Security+

EXAM PREP EDITION 2025

25-PAGE VISUAL

For Exam Success | SY0-701 | All 5 Domains Covered

D1	D2	D3	D4	D5
General Security Concepts	Threats,Vuln & Mitigations	Security Architecture	Security Operations	Governance,Risk & Compliance

90 min	90 Qs	750/900	5 Domains
Exam Duration	Question Count	Passing Score	Coverage

DOMAINS COVERED: General Security Concepts • Threats, Vulnerabilities & Mitigations
Security Architecture • Security Operations • Governance, Risk & Compliance

Study smart. Pass faster.

This cheat sheet distills **all five Security+ SY0-701 domains** into 25 visual pages. Use it alongside your study materials for rapid recall and exam-day confidence.

■ RECOMMENDED STUDY PLAN

First Pass (Week 1–2)	Active Recall (Week 3–4)	Exam Sprint (Final Week)
Step 1	**Step 2**	**Step 3**
Read each page end-to-end. Don't memorize yet — build familiarity. Highlight concepts you don't recognise and flag them for deeper study.	Cover the details; study just the diagrams. Ask: what does each shape/arrow mean? Use the colour-coding to reinforce domain separation in your memory.	Use the page-25 rapid-recall tables daily. Re-read Exam Tip callouts. Do a timed 90-question mock exam, then return here to patch weak spots.

■ DOMAIN COLOUR KEY

■ ICON & CALLOUT LEGEND

EXAM TIP	High-yield exam topic — memorise this!
■ WARNING	Common mistake made by exam candidates
■ KEY TERM	Definition you must know verbatim
↔ COMPARE	Two concepts that are frequently confused

EXAM TIP

On exam day: scan the Rapid Recall tables on page 25 first (10 min). During the test, eliminate obviously wrong answers first — Security+ often tests BEST answer, not just correct answer. Watch for questions that specify 'MOST secure' or 'LEAST expensive'.

CIA TRIAD

CONFIDENTIALITY
Ensuring data is accessible only to authorised users. Controls: encryption, access control lists, MFA.

INTEGRITY
Ensuring data is accurate and unaltered. Controls: hashing (SHA-256), digital signatures, checksums.

AVAILABILITY
Ensuring systems/data are accessible when needed. Controls: redundancy, load balancing, backups, RAID.

SECURITY CONTROL TYPES

PREVENTIVE

Firewall
Blocks unauthorised traffic
Encryption
Protects data in transit/rest
Access Control
Limits who can access resources
MFA
Requires multiple auth factors

DETECTIVE

IDS/IPS
Detects & alerts on intrusions
SIEM
Aggregates & correlates logs
Audit Logs
Records system activities
Motion Sensor
Physical detection

CORRECTIVE

Backups
Restores data after incident
Patch Mgmt
Fixes known vulnerabilities
IR Plan
Structured incident response
Quarantine
Isolates infected systems

DETERRENT

Warning Signs
Discourages attackers
Security Cameras
Visible surveillance
Legal Policy
Communicates consequences
Guard Post
Visible physical presence

CONTROL CATEGORIES

TECHNICAL	Software/hardware controls: firewall, IDS, encryption, ACL
ADMINISTRATIVE	Policies & procedures: security policy, training, background checks
PHYSICAL	Physical barriers: locks, cameras, fences, security guards

EXAM TIP

The CIA Triad is tested heavily. Remember: Confidentiality = encryption/ACL, Integrity = hashing/signatures, Availability = redundancy/backups. Control types: Preventive stops it, Detective finds it, Corrective fixes it.

THREAT ACTOR SPECTRUM (Low Sophistication → High)

Script Kiddie
Low skill
Off-the-shelf tools
Opportunistic

Insider Threat
Trusted access
Malicious/accidental
Data theft

Hacktivist
Ideological motive
DDoS, defacement
Med sophistication

Cyber Criminal
Financial motive
Ransomware, fraud
High resources

APT
Nation-state backed
Long-term access
Extremely targeted

Nation State
Highest resources
Cyber warfare
Supply chain attacks

SOCIAL ENGINEERING ATTACKS

Phishing	Mass email attack impersonating legitimate entities to steal credentials
Spear Phishing	Targeted phishing using victim-specific info for higher success rate
Vishing	Voice phishing — phone calls impersonating IT/bank support
Smishing	SMS-based phishing with malicious links or urgent requests
Whaling	Phishing targeting high-value executives (CEOs, CFOs)
Pretexting	Fabricated scenario to gain trust and extract information
Tailgating	Physical access by following authorised person through secure door
Baiting	Leaving infected USB drives for curious victims to plug in

MALWARE TYPES

Virus	Attaches to files; needs host to spread
Worm	Self-replicates across networks without host
Trojan	Disguised as legitimate software
Ransomware	Encrypts data; demands payment for key
Rootkit	Hides in OS; grants persistent privileged access
Spyware	Monitors user activity, captures keystrokes/data
Adware	Displays unwanted ads; often bundles spyware
Botnet	Network of infected machines (bots) for DDoS/spam

EXAM TIP

Remember the attacker motivation: Script Kiddies = bragging rights, Insiders = revenge/profit, Hacktivists = ideology, Cyber Criminals = money, Nation-States = espionage/disruption. Exam often asks 'MOST likely threat actor'.

MAJOR SECURITY FRAMEWORKS

NIST CSF
National Institute of Standards & Techno

Identify | Protect | Detect | Respond | Recover

Voluntary framework for critical infrastructure; widely adopted in US government & private sector.

