CompTIA Security+ SY0-701

Full Learning Guide

Welcome to your complete Security+ SY0-701 learning guide.
*This manual is designed to **teach you every domain deeply**, not just summarize.*

Learning Objectives and Expectations

We'll cover:

- Every exam objective in detail.
- Every critical concept you must know and connect together.
- How to think like a security professional, not just memorize.

Each domain guide includes:

- Full concept breakdowns.
- Real-world examples.
- Exam tips and memory tricks.

Security+ SY0-701 Domains

Each domain is weighted differently, 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)

Top 10 Security+ Exam Tips

1. **Review Lightly Before Exam:** Focus on key topics (ports, OSI layers, encryption) — no cramming new material.
2. **Get Good Sleep:** Being well-rested improves memory, speed, and focus.
3. **Arrive Early and Be Ready**: Bring two IDs, dress in layers, and double-check tech setup if testing online.
4. **Stay Calm**: Deep breaths before starting; think positively about your preparation.
5. **Skip PBQs Smartly**: Skip PBQs if they're time-consuming; answer multiple-choice first, then return.
6. **Manage Time**: Aim for 1 minute per question; keep moving if stuck—mark and come back.
7. **Read Questions Carefully**: Watch for keywords like BEST, NOT, FIRST, and understand exactly what's asked.
8. **Use Elimination**: Cross out wrong answers first to improve your chances when guessing.
9. **Answer Every Question**: No penalty for wrong answers—guess if needed before time runs out.
10. **Review If Time Allows**: Check flagged questions carefully, but only change answers if you're sure.

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!

Missing a few tricky questions won't ruin your chances — **stay calm**, trust your preparation, and keep moving forward.

Domain 1: General Security Concepts (12%)

Goal of Domain 1:
You must understand core security principles, security controls, risk management basics, cryptography fundamentals, and physical security.
This domain sets the foundation for everything else in cybersecurity.

1.1 Security Control Types and Categories

Learn: What is a Security Control?

- A security control is any safeguard or measure that reduces risk to assets.
- Think of it like defenses in a castle: walls, guards, moats, alarms — all are controls protecting valuables.

Categories of Controls (By implementation type)

1. Technical (Logical)

- Technology-based controls.
- Examples:
  - Firewalls
  - Anti-virus software
  - Encryption
  - Intrusion Detection Systems (IDS)

2. Administrative (Managerial)

- Policies and procedures humans must follow.
- Examples:
  - Security policies (like Acceptable Use Policy)
  - Hiring practices (background checks)
  - Training programs (security awareness)

3. Physical

- Controls you can physically touch.

- Examples:
  - Locked doors
  - Security cameras
  - Fences
  - Biometrics at doors (like fingerprint access)

Functional Types of Controls (By security purpose)

1. Preventive

- *Prevents* an incident before it happens.
- Examples:
  - Firewalls blocking unauthorized traffic
  - Password policies requiring strong passwords
  - Locked doors

2. Detective

- *Detects* an incident as it happens or afterward.
- Examples:
  - Security alarms
  - Intrusion Detection Systems (IDS)
  - Audit logs

3. Corrective

- *Fixes* the damage after an incident.
- Examples:
  - Backup restoration after ransomware attack
  - Antivirus removing malware
  - Patching a vulnerability after a breach

4. Deterrent

- *Discourages* attacks by increasing perceived risk.
- Examples:
  - Warning signs ("This area under surveillance")
  - Visible security guards

5. Compensating

- *Alternative* controls when the primary control isn't feasible.
- Examples:
  - If you can't encrypt an old system’s hard drive, use strict physical security (locked room) instead.

6. Directive

- *Directs* people toward correct actions.
- Examples:
  - Signs ("No Tailgating")
  - Security awareness training

Important:
On the exam, you may be given a control and asked:

- What type is it? (Technical/Admin/Physical)
- What function is it? (Preventive/Detective/etc.)

1.2 Core Security Principles

CIA Triad

The three fundamental goals of cybersecurity:

C — Confidentiality

- Ensuring only authorized people can access information.
- Techniques: encryption, access controls, authentication.
- Example: Encrypting sensitive email to prevent eavesdropping.

I — Integrity

- Ensuring data is accurate and unaltered.
- Techniques: hashing, digital signatures, file permissions.
- Example: A checksum on a downloaded file verifies it wasn’t tampered with.

A — Availability

- Ensuring information is accessible when needed.
- Techniques: redundant systems, DDoS protection, backups.
- Example: A redundant power supply keeps a server online during power failures.

Non-Repudiation

Definition:

- Guarantee that a sender cannot deny having sent a message and the recipient cannot deny having received it.

Techniques:

- Digital signatures (proving identity and integrity)
- Logging systems

Example:

- An email digitally signed with a private key ensures proof of origin.

Important:
Expect questions asking "Which principle is affected?" when given a scenario.

1.3 AAA — Authentication, Authorization, Accounting

Authentication

Proving who you are.

- Username + password
- Biometrics (fingerprint, face)
- Smartcards
- OTP (one-time password) apps

MFA (Multi-Factor Authentication):
Use two or more different types:

- Something you know (password)
- Something you have (smartcard)
- Something you are (fingerprint)

Authorization

Defining what you can do once authenticated.

