CompTIA Security+ SY0-701

Quick Exam Refresher

*This is your condensed, **high-impact review guide** for Security+ SY0-701. It's designed for **quick recall** and confidence-building right before the exam — not deep instruction.*

Security+ SY0-701 Domains

Each domain is weighted differently on the exam, with Security Operations being the largest:

- Domain 1: General Security Concepts (12%)
- Domain 2: Threats, Vulnerabilities, and Mitigations (22%)
- Domain 3: Security Architecture (18%)
- Domain 4: Security Operations (28%)
- Domain 5: Security Program Management and Oversight (20%)

Quick Reminder: How the Exam Works

- Number of Questions: Up to 90
- Format: Multiple choice + Performance-Based Questions (PBQs)
- Time Limit: 90 minutes
- Passing Score: 750/900 (about 83%)
- Test Provider: Pearson VUE (onsite or online)

Remember — you don't need to be perfect to pass!

The Security+ passing score is about **83%**. That means you **can miss around 15–16 questions out of 90** and still pass!

Domain 1: General Security Concepts (12%)

CIA Triad – Confidentiality, Integrity, Availability (ensure authorized access, prevent tampering, and guarantee uptime)

AAA – Authentication, Authorization, Accounting (prove identity, define access, log activity)

Non-Repudiation – Digital signatures prove a user took an action

Zero Trust – No user or device is trusted by default; always verify

Change Management – Approve/test/track changes to reduce risk

Security Controls

- Preventive: stop incidents (e.g., firewall)
- Detective: find incidents (e.g., IDS)
- Corrective: recover from incidents (e.g., restore backups)
- Deterrent: discourage attacks (e.g., warning banners)
- Compensating: backup controls if primary fails

Control Categories

- Technical (e.g., encryption)
- Administrative (e.g., training, policies)
- Physical (e.g., locks, cameras)

Basic Crypto

- Symmetric (AES): same key for encryption/decryption
- Asymmetric (RSA): public/private keys
- Hashing (SHA-256): data fingerprint for integrity
- PKI: trust model with certificates, CA, CRL, OCSP

Domain 2: Threats, Vulnerabilities, and Mitigations (22%)

Threat Actors

- Nation-states (APT groups), organized crime (ransomware gangs), insiders (malicious/disgruntled employees), hacktivists (political motives), script kiddies (unskilled attackers)

Common Attacks

- **Social Engineering:** Phishing (email), Vishing (phone), Smishing (SMS)
- **Malware:** Virus, Worm, Trojan, Ransomware, Rootkit, Keylogger, Spyware
- **Web-Based Attacks:** XSS (client-side script injection), SQLi (database manipulation), CSRF (forces authenticated users to act)
- **Network-Based Attacks:** MITM (Man-in-the-Middle), DNS poisoning, ARP spoofing, DoS/DDoS
- **Password Attacks:** Brute force, spraying, rainbow tables, dictionary

Vulnerabilities

- Misconfigurations, unpatched software, default credentials
- Cloud: exposed S3 buckets, lax IAM roles, VM escape
- Zero-day: unknown and unpatched flaws

Indicators of Compromise (IOC)

- CPU/memory spikes, unauthorized processes, outbound traffic to suspicious IPs, unexpected encryption of files, disabled AV/logging

Mitigations

- Network segmentation, strong ACLs, IDS/IPS deployment, allowlisting apps, frequent patching, security awareness training, multi-factor authentication (MFA), sandboxing for file analysis

Forensics & Investigations

- Chain of Custody: Document handling of evidence
- Order of Volatility: RAM > processes > disk > backups
- Imaging: Work on forensic copy, not original
- Sources: Logs, NetFlow, packet captures, memory dumps

Domain 3: Security Architecture (18%)

Architecture Types

- Deployment types: On-Premises, Cloud (IaaS = most control, SaaS = least control), Hybrid
- Structural styles: Centralized (data center-focused) vs. Decentralized (edge computing)
- Application environments: Containers (Docker), Microservices, Serverless (e.g., AWS Lambda)

Shared Responsibility Model

- Cloud provider secures hardware/network/infrastructure
- Customer secures data, identities, apps, configurations

Network Design

- Segmentation with VLANs/subnets, DMZ for public-facing services
- Firewalls (stateful/NGFW), WAFs for HTTP traffic, IDS/IPS for detection/blocking
- NAC enforces endpoint security posture before access
- Secure VPNs (IPSec, SSL-VPN) for remote access

Wireless Security

- **WPA3**: Strongest current encryption standard
- Enterprise authentication: **802.1X with RADIUS**
- Disable WPS (vulnerable auto-connect feature)