ISO 27001
International Organization for Standardi

Context | Leadership | Planning | Support | Operation | Eval | Improve

International standard for Information Security Management Systems (ISMS). Certifiable.

NIST 800-53
Security & Privacy Controls for Federal

Access Control | Audit | Config Mgmt | IR | Risk Assessment

Comprehensive catalog of security controls for US federal agencies. Basis for FedRAMP.

CIS Controls
Center for Internet Security Critical Se

Inventory | Secure Config | Data Prot | Account Mgmt | Vulnerability Mgmt

18 prioritised security controls. IG1=basic, IG2=foundational, IG3=organizational.

MITRE ATT&CK FRAMEWORK (Tactics Overview)

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Recon	Resource Dev	Initial Access	Execution	Persistence	Privilege Esc	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	C2	Exfiltration	Impact

EXAM TIP

NIST CSF = 5 functions (Identify-Protect-Detect-Respond-Recover). ISO 27001 = certifiable ISMS. CIS Controls = 18 prioritised actions. MITRE ATT&CK; = tactics & techniques matrix — used for threat hunting & detection.

RISK FORMULA & CONCEPTS

RISK = Likelihood × Impact

SLE = Asset Value × EF | ALE = SLE × ARO | ROI on controls = ALE(before) – ALE(after) – Cost

Asset Value (AV)
The monetary value of the asset being protected

Exposure Factor (EF)
Percentage of asset lost in a single incident (0–100%)

Single Loss Expectancy (SLE)
Expected monetary loss per single incident: AV × EF

Annual Rate of Occurrence (ARO)
How many times an incident is expected per year

Annual Loss Expectancy (ALE)
Expected loss per year: SLE × ARO

Residual Risk
Risk remaining after controls are applied

RISK TREATMENT STRATEGIES

AVOID	MITIGATE (Reduce)	TRANSFER	ACCEPT
Stop the risky activity completely	Implement controls to reduce likelihood/impact	Shift risk to third party (insurance, outsourcing)	Acknowledge risk; no action (residual risk)

RISK MATRIX

← IMPACT →			
	LOW	MEDIUM	HIGH
	LOW	MEDIUM	HIGH
	LOW	LOW	MEDIUM

← LIKELIHOOD →

EXAM TIP

Key formulas to memorise: SLE = AV × EF. ALE = SLE × ARO. Residual Risk = Inherent Risk – Controls. If ALE(before) – ALE(after) > control cost → cost-effective. Risk Acceptance requires formal sign-off from management.

MALWARE VISUAL TAXONOMY

VIRUS

Attaches to executable files. Requires host file to spread. Types: boot sector, file infector, macro, polymorphic, metamorphic.

WORM

Self-replicates across networks without user interaction. Exploits vulnerabilities. Famous: WannaCry, Morris Worm.

TROJAN

Disguised as legitimate software. Does NOT self-replicate. Creates backdoor for attacker access.

RANSOMWARE

Encrypts victim files; demands ransom for decryption key. Variants: crypto (encrypts data), locker (locks device).

ROOTKIT

Hides deep in OS/firmware. Provides persistent privileged access. Very hard to detect; survives reboots.

SPYWARE

Silently monitors/records user activity. Captures keystrokes, screenshots, browsing history.

KEYLOGGER

Records keystrokes to capture passwords & sensitive data. Can be software or hardware-based.

BOTNET

Network of compromised machines controlled by C2 server. Used for DDoS, spam, credential theft, crypto mining.

FILELESS MALWARE

Lives in memory only; writes nothing to disk. Uses PowerShell/WMI. Evades traditional AV.

LOGIC BOMB

Dormant code that triggers on specific condition (date, user action). Often planted by insiders.

EXAM TIP

Key distinction: Virus needs a host file; Worm is self-replicating standalone. Rootkits target ring 0 (kernel); hardest to remove — sometimes requires OS reinstall. Fileless malware = no disk footprint = evades hash-based AV detection.

PHISHING ATTACK LIFECYCLE

1. RECON
Attacker gathers OSINT: LinkedIn, social media, company website, emails

2. LURE CRAFT
Creates convincing pretext; spoofs domain; clones legitimate email

3. DELIVER
Sends phishing email with malicious link or attachment

4. HOOK
Victim clicks link; landed on fake login or downloads payload

5. EXPLOIT
Credentials stolen or malware executed; initial access gained

6. POST-EXPLOIT
Lateral movement; data exfiltration; persistence established

INFLUENCE PRINCIPLES (Cialdini)

Authority	Impersonates executive, IT, or law enforcement
Scarcity	Creates urgency: 'Act NOW or lose access'
Social Proof	Implies others have complied: 'Your team already did'
Liking	Builds rapport before the ask
Reciprocity	Gives something small first to create obligation
Commitment	Gets small yeses before the big request

DEFENCES AGAINST SOCIAL ENGINEERING

Security Awareness Training
Mandatory periodic training for all staff

Phishing Simulations
Regular simulated attacks to test vigilance

Email Filtering / DMARC
Block spoofed domains; validate sender identity

MFA
Even stolen credentials can't be used alone

Call-Back Verification
Verify caller identity using known number

Least Privilege
Limits damage even if attacker gains access

EXAM TIP

Security awareness training is the MOST effective defence against social engineering. MFA mitigates credential theft even after successful phishing. DMARC/DKIM/SPF are technical controls to reduce email spoofing.