- Permissions, rights, access levels.

Example:

- A user may authenticate into a network but be authorized only to access their own files.

Accounting

Tracking actions.

- Logging user activities
- Monitoring access attempts
- Reviewing logs

Example:

- Audit logs showing who logged into the database and when.

Tip:
Think:

- Authentication — "Who are you?"
- Authorization — "What can you do?"
- Accounting — "What did you do?"

1.4 Security Posture Assessment

Gap Analysis

- Compare current security posture vs desired/best practices.
- Find "gaps" (weaknesses).
- Leads to action plans to fix gaps.

Zero Trust Architecture

Principle:

- "Never trust, always verify."

Key concepts:

- No implicit trust inside or outside the network.
- Every access request must be authenticated, authorized, and encrypted.

Important:
Expect questions where you must recognize a zero-trust principle from a scenario.

1.5 Physical Security and Safety

Learn These Physical Controls:

- Fences
- Locked doors
- Biometrics (fingerprint/face access)
- Mantraps (two doors; trap intruders)
- Bollards (posts preventing vehicle access)
- Surveillance cameras (CCTV)
- Alarm systems
- Access badges

Environmental Controls

- HVAC systems (cool servers)
- Fire suppression (gas-based systems for server rooms)
- Water detection sensors
- Temperature/humidity monitors

Tip:
Remember that protecting people, facilities, and equipment is as important as protecting data.

1.6 Deception and Disruption Techniques

Honeypots and Honeynets

- Honeypot: A fake system/device to lure attackers.
- Honeynet: A fake network of honeypots.

Goal:

- Detect attackers
- Study attack methods
- Waste attacker time

Honeyfiles

- Fake sensitive files (like "passwords.txt") to detect unauthorized access.

Important:
Honeypots = detection + research tools, NOT real asset protection.

1.7 Change Management

Why Change Management?

Goal:

- Prevent security incidents caused by careless/uncontrolled changes.

Change Control Process Steps

1. Request change.
2. Analyze impact (risk assessment).
3. Get approvals.
4. Test in safe environment.

5. Schedule deployment (usually during low-usage windows).
6. Deploy with rollback plans ready.
7. Document everything.

Real-world example:
A firewall rule change accidentally opens a vulnerable port.
Proper change management would catch this during risk analysis/testing.

Tip:
Expect exam questions describing a failure — you must recognize "lack of change management" as the cause.

1.8 Basic Cryptographic Solutions

Encryption

- Scrambles data so unauthorized people can't read it.

Two Types:

1. Symmetric encryption:

- Same key used to encrypt and decrypt.
- Examples: AES, DES.

2. Asymmetric encryption:

- Two keys: public and private.
- Examples: RSA, ECC.

Public Key Infrastructure (PKI)

Key Concepts:

- Certificates (prove identity)
- Certificate Authorities (trusted issuers)
- Certificate Revocation (CRL, OCSP)

Hashing

- One-way function to create a unique fingerprint of data.
- Used for integrity checks.
- Examples: SHA-256, SHA-3.

Digital Signatures

- Use asymmetric encryption + hashing.
- Prove:
  - Data integrity
  - Sender authenticity
  - Non-repudiation

Blockchain Basics

- A decentralized ledger.
- Uses hashing and chaining of blocks.
- Common in cryptocurrency, but useful for tamper-evident systems.

Tip:
Expect basic crypto scenario questions, e.g.,

- "Which cryptographic technique ensures integrity?" (Answer: hashing)

Summary of Domain 1

Master these:

- Categories of security controls (technical/admin/physical)
- Functional types of controls (preventive, detective, etc.)
- CIA triad + non-repudiation
- AAA (authentication, authorization, accounting)
- Zero trust principles
- Physical and environmental security measures
- Honeypots, honeynets, honeyfiles
- Change management process
- Basic cryptography concepts (symmetric/asymmetric encryption, PKI, hashing, digital signatures)

If you understand these well, you will easily handle Domain 1 questions on the Security+ SY0-701 exam.

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

Goal of Domain 2:
Understand the types of threats, how vulnerabilities are exploited, how to recognize signs of attack, and how to mitigate risks.
This is the most "attacker-focused" domain — you must "think like an attacker," recognize attacks, and know defenses.

2.1 Threat Actors and Threat Vectors

Learn: What is a Threat Actor?

Threat Actor = Person or group trying to cause harm to your system.
Different actors have different skills, resources, and motives.

Types of Threat Actors

1. Nation-State Actors

- Sponsored by governments.
- Motivation: Espionage, disruption, warfare.
- Examples: Fancy Bear (Russia), APT groups (Advanced Persistent Threats).
- Traits: Highly skilled, well-funded, stealthy.

2. Organized Crime Groups

- Cybercriminals working for money.
- Motivation: Financial gain (ransomware, theft).
- Examples: Ransomware gangs like Conti.
- Traits: Professional, use ransomware-as-a-service, phishing.

3. Hacktivists

- Activists who hack for a cause.
- Motivation: Ideology, politics, social justice.
- Examples: Anonymous group.

- Traits: Varied skill levels.

4. Insiders

- Employees, contractors, or partners.
- Motivation: Revenge, profit, carelessness.
- Traits: Already have access! Dangerous.

