 HTTP, 88 Kerberos

PORTS: HIGH

- 110 POP3, 143 IMAP, 161/162 SNMP
- 389 LDAP, 443 HTTPS, 445 SMB
- 636 LDAPS, 993 IMAPS, 3389 RDP

EMAIL AUTH

- SPF = authorized sending servers
- DKIM = signs the message
- DMARC = policy on SPF/DKIM failure

CRYPTO

- Symmetric: AES, 3DES (fast, shared key)
- Asymmetric: RSA, ECC (key distribution)
- Hash: SHA-256 (integrity)
- Sign w/ private, verify w/ public

RISK & BIA

- SLE = AV × EF; ALE = SLE × ARO
- RTO = time to recover; RPO = data loss
- MTBF = reliability; MTTR = repair

IR LIFECYCLE

- Prepare → Detect → Analyze →
- Contain → Eradicate → Recover → Lessons

ZERO TRUST

- Control plane (PE/PA) decides
- Data plane (PEP) enforces
- Assume breach; verify every request

WIRELESS

- WPA3 current (SAE handshake)
- WPA2 = AES-CCMP
- Avoid WEP / WPA

AGREEMENTS

- SLA = performance targets
- MSA = master terms; SOW = the work
- MOU = intent; BPA = partnership; NDA = confidentiality

ATTACKS

- Spraying = 1 password / many users
- Brute force = many passwords / 1 user
- On-path = MITM; worm self-spreads

Free & Community Study Resources

Free and community study resources for this exam, compiled to help you actually pass. These are independent, third-party resources — IT Dojo is not affiliated with them and cannot guarantee their availability or accuracy — but each is widely used and well regarded by candidates. Always cross-check against the current official exam objectives.

FREE VIDEO TRAINING

Professor Messer SY0-701 — The complete free Security+ video course, plus monthly study groups and weekly pop quizzes.

OFFICIAL & FREE PRACTICE

CompTIA Exam Objectives — The official SY0-701 blueprint and free sample questions — anchor all study to this.

ExamCompass — Free SY0-701 practice tests organized by domain, no signup required.

QUICK REFERENCE & COMMUNITY

StationX Cheat Sheet — Free quick reference: ports, crypto, attacks, frameworks, and acronyms.

r/CompTIA — Active community with "how I passed" write-ups and study advice.

IT DOJO

Ready to earn your Security+?

IT Dojo's instructor-led Security+ boot camp delivers live expert instruction, hands-on labs, and PBQ practice that prepares your team for the exam and the job. Employer-sponsored training for DoD, federal, and corporate clients.

Course: www.itdojo.com/comptia-training/security/

Phone: 757-216-3656 | **Email:** info@itdojo.com

Hours: Monday–Friday, 8:30 AM – 4:30 PM ET

4176 South Plaza Trail, Suite 207, Virginia Beach, VA 23452