DoS vs DDoS vs AMPLIFICATION ATTACKS

DoS (Denial of Service)	DDoS (Distributed DoS)	Amplification Attack
Single attacker overwhelms target	Botnet of thousands of compromised hosts	Small request → huge response via open servers
SYN Flood, Ping of Death, Slowloris, HTTP Flood	Volumetric (bandwidth), Protocol, Application layer	DNS amplification, NTP amplification, SSDP

MAN-IN-THE-MIDDLE ATTACKS

ARP Spoofing
Sends fake ARP replies to associate attacker MAC with legit IP

DNS Poisoning
Injects false DNS records to redirect victims to malicious sites

SSL Stripping
Downgrades HTTPS to HTTP; intercepts plaintext traffic

Evil Twin AP
Rogue Wi-Fi AP mimicking legitimate one to capture traffic

Session Hijack
Steals valid session token to impersonate authenticated user

OTHER COMMON NETWORK ATTACKS

SQL Injection
Malicious SQL in input fields to dump/modify DB

XSS
Injects script into web page viewed by victims

Buffer Overflow
Overflows memory to overwrite adjacent data/execute code

Replay Attack
Captures and resends valid auth tokens/packets

Pass the Hash
Uses captured password hash without cracking it

EXAM TIP

ARP Spoofing = Layer 2 MITM. DNS Poisoning = Layer 7. Defend MITM with: HTTPS Everywhere, HSTS, certificate pinning, dynamic ARP inspection. SYN Flood mitigation = SYN cookies. DDoS mitigation = upstream scrubbing / CDN / rate limiting.

OWASP TOP 10 WEB APPLICATION VULNERABILITIES (2021)

A01 — Broken Access Control
Users can act outside intended permissions. Horizontal/vertical privilege escalation.

A02 — Cryptographic Failures
Weak encryption, exposed sensitive data, deprecated algorithms (MD5, SHA-1).

A03 — Injection
SQL, LDAP, OS command injection via untrusted data. Use parameterised queries.

A04 — Insecure Design
Missing security controls by design. Threat modelling required in SDLC.

A05 — Security Misconfiguration
Default credentials, unnecessary features enabled, verbose error messages.

A06 — Vulnerable Components
Using libs/frameworks with known CVEs. Keep dependencies patched.

A07 — Auth Failures
Broken auth, weak passwords, session fixation, credential stuffing.

A08 — Integrity Failures
Untrusted deserialization, insecure CI/CD pipelines, auto-updates without signing.

A09 — Logging Failures
Insufficient logging/monitoring; enables attackers to persist undetected.

A10 — SSRF
Server-Side Request Forgery — server fetches attacker-controlled external resource.

SQL INJECTION ANATOMY

Vulnerable Query:

```
SELECT * FROM users WHERE username='[INPUT]' AND password='[INPUT]'
```

Attacker Input:

```
admin' OR '1'='1' --
```

EXAM TIP

A01 Broken Access Control is the #1 OWASP risk. Always test with low-privilege accounts. SQLi prevention = parameterised queries + input validation + stored procedures. XSS prevention = output encoding + Content Security Policy (CSP).

VULNERABILITY MANAGEMENT LIFECYCLE

DISCOVER	SCAN	ASSESS	REMEDIATE	VERIFY	REPORT
Asset inventory; identify all systems and software	Run vuln scanners (Nessus, OpenVAS); identify CVEs	Prioritise by CVSS score, exploitability, asset criticality	Patch, reconfigure, or apply virtual patching / WAF rule	Re-scan to confirm remediation; validate no new vulns	Document findings, trend analysis, executive metrics

CVSS SCORING SCALE & REMEDIATION PRIORITY

None	LOW	MEDIUM	HIGH	CRITICAL
0.0	0.1–3.9	4.0–6.9	7.0–8.9	9.0–10.0

VULN SCAN vs PEN TEST

Vuln Scan

- Automated tool (Nessus, Qualys)
- Identifies known CVEs
- Non-intrusive
- Run frequently (weekly/monthly)
- Reports potential vulnerabilities