5. Script Kiddies

- Unskilled individuals using tools made by others.
- Motivation: Fun, fame, curiosity.
- Traits: Low sophistication, but can still cause damage.

6. Shadow IT

- Employees using unauthorized tech.
- Motivation: Convenience, speed.
- Risks: Security gaps (unknown apps, no monitoring).

Important:
Expect exam scenarios describing an attacker — you must identify the actor type based on motives and resources.

2.2 Threat Vectors (Attack Paths)

Learn: How Do Threats Reach Us?

Threat Vector = The way a threat actor gains access to a system.

Common Threat Vectors

1. Message-Based Attacks

- Phishing emails
- Smishing (SMS phishing)
- Vishing (voice phishing)

2. File-Based Attacks

- Malware hidden in documents, PDFs, executables.

3. Web-Based Attacks

- Drive-by downloads
- Malicious websites (watering hole attacks)

4. Removable Media

- USB drives with malware
- Rogue devices

5. Supply Chain Compromise

- Infected software updates
- Compromised hardware vendors

6. Network-Based Attacks

- Eavesdropping (sniffing)
- Man-in-the-Middle attacks (MITM)

Real-World Tip:
Attackers often combine vectors — phishing email → malware download → remote access.

Mnemonic:
"Messages, Files, Websites, Devices, Vendors, Networks." — MFWDVN.

2.3 Vulnerabilities

Learn: What is a Vulnerability?

Vulnerability = Weakness or flaw that can be exploited.

Common Vulnerability Categories

1. Application Vulnerabilities

- SQL Injection
- Cross-Site Scripting (XSS)
- Buffer Overflows
- Race Conditions (TOC/TOU)

2. OS Vulnerabilities

- Unpatched software
- Privilege escalation flaws
- Outdated/unsupported systems

3. Hardware/Firmware Vulnerabilities

- Default passwords
- Unpatched firmware
- Physical device tampering

4. Virtualization/Cloud Vulnerabilities

- VM escape
- Misconfigured cloud storage (public S3 buckets)

5. Configuration Weaknesses

- Default settings left active
- Overly permissive firewall rules
- Open ports/services

6. Zero-Day Vulnerabilities

- Unknown to vendor, no patch available yet.
- Most dangerous.

Tip:
When you see a scenario about poor configurations, unpatched systems, or mismanaged cloud — it's a vulnerability problem.

2.4 Indicators of Malicious Activity (IOC - Indicators of Compromise)

Learn: How to Recognize an Attack

Common Indicators

- Unusual outbound traffic (data exfiltration)
- High CPU/memory usage (crypto miners, malware)
- Unknown running processes/services (malware persistence)
- Strange account behavior (account compromise)
- Unauthorized changes (rootkits, insider activity)
- Disabled security tools (antivirus, logging disabled)

Malware Types to Know

1. Virus

- Attaches to files, spreads when opened.

2. Worm

- Spreads itself across networks automatically.

3. Trojan Horse

- Pretends to be legitimate software.

4. Ransomware

- Encrypts files, demands payment.

5. Rootkit

- Hides deep in system (kernel level).

6. Spyware

- Secretly collects user data.

7. Logic Bomb

- Malicious code that activates on trigger.

8. Keylogger

- Captures keystrokes.

Attack Techniques to Know

- DDoS — Flood network/services to crash them.
- DNS Poisoning — Redirect users to fake sites.
- ARP Poisoning — Redirect network traffic.
- Password Attacks:
  - Brute Force (try all passwords)
  - Dictionary Attack (try wordlist)
  - Password Spraying (few passwords against many accounts)

Important:
You must recognize an attack from symptoms in exam scenarios.

2.5 Mitigation Techniques

Learn: How to Defend Against Threats

Common Mitigations

1. Network Segmentation

- Divide network into smaller zones.
- Stop malware spread.

2. ACLs (Access Control Lists)

- Firewall rules: Allow/block based on IP, port, protocol.

3. Patch Management

- Regular updates for OS, apps, firmware.

4. Application Allowlisting

- Only approved programs can run.

5. Isolation and Sandboxing

- Open untrusted files in controlled environment.

6. Encryption

- Protect data at rest and in transit.

7. Monitoring and Detection

- IDS/IPS systems
- SIEM tools (log aggregation and analysis)

8. Least Privilege Enforcement

- Users/systems only get necessary access.

9. Configuration Management

- Baseline secure configs
- Regular reviews

10. Incident Response Plans

- Be ready to respond fast (covered deeply in Domain 4).

Tip:
On the exam, if asked "How can you mitigate XYZ?", think:
Isolate → Monitor → Patch → Restrict Access.

Summary of Domain 2

You must master:

- Different types of threat actors (and their motivations)
- Threat vectors (ways attacks happen)
- Common vulnerabilities (application, OS, cloud, config)
- Recognizing indicators of compromise (malware symptoms)
- Malware types and attack techniques
- Best mitigation strategies (segmentation, patching, least privilege, monitoring)

If you understand Domain 2 well, you will dominate all "attack scenario" and "mitigation recommendation" questions on the Security+ SY0-701 exam.

Domain 3: Security Architecture (18%)

Goal of Domain 3:
Understand how to design secure systems and networks, choose the right security tools, manage data protection, and ensure resilience and availability.

