CISSP MASTER STUDY NOTES

Complete Revision Guide — All 8 Domains

Prepared by
Krishna Chandra Muduli, CISSP
Cybersecurity Lead Engineer | CISSP Certified | CEH | AWS-SAP
Published at: krishnamuduli.co.in/learning_hub.html

"Everything you need to revise before CISSP — simple, powerful, and in one place."

What's Inside

- All 8 CISSP Domain overviews with key concepts
- Important terms & definitions (easy to remember)
- Real-life examples from corporate, cloud & SOC environments
- Exam tips, traps & memory tricks
- Comparison tables (Symmetric vs Asymmetric, DAC vs MAC, etc.)
- Mnemonics for each domain
- 4–5 CISSP-style practice questions per domain with explanations
- Quick Revision Notes for last-day study

DOMAIN 1
Security and Risk Management

Domain Overview

This is the LARGEST domain in CISSP (15% of exam). It covers the foundation of cybersecurity — how organizations manage risk, set policies, follow laws, and build a security culture. Think of it as the "CEO mindset" of cybersecurity.

Why it matters: Every security decision — budgets, tools, policies — must be justified through risk management. This domain teaches you to think like a business leader, not just a technician.

★ Most Important Topics

- **CIA Triad** (Confidentiality, Integrity, Availability)
- **Risk = Threat x Vulnerability x Asset Value**
- **Risk Treatment**: Accept, Transfer, Mitigate, Avoid
- **Security Governance** & Policy Framework
- **Legal, Regulatory & Compliance** (GDPR, HIPAA, SOX)
- **Security Awareness Training**
- **Business Continuity Planning (BCP)** vs Disaster Recovery (DRP)

Key Concepts

CIA Triad

CIA Pillar	What It Means & Example
Confidentiality	Only authorized people can access the data. Example: Encryption, Access Controls
Integrity	Data is accurate and not tampered with. Example: Hashing (SHA-256), Digital Signatures
Availability	Systems are up and working when needed. Example: Redundancy, Backups, DDoS protection

Risk Management Process

Step	Description
Identify Assets	What do we need to protect? (servers, data, people)
Identify Threats	What could go wrong? (hackers, fire, flood, insider)
Identify Vulnerabilities	What weaknesses exist? (unpatched software, weak passwords)

Calculate Risk	Risk = Threat x Vulnerability x Asset Value
Select Controls	Choose safeguards to reduce risk
Monitor & Review	Continuously check if controls are working

Risk Treatment Options

Treatment	Explanation
Accept (Tolerate)	Risk is low or cost to fix is higher than risk. Do nothing.
Transfer	Buy cyber insurance or outsource to a third party.
Mitigate (Reduce)	Apply security controls to lower probability or impact.
Avoid	Stop the risky activity altogether.

Key Risk Terms

Term	Definition
ALE	Annual Loss Expectancy = ARO x SLE (total expected yearly loss)
SLE	Single Loss Expectancy = Asset Value x Exposure Factor
ARO	Annual Rate of Occurrence (how often threat happens per year)
EF	Exposure Factor = % of asset damaged in one incident (0–1)
Residual Risk	Risk remaining AFTER controls are applied
Total Risk	Risk if NO controls exist
Risk Appetite	How much risk the org is willing to accept

Security Governance & Policies

- **Policy** → High-level statement of intent ("We will protect all customer data")
- **Standard** → Specific mandatory rules ("Passwords must be 12+ chars")
- **Guideline** → Recommended best practices (not mandatory)
- **Procedure** → Step-by-step instructions for specific tasks
- **Baseline** → Minimum security level required for all systems

Security Frameworks & Laws

Framework/Law	Purpose
NIST CSF	Framework: Identify, Protect, Detect, Respond, Recover
ISO 27001	International standard for Information Security Management System
COBIT	IT Governance framework for business alignment
GDPR	EU regulation — protect personal data of EU citizens
HIPAA	US law — protect health information (PHI)
SOX	US law — financial reporting controls for public companies
PCI-DSS	Payment Card Industry standard for credit card security

Business Continuity vs Disaster Recovery

Term	Meaning
BCP (Business Continuity Plan)	Keep business running DURING a disaster
DRP (Disaster Recovery Plan)	Restore IT systems AFTER a disaster
BIA (Business Impact Analysis)	Identify critical functions and their impact if lost
RTO (Recovery Time Objective)	Maximum time to restore a system after outage
RPO (Recovery Point Objective)	Maximum acceptable data loss (in time)
MTD (Maximum Tolerable Downtime)	Longest time a business can be down before serious harm

MNEMONIC: CIA Triad
"Can I Access?" — Confidentiality (Can only authorized users?), Integrity (Is data accurate?), Availability (Are systems up?)