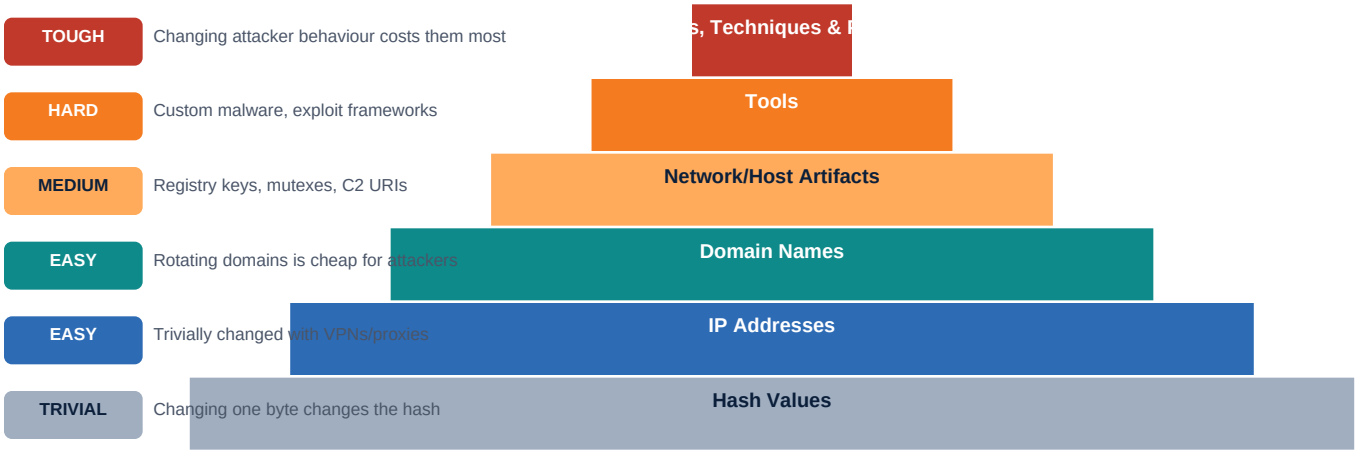
PATCH MANAGEMENT BEST PRACTICES

Emergency Patch	CVSS 9+: Apply within 24 hours
Critical Patch	CVSS 7–8.9: Apply within 7 days
High Patch	CVSS 4–6.9: Apply within 30 days
Low/Info	CVSS <4: Next maintenance window
Test First	Always test patches in non-prod before deploy

EXAM TIP

CVSS = Common Vulnerability Scoring System. Zero-day = no patch available yet. Virtual patching = WAF rule to block exploit while waiting for official patch. Always: Scan → Assess by criticality → Remediate → Verify → Document.

PYRAMID OF PAIN (Attacker-Defender Cost Model)



INDICATORS OF COMPROMISE (IOC) & THREAT INTEL SOURCES

File Hashes
MD5/SHA-256 of known malware files

IP Addresses
Known C2 servers, Tor exit nodes, botnet IPs

Domain Names
Malicious domains used for phishing or C2

URLs
Specific malicious endpoints or redirect chains

Email Addresses
Sender addresses used in phishing campaigns

Registry Keys
Persistence mechanisms written to Windows registry

Network Signatures
YARA rules, Snort rules matching malicious traffic

Behavioural Patterns
TTPs mapped to MITRE ATT&CK framework

EXAM TIP

Pyramid of Pain: TTPs are hardest for attacker to change = most valuable to defenders. Hash blocking = trivial to bypass (change one byte). Threat Intelligence sharing: ISACs (Information Sharing & Analysis Centers) by sector.

NETWORK SEGMENTATION STRATEGIES

VLAN
Virtual Local Area Network

- Layer 2 segmentation on managed switches
- Logical separation without physical hardware
- Reduces broadcast domains
- Tagged (802.1Q) or untagged ports

DMZ
Demilitarised Zone

- Buffer zone between internet & internal network
- Hosts public-facing services (web, mail, DNS)
- Two-firewall architecture recommended
- Internal LAN never directly reachable

Zero Trust
Never Trust, Always Verify

- No implicit trust based on network location
- Verify every user, device, and request
- Micro-segmentation at workload level
- Least-privilege access for every connection

Air Gap
Physical Isolation

- No network connection to untrusted networks
- Used for critical systems (SCADA, nuclear)
- Data transfer via sanitised removable media
- Highest security; lowest usability

NETWORK ACCESS CONTROL (NAC) & WIRELESS SECURITY

NAC	Enforces security policy before granting network access. Checks patch level, AV status.
802.1X	Port-based auth for wired/wireless. Uses RADIUS server + supplicant + authenticator.
WPA3	Current Wi-Fi standard. Uses SAE handshake. Replaces WPA2 CCMP/AES.
WPA2	CCMP/AES encryption. WPA2-Enterprise uses 802.1X. Vulnerable to KRACK.
Evil Twin	Rogue AP attack. Mitigation: detect unexpected SSIDs, use VPN on Wi-Fi.

EXAM TIP

Zero Trust = 'Never trust, always verify'. Micro-segmentation limits lateral movement. DMZ uses two firewalls: one facing internet, one facing internal LAN. 802.1X = RADIUS for wired/wireless authentication.

FIREWALL TYPES COMPARISON

Packet Filter Firewall	Stateful Inspection	NGFW (Next-Gen)	WAF (Web App)	Proxy Firewall
Layer 3–4	Layer 3–5	Layer 3–7	Layer 7	Layer 7
Inspects source/destination IP, port, protocol. Stateless. Fast but limited.	Tracks connection state table. Knows if packet belongs to established session.	Deep packet inspection, application awareness, IPS, SSL inspection, user identity.	Protects web apps. Inspects HTTP/HTTPS. Blocks SQLi, XSS, OWASP Top 10.	Terminates and re-initiates connections. Full content inspection. Forward & reverse proxy.

IDS vs IPS

IDS	IPS
Passive: monitors and alerts only	Active: detects AND blocks threats
Cannot block traffic	Deployed inline (can introduce latency)
Deployed out-of-band	Can drop/reject malicious packets
HIDS (host-based) or NIDS (network)	Higher risk of false positives blocking legit traff
Signature-based or anomaly-based	Consider fail-open vs fail-closed

KEY SECURITY PROTOCOLS

TLS 1.3	Transport encryption. Replaces SSL. Use for HTTPS, SMTP, FTPS.
SSH v2	Encrypted remote admin. Replaces Telnet/rlogin.
IPSec	VPN tunnelling. AH=integrity, ESP=confidentiality. Modes: Transport/Tunnel.
DNSSEC	Adds digital signatures to DNS records. Prevents DNS poisoning.
SFTP/FTPS	Secure file transfer. SFTP=SSH-based, FTPS=TLS-wrapped FTP.
HTTPS	HTTP over TLS. Port 443. Uses X.509 certificates.