In this domain, you move from individual attacks (Domain 2) to building strong defenses and secure environments.

3.1 Architecture Models and Concepts

Learn: Different Ways to Architect Systems and Their Security Impacts

---

Deployment Models

1. On-Premises

- Systems hosted in organization-owned buildings.
- Pros: Full control.
- Cons: High upfront cost, ongoing maintenance.

2. Cloud Computing

- Systems hosted by cloud providers (AWS, Azure, etc.)
- Models:
  - IaaS (Infrastructure as a Service): You control OS and apps (e.g., AWS EC2).
  - PaaS (Platform as a Service): Provider manages OS, you manage apps (e.g., Heroku).
  - SaaS (Software as a Service): Provider manages everything, you just use app (e.g., Gmail).

3. Hybrid

- Mix of on-premises and cloud.
- Challenge: Securing data across both environments.

Key Concept:
Understand the Shared Responsibility Model:

- Cloud provider: responsible for security *of* the cloud (hardware, infra).
- You (customer): responsible for security *in* the cloud (your apps, data).

Architectural Approaches

1. Centralized vs. Decentralized

- Centralized = Single data center.
- Decentralized = Many smaller nodes (e.g., edge computing).
- Security Challenge: Decentralized = wider attack surface.

2. Virtualization

- Running multiple VMs on a single physical server.
- Security Concern: Hypervisor attacks (VM escape).

3. Containers and Microservices

- Lightweight virtualized apps (Docker, Kubernetes).
- Security Focus: Secure container images, limit container privileges.

4. Infrastructure as Code (IaC)

- Manage servers, networks via scripts (Terraform, CloudFormation).
- Security Risk:
  - A misconfigured template could cause widespread vulnerabilities fast.

Example Scenario Tip:
If a question mentions IaC misconfiguration, it's about configuration drift or mass vulnerabilities.

Special Environments

1. Serverless (Function-as-a-Service)

- You just upload code; no server management (e.g., AWS Lambda).
- Security Focus:
  - Securing code and event triggers.

2. Embedded/IoT Systems

- Devices like cameras, sensors, medical devices.
- Security Challenge:
    - Often lack strong built-in security.
    - Hard to patch/update.

3. Industrial Control Systems (ICS) and SCADA

- Control physical processes (power plants, factories).
- Security Risk:
    - Nation-state threats.
    - Downtime = Life-threatening risks.

Tip:
When ICS/SCADA are involved, always think:

- Segmentation
- Physical security
- Minimal internet exposure

3.2 Securing Enterprise Infrastructure

Learn: How to Build a Strong Internal Security Framework

Network Design Principles

1. Segmentation

- Breaking the network into pieces (e.g., VLANs, subnets).
- Goal: Limit spread of breaches.

2. DMZ (Demilitarized Zone)

- Buffer zone between internal and external networks.
- Hosts public services (web servers) isolated from internal assets.

3. Secure Network Topology

- Internal network > DMZ > Internet.
- Extra firewalls between departments (HR, finance separated).

Device Placement

- Firewalls: At network boundaries and between zones.
- IDS/IPS Sensors: At critical network chokepoints.
- Load Balancers: To distribute traffic for availability.
- VPN Gateways: At network edges for remote users.

Real-World Tip:
Expect questions asking where to place security devices for max protection.

Secure Network Access

1. Firewalls

- Packet filtering, stateful inspection, deep packet inspection.
- Next-Gen Firewalls (NGFW): Add layer 7 (application-level) filtering.

2. VPNs (Virtual Private Networks)

- Encrypt remote user traffic into network.
- Protocols: IPSec, SSL/TLS.

3. NAC (Network Access Control)

- Health-check devices before allowing network access.
- Example: Must have antivirus and updated OS.

Important:
NAC = “Don’t trust devices blindly.”

Secure Protocols

- SSH: Secure shell for remote admin (replaces Telnet).
- HTTPS: Encrypted web traffic.

- SFTP/FTPS: Secure file transfer.
- TLS: Replaces SSL for encryption.

Wireless Security

- Use WPA3 (or WPA2 Enterprise if WPA3 unavailable).
- Implement 802.1X (RADIUS authentication).
- Disable WPS (it’s insecure).
- Monitor for rogue access points.

Wireless Tip:
Best wireless security =

- WPA3 +
- 802.1X (certs or username/password login) +
- MAC filtering (optional)

3.3 Data Protection Strategies

Learn: How to Protect Data Throughout Its Life

Data States

1. At Rest

- Stored on hard drives, databases, cloud storage.
- Protect with: Disk encryption, access controls.

2. In Transit

- Moving across networks.
- Protect with: TLS, VPNs, IPSec tunnels.

3. In Use

- Being processed in RAM.

- Protect with: Secure enclaves, memory protection.

Data Classification

- Label data based on sensitivity:
    - Public
    - Internal Use Only
    - Confidential
    - Highly Confidential (e.g., PII, HIPAA data)

Tip:
Exam may ask: "What classification would customer credit card data be?"
Answer: Highly confidential.

Roles in Data Management

- Data Owner: Sets policies (executive level).
- Data Steward/Custodian: Implements policies (IT/security teams).