MNEMONIC: Risk Treatment = ATMA
Accept → Transfer → Mitigate → Avoid

Important Terms & Definitions

Term	Definition

Threat	Any potential danger to an asset (e.g., hacker, malware, flood)
Vulnerability	A weakness that can be exploited (e.g., unpatched software)
Risk	Possibility of harm = Threat exploiting a Vulnerability
Asset	Anything valuable to the organization (data, hardware, people)
Control	A safeguard or countermeasure to reduce risk
Due Diligence	Doing research before making a decision (knowing the risks)
Due Care	Taking action to address known risks (fixing them)
Prudent Person Rule	Act as a reasonable, careful person would in similar circumstances

Real-Life Examples

Corporate Scenario:
A bank discovers that ransomware could encrypt their customer database. Using risk management, they calculate: Asset Value = $10M, EF = 80%, SLE = $8M, ARO = 0.2 (once every 5 years), so ALE = $1.6M. They decide to buy cyber insurance for $200K/year (risk transfer) and also patch all servers (risk mitigation).

Cloud Scenario:
An AWS-hosted SaaS company must comply with GDPR. They conduct a BIA and find their order processing system has an RTO of 4 hours. They implement multi-region failover to meet this requirement, and train all staff on privacy policies — linking BCP, compliance, and security awareness.

Exam Tips

CISSP exam always asks from a MANAGEMENT perspective, not a technical one. Choose the option that a CISO or senior manager would pick.

- **Trick**: If a question says "FIRST thing to do" — usually the answer involves RISK ASSESSMENT or BIA first.
- **Trick**: "Due care" = doing the right thing. "Due diligence" = knowing what the right thing is.
- **Trick**: ALE formula: SLE = Asset Value × EF, then ALE = SLE × ARO
- **Trap**: BCP is about KEEPING the business running. DRP is about RECOVERING IT systems.
- **Focus**: Know the difference between policy, standard, guideline, and procedure.
- **Focus**: Understand when to use each risk treatment option.

Quick Revision Notes

- CIA = Confidentiality, Integrity, Availability
- Risk = Threat × Vulnerability × Asset Value
- ALE = ARO × SLE; SLE = Asset Value × EF
- Risk Treatment = Accept, Transfer, Mitigate, Avoid
- Policy > Standard > Guideline > Procedure
- BCP = Keep running during disaster; DRP = Recover IT after
- RTO = Max time to restore; RPO = Max data loss acceptable
- Due Care = act; Due Diligence = know before acting
- GDPR (EU), HIPAA (health), SOX (finance), PCI-DSS (cards)

Practice Questions

Q1: A CISO is informed that a web application vulnerability exists but the cost to fix it exceeds the potential loss. What is the BEST response?

A) Immediately patch the vulnerability

B) Accept the risk and document the decision

C) Transfer the risk through insurance

D) Avoid the risk by shutting down the application

✓Answer: B | When the cost to remediate exceeds potential loss, accepting and documenting is the prudent business decision. This demonstrates due care.

Q2: An organization wants to calculate how much money they could lose per year from a specific threat. Which formula should they use?

A) SLE = Asset Value × ARO

B) ALE = SLE × ARO

C) ALE = Asset Value × EF

D) SLE = ARO × EF

✓Answer: B | ALE (Annual Loss Expectancy) = SLE × ARO. SLE = Asset Value × EF. This quantifies annual expected loss.

Q3: A company's critical payment system has an RTO of 2 hours. The current backup process takes 6 hours to restore. What should the security team do FIRST?

A) Conduct a new BIA

B) Purchase faster storage hardware

C) Update the DRP to meet RTO requirements

D) Escalate to executive management

✓Answer: A | The FIRST step is always assessment. A new BIA will confirm the RTO, business impact, and guide the right corrective actions.

Q4: A manager says "I will accept the risk but I need written approval." This is an example of which concept?

A) Risk Mitigation

B) Risk Transfer

C) Risk Acceptance

D) Risk Avoidance

✓Answer: C | Accepting risk with documented approval is Risk Acceptance. This is appropriate when cost of control > cost of risk.