EXAM TIP

NGFW = DPI + application awareness + user identity + IPS. WAF protects web apps (Layer 7). Use both: WAF for app-layer, NGFW for network-layer. IPS inline = can block; IDS out-of-band = detect only. Fail-closed = default deny.

SHARED RESPONSIBILITY MODEL

Responsibility	On-Premises	IaaS	PaaS	SaaS
Applications	Customer	Customer	Customer	Provider
Data	Customer	Customer	Customer	Customer
Runtime	Customer	Customer	Provider	Provider
Middleware	Customer	Customer	Provider	Provider
OS	Customer	Customer	Provider	Provider
Virtualisation	Customer	Provider	Provider	Provider
Network	Customer	Provider	Provider	Provider
Storage/Hardware	Customer	Provider	Provider	Provider

CLOUD DEPLOYMENT MODELS & SECURITY CONTROLS

Public Cloud
AWS, Azure, GCP. Shared infrastructure. Lower cost. Provider manages physical security.

Private Cloud
Dedicated hardware. Higher cost. Greater control. Used by gov/finance.

Hybrid Cloud
Mix of public/private. Complexity increases. Requires consistent policy/identity management.

Community Cloud
Shared by orgs with common requirements (e.g., government, healthcare).

KEY CLOUD SECURITY TOOLS

- **CASB** — Cloud Access Security Broker — visibility & control over cloud app usage
- **CSPM** — Cloud Security Posture Mgmt — identifies misconfigurations in cloud env
- **SWG** — Secure Web Gateway — filters web traffic, enforces policy for cloud users
- **CWPP** — Cloud Workload Protection Platform — secures VMs, containers, serverless

EXAM TIP

Shared Responsibility: Customer ALWAYS owns their data regardless of cloud model. SaaS = provider manages almost everything. IaaS = customer manages OS upward. Key cloud risks: misconfiguration, insecure APIs, data exposure, account hijacking.

AUTHENTICATION FACTORS (MFA)

Something YOU KNOW	Something YOU HAVE	Something YOU ARE	Somewhere YOU ARE	Something YOU DO
Password, PIN, passphrase, security question	Smart card, hardware token (FIDO2), OTP app, phone	Fingerprint, retina scan, facial recognition, vein pattern	Geolocation, IP-based access, GPS	Typing cadence, gait analysis, gesture patterns
Weakest alone — subject to phishing, brute force, password reuse	Requires physical possession; harder to phish remotely	Biometrics — high convenience; can't be forgotten; difficult to change if compromised	Contextual factor — restricts access based on physical location	Behavioural biometrics — continuous authentication; transparent to user

AAA FRAMEWORK

Authentication
Verifying IDENTITY — who are you? (password, MFA, certificate)

Authorisation
Verifying PERMISSIONS — what can you do? (ACL, RBAC, policies)

Accounting
Tracking ACTIVITY — what did you do? (audit logs, SIEM)

ACCESS CONTROL MODELS

MAC	Mandatory Access Control — labels (Top Secret). Gov/military. Rigid.
DAC	Discretionary Access Control — owner sets permissions. Most flexible.
RBAC	Role-Based — permissions based on job role. Most common enterprise.
ABAC	Attribute-Based — fine-grained; evaluates multiple attributes.

SSO, FEDERATION & IDENTITY PROTOCOLS

SSO — Single Sign-On — authenticate once, access multiple systems	SAML 2.0 — XML-based federation standard for web SSO between IdP and SP	OAuth 2.0 — Authorisation framework (not authentication). Used for API access delegation
OpenID Connect — Authentication layer on top of OAuth 2.0. Returns identity tokens (JWT)	LDAP — Lightweight Directory Access Protocol. Used to query Active Directory	Kerberos — Ticket-based auth using TGT/TGS. Default for Windows AD domains

EXAM TIP

MFA types: Something you KNOW + HAVE + ARE. Using 2+ factors = MFA. SAML = federated SSO (enterprise). OAuth = authorisation (API). OpenID Connect = authentication on OAuth. Kerberos = Windows AD ticket system. LDAP = directory queries.

SYMMETRIC vs ASYMMETRIC ENCRYPTION

SYMMETRIC (Shared Key)

- One key for encryption AND decryption
- Fast — suitable for bulk data encryption
- Key distribution problem (how to share key?)
- AES-256 (standard), 3DES (legacy), RC4 (broken)
- Use: TLS data channel, disk encryption, VPNs

ASYMMETRIC (Public/Private Key Pair)

- Public key encrypts; private key decrypts
- Slower — used for key exchange & digital sigs
- Solves key distribution problem
- RSA (2048/4096-bit), ECC, Diffie-Hellman
- Use: TLS handshake, S/MIME email, code signing

HASHING ALGORITHMS & DIGITAL SIGNATURES

MD5 — 128-bit
BROKEN — collision attacks. Legacy only.

SHA-1 — 160-bit
BROKEN — deprecated. Avoid.

SHA-256 — 256-bit
Current standard. Part of SHA-2 family.

SHA-3 — Variable
Next-gen Keccak design. Quantum-resistant.

HMAC — Keyed hash
Hash + secret key. Message authentication.

bcrypt — Variable
Password hashing. Slow by design (brute-force resistant).