Data Protection

- **States:** At Rest (disk), In Transit (TLS), In Use (RAM)
- **Methods:** Encryption, Tokenization, Hashing (SHA-256), Masking (partial display)
- Data Classification: Public, Private, Confidential, Top Secret

Resilience and Redundancy

- RAID for disk redundancy, Clustering for failover, Load Balancing for uptime
- Power: UPS and generators

Disaster Recovery & Backups

- Sites: Hot (live), Warm (ready, delayed), Cold (infrastructure only)
- Backups: Full (entire set), Incremental (since last backup), Differential (since full), Snapshot (point-in-time)

Domain 4: Security Operations (28%)

System Hardening

- Disable unused ports/services
- Apply secure configurations and baselines
- Enforce patching, strong password policies, and host firewalls

Asset Management

- Maintain up-to-date inventory of hardware/software
- Tagging, secure procurement, lifecycle tracking (acquisition to disposal)

Device Types

- IoT/embedded: Isolate, limit access, firmware updates
- Mobile: MDM, remote wipe, screen locks, encryption
- Network: Secure configurations, SNMPv3, disable unused interfaces

Vulnerability Management

- Scanners: Nessus, OpenVAS
- Types: Authenticated vs. Unauthenticated
- Remediation: Patch, replace, configure; prioritize by severity
- Pen Testing: Simulated attack (black/gray/white box)

Monitoring & Detection

- Tools: SIEM, EDR/XDR, IDS/IPS, UBA, SOAR
- FIM for change detection; DLP to prevent data exfiltration
- Analyze logs (firewall, authentication, syslog) for IOCs

Incident Response Lifecycle

1. **Preparation:** Playbooks, tools, communication
2. **Detection & Analysis:** Identify events and severity
3. **Containment:** Limit spread (disconnect systems)
4. **Eradication:** Remove malware, disable accounts
5. **Recovery:** Restore services, monitor closely
6. **Lessons Learned:** Post-mortem and improvement

Identity & Access Management (IAM)

- Models: RBAC, ABAC, MAC, DAC
- Techniques: MFA, SSO, Federation (SAML, OIDC)
- Policies: Least privilege, password lockout, access recertification

Domain 5: Security Program Management and Oversight (20%)

Governance

- Documentation hierarchy: Policies > Standards > Guidelines > Procedures
- Key Roles: CISO (strategy), Data Owner (classification), Custodian (implementation), Privacy Officer (compliance)
- Common Frameworks: NIST CSF, ISO 27001, COBIT, PCI-DSS, HIPAA, GDPR

Risk Management

- Quantitative Terms:
  - SLE = Asset Value × Exposure Factor
  - ARO = Annual frequency
  - ALE = SLE × ARO
- Recovery Metrics:
  - **RTO** – Max time to restore
  - **RPO** – Max data loss
- Response Types: Accept, Transfer, Mitigate, Avoid

Vendor & Supply Chain Risk

- Due diligence: Security reviews, questionnaires
- Agreements: SLA, NDA, BPA, MSA
- Right to audit, breach notification requirements
- Monitor vendor security postures continuously

Compliance & Auditing

- Internal and external audits
- Compliance tools and continuous monitoring
- SOC 2, ISO certs, PCI scans
- Evidence collection, attestation, legal hold

Training & Awareness

- Annual security awareness for all staff
- Phishing simulations, role-based training
- Executive support critical to drive culture
- Metrics to assess effectiveness

Common Protocols and Port Numbers

Protocol	Port(s)	Description
FTP	20/21	Insecure file transfer
SSH	22	Secure shell for remote access
Telnet	23	Insecure remote terminal access
SMTP	25	Sends email (unencrypted)
DNS	53	Domain name resolution
DHCP	67/68	Dynamic IP address assignment
TFTP	69	Lightweight file transfer (insecure)
HTTP	80	Insecure web traffic
Kerberos	88	Authentication protocol (SSO)
POP3	110	Retrieves email (unencrypted)
NTP	123	Network time synchronization
NetBIOS	137–139	Windows network naming services
IMAP	143	Email retrieval (unencrypted)
SNMP	161	Network monitoring and management
LDAP	389	Directory access (unencrypted)
HTTPS	443	Secure web traffic
SMTPS	465	Secure email sending (SMTP with SSL)
FTPS	990	Secure FTP (FTP over SSL)
IMAPS	993	Secure IMAP email access
POP3S	995	Secure POP3 email retrieval
RDP	3389	Remote Desktop Protocol