Techniques for Protecting Data

- Encryption (AES for files, TLS for traffic).
- Hashing (integrity checking, not encryption!).
- Masking (hide sensitive parts, e.g., show only last 4 digits of SSN).
- Tokenization (replace sensitive data with non-sensitive substitutes).

Special Concepts

- Data Sovereignty: Data must stay within legal jurisdiction (important in cloud setups).
- Obfuscation Techniques:
    - Steganography (hiding data inside files)
    - Code obfuscation (making software harder to reverse-engineer)

3.4 Resilience and Redundancy

Learn: How to Ensure Systems Stay Up During Problems

Redundancy Principles

- Redundant Power:
  - UPS batteries
  - Backup generators.
- Redundant Network Links:
  - Multiple ISPs
  - Multi-path routing.
- Redundant Servers/Storage:
  - Clustering servers (failover)
  - RAID arrays for storage.

Backup Strategies

- Full Backup: Everything.
- Incremental Backup: Changes since last backup.
- Differential Backup: Changes since last full backup.

Example Tip:
Incremental = Faster backup, slower restore.
Differential = Slower backup, faster restore.

Disaster Recovery Sites

1. Hot Site

- Fully functional copy.
- Near-instant failover.

2. Warm Site

- Partially ready, needs config.

3. Cold Site

- Empty location, just building/electricity.

Important:
Cost vs speed of recovery!
Hot site = expensive but fast.
Cold site = cheap but slow.

Business Continuity

- BCP (Business Continuity Plan):
  - Keep critical functions running.
- DRP (Disaster Recovery Plan):
  - Restore IT services after disaster.

Testing

- Tabletop Exercises: Walkthroughs with decision-makers.
- Simulation Exercises: Full or partial drills.

Tip:
Expect questions on which type of backup or disaster recovery site suits a business scenario.

Summary of Domain 3

You must master:

- Cloud, on-prem, hybrid deployment models
- Shared responsibility in cloud
- Segmentation, DMZs, secure topology
- Proper device placement (firewalls, VPNs, IDS/IPS)
- Secure protocols (SSH, TLS, SFTP)
- Wireless security (WPA3, 802.1X)
- Data protection at rest, in transit, in use
- Data classification, encryption, tokenization, masking
- Redundancy, backup types, disaster recovery sites
- Business continuity planning

Domain 4: Security Operations (28%)

Goal of Domain 4:
Learn how security is applied daily in organizations:

- Hardening systems
- Managing vulnerabilities
- Monitoring for threats
- Responding to incidents
- Managing identities and automation.

This domain is the *biggest* on the exam.

4.1 Security Administration on Computing Resources

Learn: How to Secure Devices, Systems, and Networks

System Hardening Techniques

1. Secure Baselines

- A baseline is the secure configuration state.
- Example:
    - Disable unused ports.
    - Set minimum password lengths.
    - Install essential patches.

Hardening Endpoints (Workstations, Servers)

- Disable unnecessary services (e.g., FTP, Telnet).
- Enforce strong password policies.
- Install and maintain antivirus.
- Enable host-based firewalls (Windows Defender Firewall, UFW on Linux).
- Regularly update OS and apps.

Hardening Mobile Devices

- Use Mobile Device Management (MDM).
- Enforce encryption (e.g., full device encryption on phones).
- Require PINs or biometrics.
- Enable remote wipe capabilities.
- Separate work/personal data (containerization).

Hardening Network Devices

- Change default usernames/passwords.
- Encrypt management traffic (SSH, SNMPv3).
- Disable unused ports and services.
- Use secure protocols only.
- Regularly update firmware.

Hardening Embedded/IoT Devices

- Change default passwords.
- Update firmware frequently.
- Isolate devices on their own network/VLAN.
- Monitor network traffic for anomalies.

Real-World Tip:
IoT and embedded devices are major risks because vendors often stop updating them.

4.2 Asset Management and Lifecycle

Learn: How to Manage What You Own

Asset Inventory

- Maintain an up-to-date list of all hardware and software assets.
- Use asset tags, serial numbers, and inventory software.

Asset Lifecycle Phases

1. Procurement: Evaluate security before purchase.
2. Deployment: Configure securely before use.
3. Maintenance: Update, monitor, and patch.
4. Decommissioning: Properly wipe and destroy data.

Secure Disposal Techniques

- Clearing: Overwriting data (e.g., formatting a drive).
- Purging: Multiple overwrites, Degaussing (magnetic erase).
- Destroying: Physically destroying the drive (shredding).

Tip:
Expect questions where a company throws away computers without wiping — recognize it as data exposure risk.

4.3 Vulnerability Management

Learn: How to Find and Fix Weaknesses

Vulnerability Scanning

- Use scanners (e.g., Nessus, OpenVAS) to find missing patches, misconfigs.
- Types:
  - Authenticated Scan: Access to inside info (more accurate).
  - Unauthenticated Scan: Simulates external attacker's view.

Managing Vulnerabilities

1. Identify vulnerabilities (scans, threat intel).
2. Assess risk (likelihood × impact).

3. Prioritize fixes (critical first).
4. Remediate (patch, reconfigure, replace).
5. Verify fixes.

Penetration Testing vs Vulnerability Scanning

- Penetration Test: Actively exploiting weaknesses.
- Vulnerability Scan: Listing weaknesses without exploiting.