PKI — PUBLIC KEY INFRASTRUCTURE

CA (Certificate Authority)	Issues & signs digital certificates. Root CA > Intermediate CA > End-entity cert.
RA (Registration Authority)	Verifies identity before CA issues certificate.
CRL (Cert Revocation List)	List of revoked certs published by CA. Checked before trusting a cert.
OCSP	Online Certificate Status Protocol — real-time cert revocation check.
X.509	Standard for digital certificate format. Used in TLS, S/MIME, code signing.

EXAM TIP

Symmetric = fast, shared key (AES). Asymmetric = slow, key pair (RSA/ECC). TLS uses BOTH: asymmetric for handshake/key exchange, symmetric for data. Digital signature = hash encrypted with SENDER's private key. Verified with public key.

INCIDENT RESPONSE LIFECYCLE (NIST SP 800-61)

1 PREPARATION

- Develop IR policy & plan
- Assemble CSIRT team
- Acquire & configure tools
- Train staff; run tabletop exercises
- Define communication procedures

2 DETECTION & ANALYSIS

- Monitor SIEM/IDS alerts
- Identify indicators of compromise
- Determine scope & severity
- Classify incident type
- Document initial findings

3 CONTAINMENT

- Short-term: isolate system
- Long-term: segment network
- Preserve evidence before cleanup
- Choose: shutdown vs isolate vs monitor
- Prevent further spread

4 ERADICATION

- Remove malware/rootkits
- Patch vulnerability exploited
- Identify all affected systems
- Verify clean state via scan
- Check for persistence mechanisms

5 RECOVERY

- Restore from clean backups
- Return to production
- Monitor closely post-restoration
- Validate system integrity
- Confirm normal operations

6 LESSONS LEARNED

- Post-incident review meeting
- Document timeline of events
- Identify gaps in controls
- Update IR plan accordingly
- Report to management/regulators

INCIDENT CATEGORIES & SEVERITY

P1 CRITICAL	Active breach, ransomware, data exfiltration in progress. Immediate response.
P2 HIGH	Confirmed compromise, malware infection, privileged account takeover.
P3 MEDIUM	Failed intrusion attempts, phishing with no click, policy violations.
P4 LOW	Suspicious activity, minor anomalies, potential misconfigurations.

EXAM TIP

NIST IR lifecycle: Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned. Order matters: CONTAIN first before eradicating. Preserve evidence BEFORE cleaning. Lessons Learned = root cause analysis + plan update. Every incident makes you stronger.

SIEM ARCHITECTURE

CRITICAL LOG SOURCES

Windows Event Logs
Event IDs: 4624(logon) 4625(fail) 4720(user create) 4776

Firewall Logs
Allowed/denied connections, source/dest IP, port, protocol

DNS Logs
Queries to unusual domains (DGA, typosquatting, C2 callbacks)

Web Server Logs
HTTP methods, status codes, user-agents, referrers

Authentication Logs
Failed logins, MFA challenges, account lockouts

MONITORING CONCEPTS

Continuous Monitoring
24/7 automated detection and alerting via SIEM/SOC

Baseline
Establish normal behaviour; alert on deviations

Threshold Alerting
Alert when metric exceeds defined limit (e.g., 5 failed logins)

Anomaly Detection
ML/behaviour-based detection of unusual patterns

UBA/UEBA
User (& Entity) Behaviour Analytics — detect insider threats

EXAM TIP

SIEM = Security Information and Event Management. Aggregates logs, correlates events, alerts analysts. Key Windows Event IDs: 4624=logon, 4625=failed logon, 4688=process create, 4720=user created. SOC Tiers: T1=triage, T2=investigation, T3=threat hunting/IR.

DIGITAL FORENSICS PROCESS

1. **IDENTIFICATION**
   Determine what evidence exists; scope the investigation; identify evidence sources (disk, RAM, network)
2. **PRESERVATION**
   Protect evidence integrity: write-blockers, forensic copies, chain of custody, hash verification
3. **COLLECTION**
   Acquire digital evidence: forensic imaging (dd, FTK Imager), RAM capture, network packet capture
4. **EXAMINATION**
   Process & filter data: carve files, recover deleted data, analyse file system metadata
5. **ANALYSIS**
   Interpret evidence: timeline analysis, correlation, attribution, identify attack vector
6. **PRESENTATION**
   Produce report: clear, factual, defensible in court. Expert testimony if needed.

ORDER OF VOLATILITY (Most → Least)

1. **CPU Registers & Cache**
   Lost immediately on power-off
2. **RAM / Physical Memory**
   Lost when system is shutdown/rebooted
3. **Network Connections**
   Active connections, ARP cache, routing tables
4. **Running Processes**
   Process list, open handles, loaded DLLs
5. **Disk Storage**
   Files, registry, event logs — persists off power
6. **Backup Media**
   Tapes, external drives — most persistent
7. **Remote/Cloud Logs**
   Archived logs on remote systems

CHAIN OF CUSTODY REQUIREMENTS

- **Identification**
  Label and uniquely identify every piece of evidence
- **Documentation**
  Record who collected it, when, where, and how
- **Handling**
  Use anti-static bags, write-blockers, sealed containers
- **Storage**
  Secure storage with access controls and audit log
- **Transfer**
  Log every transfer; require signature confirmation
- **Integrity Verification**
  Hash evidence before and after; document any discrepancy
- **Presentation**
  Maintain chain from collection to courtroom testimony

EXAM TIP

Order of Volatility: Collect most volatile FIRST (RAM before disk). Chain of custody = legal admissibility. Use write-blockers to prevent modifying evidence. Hash (SHA-256) evidence before and after analysis to prove it was not altered.