Q5: Which document provides MANDATORY requirements that everyone in the organization must follow?

A) Guideline

B) Procedure

C) Standard

D) Baseline

✓Answer: C | Standards are mandatory specific rules derived from policy. Guidelines are recommendations. Procedures are step-by-step instructions.

DOMAIN 2

Asset Security

Domain Overview

Asset Security is about protecting information and assets throughout their entire lifecycle — from the moment they are created until they are securely destroyed. This domain accounts for 10% of the CISSP exam.

Why it matters: You can't protect what you don't know you have. This domain ensures organizations properly classify, handle, and dispose of their most valuable resource — data.

★ Most Important Topics

- **Data Classification** (Government vs. Commercial)
- **Data Roles**: Owner, Custodian, User, Processor, Controller
- **Data Lifecycle**: Create → Store → Use → Share → Archive → Destroy
- **Data Retention Policies**
- **Secure Data Destruction** methods
- **Privacy Protection** principles

Key Concepts

Data Classification Levels

Government Classification	Description
Top Secret	Highest classification. Unauthorized disclosure = grave damage to national security.
Secret	Serious damage to national security if disclosed.
Confidential	Damage to national security if disclosed.
Unclassified	No damage. Public use is acceptable.

Commercial Classification	Description
Confidential/Proprietary	Highest commercial level. Trade secrets, M&A info. Very restricted.
Private	Personal data of employees, HR records. Internal only.
Sensitive	Needs extra protection but less than confidential. Financial data.

Public	Safe to share with anyone. Press releases, marketing materials.

Data Roles — Who Does What?

Role	Responsibility
Data Owner	Senior executive responsible for classifying and protecting data. Makes policy decisions.
Data Custodian	IT/Security team that stores and maintains data security. Implements controls.
Data User	End users who access data for their job. Must follow policies.
Data Processor	Third party that processes data on behalf of the controller (GDPR term).
Data Controller	Organization that decides HOW and WHY data is processed (GDPR term).
Data Steward	Ensures data quality, accuracy, and governance standards are met.

Data Lifecycle

Create → Store → Use → Share → Archive → Destroy

- **Create**: Apply classification immediately when data is created.
- **Store**: Encrypt sensitive data at rest; access controls apply.
- **Use**: Enforce least privilege; log access; DLP tools monitor.
- **Share**: Encrypt in transit; use secure channels (TLS, VPN).
- **Archive**: Retain per policy; maintain encryption even in cold storage.
- **Destroy**: Use certified destruction methods — no residual data.

Data Destruction Methods

Method	How it Works
Overwriting	Write new data over old data multiple times (DoD 5220.22-M standard).
Degaussing	Strong magnetic field destroys data on magnetic media (HDDs, tapes).
Shredding	Physical destruction — cutting media into tiny pieces.

Incineration	Burning. Used for classified documents.
Cryptographic Erasure	Destroy encryption key, making encrypted data unreadable.
Wiping vs Deleting	Delete = removes file reference only. Wipe = overwrites actual data.

MNEMONIC: Data Roles → OCUP
Owner (classifies), Custodian (protects), User (accesses), Processor/Controller (GDPR)

MNEMONIC: Data Lifecycle → CS-USAD
Create, Store, Use, Share, Archive, Destroy

Important Terms & Definitions

Term	Definition
Data Remanence	Residual data left on media after deletion — can be recovered by attackers.
Scoping	Limiting security controls to only what is needed.
Tailoring	Customizing baseline controls for specific environment needs.
Data Loss Prevention (DLP)	Technology that detects and prevents unauthorized data transfer.
Information Rights Management (IRM)	Controls how documents can be used (view, print, copy, forward).
Baseline	Minimum security configuration required for all systems.
Retention Policy	How long data must be kept before it can be destroyed.

Real-Life Examples

Healthcare Scenario:
A hospital classifies patient records as "Confidential." The Data Owner (CMO) sets access policies. The Data Custodian (IT team) encrypts the database and sets up access controls. Nurses are Data Users with role-based access to only the patients they treat.

Corporate Scenario:
A company is replacing old hard drives. They use degaussing for magnetic drives and shredding for SSDs (since degaussing doesn't work on SSDs). They document each

destruction with a certificate to prove compliance with data retention and destruction policies.

Exam Tips

SSDs cannot be degaussed — they are not magnetic. Always use overwriting or physical destruction for SSDs.