Important:
Pen tests need written authorization (rules of engagement).

Patch Management

- Schedule regular updates.
- Test patches before deployment.
- Emergency patching for critical vulnerabilities (zero-days).

4.4 Security Monitoring, Alerting, and Analysis

Learn: How to Watch and Respond to Threats

SIEM (Security Information and Event Management)

- Aggregates logs from many sources.
- Correlates events to detect threats.

Common Data Sources

- Firewall logs
- IDS/IPS alerts
- OS logs (Windows Event Viewer, Linux syslog)

- Authentication logs
- Application logs (web servers, databases)

Detective Technologies

- IDS (Intrusion Detection System): Detects and alerts.
- IPS (Intrusion Prevention System): Detects and blocks.

Security Tools

- EDR (Endpoint Detection and Response): Detect threats at endpoints.
- UBA (User Behavior Analytics): Detects unusual user activities.
- DLP (Data Loss Prevention): Prevents sensitive data leaks.
- Honeytokens: Fake data to catch attackers.

Performance Monitoring

- Watch for unexpected CPU/memory/network usage.
- Baseline normal behavior to detect anomalies.

Tip:
If an alert shows massive data upload at midnight, it could indicate exfiltration.

4.5 Identity and Access Management (IAM)

Learn: How to Manage Users and Access Rights

Authentication Methods

- Passwords
- MFA (Multi-Factor Authentication)
- Smartcards

- Biometrics (fingerprints, facial recognition)

Authentication Protocols

- Kerberos: Secure network authentication.
- LDAP/LDAPS: Directory services.
- SAML/OAuth2/OIDC: Federation (login with external identities).

Access Control Models

1. DAC (Discretionary Access Control)

- Owner controls access (Windows file permissions).

2. MAC (Mandatory Access Control)

- Strict policies enforced by system (e.g., government classification).

3. RBAC (Role-Based Access Control)

- Access based on user roles (e.g., "Finance" role).

4. ABAC (Attribute-Based Access Control)

- Access based on user and resource attributes.

Important:
Understand least privilege and need-to-know.

Privileged Account Management

- Separate admin and user accounts.
- Monitor admin activities.
- Use password vaults for shared credentials.

Account Policies

- Strong password policies (length > complexity).
- Lockout after failed attempts.
- Password expiration (though NIST now says longer passwords are better than frequent changes).

Tip:
NIST 800-63B recommends long passphrases, NOT constant password changes unless suspected compromise.

4.6 Automation and Orchestration

Learn: How Automation Helps Security

Why Automate?

- Faster response times.
- Consistency in actions.
- Scalability (handling lots of data and events).

Examples of Automation

- Auto-deploy patches (automated patch management).
- Auto-quarantine infected machines (SOAR platforms).
- Auto-revoke access after termination.

DevSecOps

- Integrate security into DevOps pipelines.
- Example: Static code analysis tools in CI/CD pipelines.

Important:
Automation reduces human error but needs careful oversight.

4.7 Incident Response (IR)

Learn: How to Handle Security Incidents

IR Process Steps

1. Preparation: Plans, tools, team.
2. Detection and Analysis: Identify incidents.
3. Containment: Limit the spread.
4. Eradication: Remove the threat.
5. Recovery: Restore normal operations.
6. Lessons Learned: Improve for next time.

IR Plans

- Identify who to contact.
- Communication plans (including law enforcement if needed).
- Clear escalation paths.

Containment Strategies

- Disconnect infected systems.
- Revoke compromised credentials.
- Disable malicious accounts.

Tip:
Containment first, then eradication. Stop bleeding before healing.

4.8 Digital Forensics and Investigations

Learn: Basics of Forensic Investigations

Evidence Handling

- Chain of Custody: Document who handled evidence, when.
- Imaging Drives: Work from forensic copies, never originals.
- Order of Volatility: Collect volatile evidence first (RAM, network connections).

Common Data Sources for Investigation

- Firewall logs
- Server event logs
- Email headers
- Memory dumps
- Hard disk images

Forensic Analysis

- Identify attack vectors.
- Timeline events.
- Document findings clearly for legal processes.

Tip:
If you touch evidence without logging it, chain of custody is broken — evidence may be invalid in court.

Summary of Domain 4

You must master:

- How to harden systems, networks, mobile/IoT devices
- Asset lifecycle: procurement to destruction
- Vulnerability scanning, patch management, pen testing
- SIEM, IDS/IPS, security monitoring tools
- IAM: authentication, access control models, privileged accounts
- Automation and DevSecOps basics
- Full incident response process
- Basics of digital forensics and evidence handling

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

Goal of Domain 5:
Understand how security is managed at the organizational level — governance, risk, compliance, vendor management, training, and audits.

Think: How to build and maintain a full security program, not just respond to threats.

5.1 Security Governance

Learn: Policies, Frameworks, and Roles

Policies, Standards, Guidelines, Procedures

1. Policies

- High-level rules and intentions.
- Example: "All company laptops must use encryption."

2. Standards

- Mandatory specific rules.
- Example: "Use AES-256 encryption on all laptops."

3. Guidelines

- Recommendations, not mandatory.
- Example: "It’s recommended to back up important data daily."

4. Procedures

- Step-by-step instructions.
- Example: "How to enable BitLocker on Windows 11."