BACKUP TYPES COMPARISON

FULL BACKUP

All data every time

- Longest to create
- Fastest to restore
- Most storage space
- Simplest recovery

Sun: Full

INCREMENTAL

Changes since LAST backup

- Fastest to create
- Slowest to restore
- Least storage used
- Need full + all incrementals to restore

Sun: Full | Mon-Sat: Incremental each day

DIFFERENTIAL

Changes since LAST FULL

- Medium speed to create
- Faster restore than incremental
- Medium storage
- Need full + latest differential

Sun: Full | Mon-Sat: Diff grows each day

SNAPSHOT

Point-in-time copy (VM/storage)

- Near-instant creation
- Space-efficient (CoW)
- Rapid VM recovery
- Common in cloud/virtualisation

Continuous snapshots

RTO, RPO & HIGH AVAILABILITY CONCEPTS

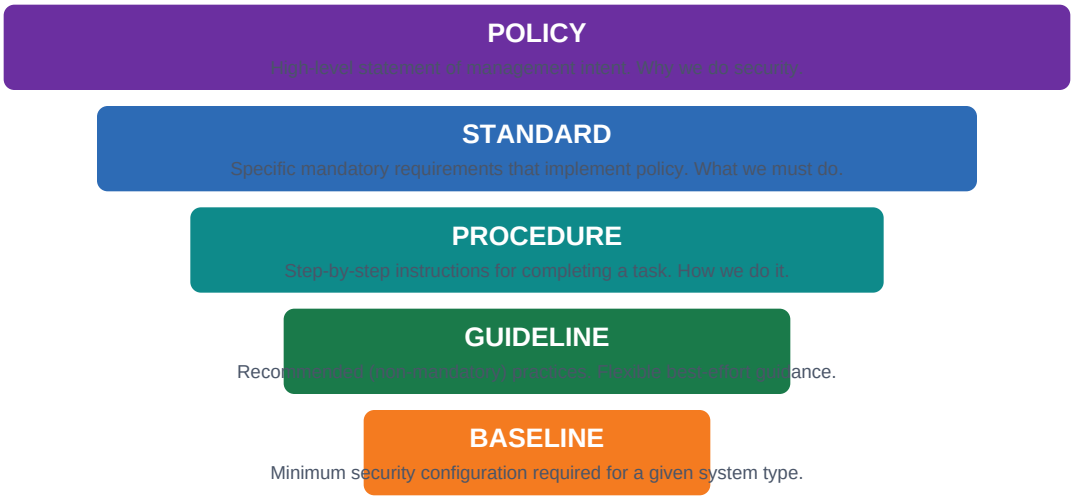
RTO	RPO	MTTR	MTBF
Recovery Time Objective	Recovery Point Objective	Mean Time To Repair	Mean Time Between Failures

Load Balancing	Distributes traffic across multiple servers. Round-robin, weighted, least-connection.
Failover Cluster	Primary system fails → traffic automatically switches to standby node.
RAID	Redundant Array of Independent Disks. RAID 1=mirror, RAID 5=parity, RAID 10=mirror+stripe.
Geo-Redundancy	Multiple geographically distributed data centres. Protects against site-level disasters.

EXAM TIP

RTO = how long you CAN be down. RPO = how much data you CAN lose. Incremental = faster backup, slower restore. Differential = faster restore, more space. 3-2-1 Rule: 3 copies, 2 different media types, 1 offsite.

POLICY HIERARCHY



CRITICAL SECURITY POLICIES

AUP	Acceptable Use Policy — defines permitted/prohibited use of org technology resources
Data Classification	Defines data sensitivity levels: Public, Internal, Confidential, Restricted/Top Secret
Password Policy	Minimum length (12+), complexity, rotation period, no reuse, MFA requirement
NDA	Non-Disclosure Agreement — legal contract protecting confidential information
BYOD Policy	Bring Your Own Device — rules for personal devices on corporate network (MDM, containerisation)
Change Mgmt	Formal process for system changes: request → review → approve → implement → verify
Clean Desk Policy	Sensitive info locked away when not in use. Prevents shoulder surfing & physical theft
MOU/MOA	Memorandum of Understanding/Agreement — non-binding/binding inter-org agreements

EXAM TIP

Policy hierarchy: Policy (WHY) → Standard (WHAT) → Procedure (HOW) → Guideline (RECOMMENDED). Data Classification drives controls: more sensitive = stricter controls. AUP should be signed by all employees. BYOD needs MDM and containerisation.

KEY REGULATORY COMPLIANCE FRAMEWORKS

HIPAA
Health Insurance Portability & Accountability Act
USA | Healthcare

- Protects PHI (Protected Health Info)
- Privacy Rule + Security Rule + Breach Notification
- Business Associate Agreements (BAAs) required
- Penalty: up to $1.9M per violation category/year

GDPR
General Data Protection Regulation
EU/EEA | All sectors

- Right to access, erasure, portability
- Data Protection Officer (DPO) required for some orgs
- Breach notification within 72 hours
- Penalty: up to 4% global annual revenue

PCI DSS
Payment Card Industry Data Security Standard
Global | Payment car

- 12 requirements across 6 goals
- Required for any org storing/processing card data
- Annual assessment (QSA for large merchants)
- Levels 1-4 based on transaction volume

SOC 2
System & Organisation Controls 2
USA | SaaS/cloud ser

- 5 Trust Services Criteria (TSC): Security,
- Availability, Confidentiality, Processing Integrity, Privacy
- Type I: design effectiveness; Type II: operational
- Required by enterprise customers for vendors

ADDITIONAL STANDARDS & REGULATIONS

FERPA	Educational records privacy (USA)	**COPPA**	Children's online privacy (USA under 13	**GLBA**	Financial data — Gramm-Leach-Bliley Act
FISMA	Federal agency security — NIST 800-53	**CMMC**	DoD contractor cybersecurity maturity m	**ISO 27001**	Certifiable ISMS standard (international)

EXAM TIP

HIPAA = healthcare PHI (USA). GDPR = EU citizen data (global reach). PCI DSS = payment card data. SOC 2 = SaaS/cloud provider audit. Violation penalties: GDPR is heaviest (4% global revenue). Compliance != Security — being compliant is the minimum, not the goal.

SECURITY AWARENESS PROGRAM LIFECYCLE

ASSESS
Identify knowledge gaps, conduct phishing simulation, baseline risk score

DESIGN
Tailor content by role/risk; choose delivery methods; set learning objectives

DELIVER
LMS modules, posters, email campaigns, lunch & learns, gamification

TEST
Phishing simulations, tabletop exercises, spot checks, quizzes

MEASURE
Track click rates, completion, incident trends; report metrics to leadership

IMPROVE
Update content; address gaps; adjust frequency; reinforce good behaviour

INSIDER THREAT TYPES

Malicious Insider
Intentionally harms org — data theft, sabotage, espionage

Negligent Insider
Accidental damage — misconfiguration, falling for phishing

Compromised Insider
Account taken over by attacker using insider's credentials

Third-Party Insider
Vendor/contractor with over-privileged access causing harm

HUMAN RISK MITIGATIONS

Least Privilege	Users have minimum access required for their job
Separation of Duties	No single person controls an entire critical process
Mandatory Vacation	Forces others to cover role; reveals fraud/misconduct
Job Rotation	Rotates roles; reduces single-person dependency
Background Checks	Pre-hire and periodic re-investigations
UBA/DLP	Monitor behaviour and data movement anomalies

EXAM TIP

Humans are the weakest link in cybersecurity. Security awareness training reduces risk significantly. Insider threats are harder to detect than external attackers because they have legitimate access. DLP (Data Loss Prevention) tools help catch data exfiltration before it leaves the organisation.

CRITICAL PORTS & PROTOCOLS

20/21	FTP	File Transfer (insec	22	SSH/SFTP/SCP	Secure remote/file	23	Telnet	Insecure remote (a	25	SMTP	Email sending
53	DNS	Domain name resol	67/68	DHCP	Dynamic IP assignn	80	HTTP	Web (unencrypted)	110	POP3	Email retrieval
119	NNTP	Usenet news protoc	123	NTP	Time synchronisatic	135	RPC	Windows remote ca	137–139	NetBIOS	Windows networking
143	IMAP	Email (server-side)	161/162	SNMP	Network device mgi	389	LDAP	Directory services	443	HTTPS	Secure web
445	SMB	Windows file sharin	465/587	SMTPS	Secure email	514	Syslog	Log aggregation	636	LDAPS	Secure directory
993	IMAPS	Secure IMAP	995	POP3S	Secure POP3	1433	MS SQL	SQL Server	1723	PPTP	VPN (legacy)
3306	MySQL	MySQL database	3389	RDP	Remote Desktop Pr	5060	SIP	VoIP signalling	8080	HTTP-Alt	Web proxy/dev

ENCRYPTION ALGORITHMS

AES	Symmetric | 128/192/256-bit | Current standard
3DES	Symmetric | 168-bit | Legacy — being phased out
RSA	Asymmetric | 2048/4096-bit | Key exchange & sigs
ECC	Asymmetric | Smaller keys, same security as RSA
DH/DHE	Key exchange protocol — forward secrecy with DHE
SHA-256	Hashing | 256-bit output | Part of SHA-2 family
MD5	Hashing | 128-bit | BROKEN — do not use

ACRONYM QUICK REFERENCE

AAA	Authentication, Authorisation, Accounting
ACL	Access Control List
CASB	Cloud Access Security Broker
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities & Exposures
CVSS	Common Vulnerability Scoring System
DLP	Data Loss Prevention
IOC	Indicator of Compromise
MFA	Multi-Factor Authentication
SIEM	Security Info & Event Management
SOC	Security Operations Centre
TTP	Tactics, Techniques & Procedures

LAST-MINUTE EXAM TIPS

Read carefully
Look for: BEST, FIRST, MOST, LEAST. Security+ tests best answer, not just correct.

Eliminate obviously wrong
Usually 2 answers are clearly off. Focus on the remaining 2.

CIA Triad defaults
When in doubt: encryption→Confidentiality, hashing→Integrity, redundancy→Availability.

Incident Response order
ALWAYS: Contain → Eradicate → Recover. Never skip containment.

Least privilege default
When asked 'BEST access control principle' — almost always least privilege.

MFA beats passwords
MFA is almost always the best answer for authentication questions.

You've got this! ■ Review daily, stay consistent, and trust your preparation.