Tip:
Policy = "What."
Standard = "Specific How."
Guideline = "Suggested Best Practice."
Procedure = "Step-by-Step Instructions."

Common Security Policies

- Acceptable Use Policy (AUP)
- Data Classification Policy
- Incident Response Policy
- Password Policy
- Remote Access Policy

Real-World Tip:
Many breaches happen because users ignore or don’t know the policies.

Security Frameworks and Regulations

1. NIST Cybersecurity Framework (CSF)

- Functions: Identify, Protect, Detect, Respond, Recover.

2. ISO 27001

- International standard for information security management systems (ISMS).

3. GDPR (General Data Protection Regulation)

- Protects EU citizens’ personal data.

4. HIPAA (Health Insurance Portability and Accountability Act)

- Protects US healthcare data.

5. PCI DSS (Payment Card Industry Data Security Standard)

- Protects payment card data.

Important:
On the exam, recognize which framework or law applies based on a scenario.

Key Security Roles

- CISO (Chief Information Security Officer): Leads security strategy.
- Data Owner: Classifies and decides use of data.
- Data Custodian: Implements and maintains protection.
- Privacy Officer: Ensures compliance with privacy laws.

Tip:
Owners = strategic decisions; Custodians = technical implementations.

5.2 Risk Management

Learn: How to Identify, Assess, and Respond to Risks

Risk Concepts

- Asset: Anything valuable (data, hardware, reputation).
- Threat: Anything that can cause harm.
- Vulnerability: Weakness a threat can exploit.
- Risk: Threat exploiting a vulnerability.

Formula:
Risk = Likelihood × Impact

Risk Assessment

1. Qualitative Risk Assessment

- Use ratings (high, medium, low).

2. Quantitative Risk Assessment

- Use numbers:
  - Single Loss Expectancy (SLE) = Asset Value × Exposure Factor
  - Annual Rate of Occurrence (ARO)
  - Annual Loss Expectancy (ALE) = SLE × ARO

Example:

- Asset = $100,000 server
- Exposure Factor = 50% loss per attack → SLE = $50,000
- ARO = 0.2 (attack happens every 5 years)
- ALE = $50,000 × 0.2 = $10,000

Risk Responses

- Mitigate: Add controls (e.g., firewall).
- Avoid: Don't engage in risky activity.
- Transfer: Buy insurance or outsource.
- Accept: Acknowledge risk, do nothing if low.

Important:
Expect questions where you must choose the best risk response based on a scenario.

Risk Appetite and Tolerance

- Appetite: How much risk an org is willing to take.
- Tolerance: How much deviation is acceptable.

Real-World Tip:
Risk appetite shapes security budgets.

5.3 Third-Party Risk Management

Learn: How to Manage Vendor Security Risks

Vendor Due Diligence

- Security questionnaires
- Site visits
- Review of certifications (e.g., ISO 27001, SOC 2)

Contracts and Agreements

- SLA (Service Level Agreement): Uptime and support expectations.
- MOU/MOA (Memorandum of Understanding/Agreement): Friendly cooperation agreements.
- NDA (Non-Disclosure Agreement): Protect confidential info.
- BPA (Business Partnership Agreement): Formal partnership rules.

Ongoing Monitoring

- Annual security reviews.
- Audit rights in contracts.
- Breach notification clauses.

Tip:
Cloud providers (e.g., AWS, Azure) must be evaluated carefully — shared responsibility model applies.

5.4 Security Compliance

Learn: How Organizations Follow Laws and Standards

Internal vs. External Compliance

- Internal: Following own policies and standards.
- External: Following laws, regulations, industry requirements.

Audits and Assessments

- Internal Audits: Done by internal teams.
- External Audits: Done by third-party firms.

Reporting

- Compliance reports
- Audit findings
- Certifications (e.g., ISO 27001 certification)

Important:
Non-compliance can lead to:

- Legal fines
- Lawsuits
- Reputational damage

5.5 Security Auditing and Testing

Learn: How to Verify Security Measures

Types of Tests

- Vulnerability Assessment: Scan and find weaknesses.
- Penetration Testing: Actively try to exploit vulnerabilities.
- Security Audits: Compare current practices to standards.

Penetration Test Phases

1. Reconnaissance (Passive/Active Info Gathering)
2. Scanning and Enumeration
3. Gaining Access (Exploitation)
4. Maintaining Access (Persistence)
5. Covering Tracks

Red Team vs. Blue Team vs. Purple Team

- Red Team: Attackers (simulate real-world attacks).
- Blue Team: Defenders (monitor and respond).
- Purple Team: Cooperative team that helps both red and blue improve.

Rules of Engagement

- Written authorization required before pen test starts.
- Define scope, methods allowed, hours of operation.

Tip:
Never start a penetration test without legal permission!

5.6 Security Awareness and Training

Learn: How to Educate and Train Users

User Training

- Recognize phishing emails.
- Create strong passwords (passphrases recommended).
- Protect physical security (no tailgating).
- Report suspicious activity immediately.

Executive Support

- Leadership must back security training efforts.

Training Frequency

- New hire onboarding.
- Annual refreshers.
- Targeted training after incidents.

Measuring Effectiveness

- Phishing simulations.
- Quiz/test results.
- Incident rates (human-caused).

Important:
Security training must be ongoing — one-time training is not enough.

Summary of Domain 5

You must master:

- Policies, standards, procedures, frameworks (NIST, ISO, GDPR)
- Roles (CISO, Data Owner, Custodian)
- Risk identification, qualitative and quantitative analysis
- Risk responses (mitigate, accept, transfer, avoid)
- Vendor management (due diligence, contracts, monitoring)
- Compliance (internal and external audits)
- Security auditing, vulnerability scanning, pen testing
- User security training, phishing simulations, executive support

Terms and Definitions

Security Concepts

- **CIA Triad** – Confidentiality, Integrity, Availability
- **AAA** – Authentication, Authorization, Accounting
- **Non-Repudiation** – Ensures sender cannot deny an action (via digital signatures)
- **Zero Trust** – "Never trust, always verify" model for all users and devices
- **Least Privilege** – Users get minimum access required to do their job
- **Separation of Duties** – Split responsibilities among multiple people
- **Defense in Depth** – Layered security controls throughout the system
- **Due Care** – Doing what's expected to protect assets
- **Due Diligence** – Performing risk assessments and threat analysis proactively

Access Control Models

- **DAC (Discretionary Access Control)** – Owner assigns access rights
- **MAC (Mandatory Access Control)** – System enforces access based on labels/classifications
- **RBAC (Role-Based Access Control)** – Access granted based on user roles
- **ABAC (Attribute-Based Access Control)** – Access granted based on attributes (e.g., location, time)

Control Types & Categories

- **Technical Controls:** Firewalls, antivirus, encryption
- **Administrative Controls:** Policies, training, hiring practices
- **Physical Controls:** Locks, cameras, guards
- **Preventive Controls:** MFA, access control
- **Detective Controls:** IDS, logs, audits
- **Corrective Controls:** Backups, patching
- **Deterrent Controls:** Signs, warnings
- **Compensating Controls:** Alternative security if primary is not feasible

Security Roles

- **CISO:** Strategic security leader
- **Data Owner:** Determines data classification
- **Data Steward/Custodian:** Maintains/implements security
- **Privacy Officer:** Ensures compliance with privacy laws
- **System Administrator:** Manages system configs and access

Attack Categories

- **Reconnaissance:** OSINT, scanning
- **Exploitation:** Buffer overflows, SQLi
- **Persistence:** Backdoors, rootkits
- **Command and Control (C2):** External access channels
- **Exfiltration:** Data theft via FTP, DNS tunneling

Authentication Factors

- **Something you know** – Password or PIN
- **Something you have** – Smartcard, security token
- **Something you are** – Biometrics (fingerprint, retina)
- **Somewhere you are** – Geolocation/IP address
- **Something you do** – Behavioral biometrics (typing, movement)

Risk Management Terms

- **SLE (Single Loss Expectancy)** – Cost of one loss (Asset Value × Exposure Factor)
- **ARO (Annual Rate of Occurrence)** – How often an event is expected to occur annually
- **ALE (Annual Loss Expectancy)** – Yearly expected loss (SLE × ARO)
- **RPO (Recovery Point Objective)** – Maximum acceptable data loss
- **RTO (Recovery Time Objective)** – Maximum time to restore service
- **MTTR (Mean Time to Repair)** – Average time to repair a system
- **MTBF (Mean Time Between Failures)** – Average time between system failures

Incident Response Phases

1. Preparation
2. Detection & Analysis
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Backup Types

- **Full Backup** – Copies everything
- **Incremental Backup** – Since last backup
- **Differential Backup** – Since last full backup
- **Snapshot** – Instant point-in-time image

Disaster Recovery Sites

- **Hot Site** – Fully equipped and live
- **Warm Site** – Ready with partial setup
- **Cold Site** – Basic infrastructure only

Cryptography

- **Symmetric Encryption** – One key (AES, DES)
- **Asymmetric Encryption** – Public/private key pairs (RSA, ECC)
- **Hashing** – One-way function for data integrity (SHA-256, SHA-3)
- **PKI (Public Key Infrastructure)** – Uses CA, CRL, OCSP for certificate lifecycle
- **Digital Signature** – Verifies authenticity and integrity
- **Salting** – Adding random value to passwords before hashing
- **Tokenization** – Replace sensitive data with non-sensitive placeholders

Acronyms and Tools

- **SIEM** – Security Information and Event Management
- **DLP** – Data Loss Prevention
- **EDR/XDR** – Endpoint/Extended Detection and Response
- **FIM** – File Integrity Monitoring
- **SOAR** – Security Orchestration, Automation & Response
- **MDM** – Mobile Device Management
- **NAC** – Network Access Control
- **IDS/IPS** – Intrusion Detection/Prevention Systems
- **SAML** – Security Assertion Markup Language (SSO)
- **OAuth/OIDC** – Authorization protocols for web/cloud apps
- **PBQ** – Performance-Based Question (interactive exam question)
- **UEBA/UBA** – User and Entity Behavior Analytics
- **ACL** – Access Control List
- **VPN** – Virtual Private Network
- **TLS** – Transport Layer Security
- **RAID** – Redundant Array of Independent Disks
- **CRL** – Certificate Revocation List
- **OCSP** – Online Certificate Status Protocol

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