- **Trap**: Data Owner is NOT the IT person. It's usually a business executive or department head.
- **Trap**: Deleting a file does NOT destroy data. Only overwriting or physical destruction does.
- **Focus**: Know the difference between data classification levels for both government and commercial.
- **Focus**: Understand GDPR terms — Controller vs Processor.
- **Trick**: When asked about data destruction, always choose the method that eliminates ALL residual data.

Quick Revision Notes

- Data Owner classifies → Custodian protects → User accesses
- Govt: Top Secret > Secret > Confidential > Unclassified
- Commercial: Confidential > Private > Sensitive > Public
- Lifecycle: Create > Store > Use > Share > Archive > Destroy
- Degaussing only works on magnetic media — NOT SSDs
- Cryptographic Erasure = destroy the key, data becomes useless
- DLP prevents unauthorized data from leaving the organization
- Data Remanence = leftover data risk after deletion

Practice Questions

Q1: A company is retiring old SSDs. Which data destruction method is MOST appropriate?

A) Degaussing

B) Formatting

C) Physical shredding or overwriting

D) Simply deleting files

✓**Answer: C | SSDs are not magnetic, so degaussing is ineffective. Physical shredding or overwriting with certified tools is required for secure destruction.**

Q2: Who is PRIMARILY responsible for classifying data in an organization?

A) Data Custodian

B) Security Manager

C) Data Owner

D) End User

✓Answer: C | The Data Owner (typically a senior executive) is responsible for classifying data based on its value and sensitivity to the organization.

Q3: A departing employee's laptop drive still contains encrypted company files. The encryption key has been deleted. Is the data accessible?

A) Yes, because files still exist on the drive

B) No, cryptographic erasure makes data unreadable

C) Yes, with forensic tools

D) Only if the drive is physically damaged

✓Answer: B | Cryptographic erasure destroys the key, making encrypted data computationally impossible to recover — a recognized secure destruction method.

Q4: Under GDPR, a marketing firm collects customer data on behalf of an e-commerce company. What role does the marketing firm play?

A) Data Owner

B) Data Controller

C) Data Processor

D) Data Custodian

✓Answer: C | The e-commerce company is the Data Controller (decides purpose). The marketing firm is the Data Processor (processes data on behalf of controller).

DOMAIN 3

Security Architecture and Engineering

Domain Overview

This domain covers designing and building secure systems. It focuses on security models, cryptography, physical security, and cloud security principles. It accounts for 13% of the CISSP exam.

Why it matters: Security must be designed INTO systems — not bolted on. This domain ensures architects make secure design decisions from day one.

★ Most Important Topics

- **Cryptography**: Symmetric, Asymmetric, Hashing
- **Security Models**: Bell-LaPadula, Biba, Clark-Wilson, Brewer-Nash
- **Secure Design Principles**: Least Privilege, Defense in Depth, Fail Secure
- **Trusted Computing Base (TCB)**
- **Physical Security Controls**
- **Cloud Security**: IaaS, PaaS, SaaS shared responsibility
- **Side-Channel Attacks**

Key Concepts

Cryptography Fundamentals

Feature	Symmetric	Asymmetric
Feature	**Symmetric Encryption**	**Asymmetric Encryption**
Keys Used	Same key for encrypt & decrypt	Public key encrypts, Private key decrypts
Speed	FAST	SLOW
Key Exchange	Problem — how to share the key?	No problem — public key is shared openly
Examples	AES, DES, 3DES, Blowfish, RC4	RSA, ECC, Diffie-Hellman, ElGamal
Best For	Bulk data encryption (files, disks)	Key exchange, digital signatures, small data
Key Management	Complex — many keys needed	Simpler — one key pair per user

Key Cryptographic Algorithms

Algorithm	Description
AES	Advanced Encryption Standard — gold standard today. 128/192/256-bit keys.
RSA	Asymmetric. Used for key exchange and digital signatures. Based on factoring large primes.
SHA-256	Hashing algorithm. Produces 256-bit hash. Used to verify integrity.
MD5	Old hash — 128-bit. BROKEN — do not use for security.
DES	Old symmetric — 56-bit. INSECURE today.
3DES	Triple-DES — applies DES 3 times. Slow but more secure than DES.
ECC	Elliptic Curve Cryptography — short keys, strong security. Used in mobile/IoT.
Diffie-Hellman	Key exchange protocol. Allows two parties to create shared secret over insecure channel.

Hashing vs Encryption

Feature	Hashing	Encryption
Purpose	Verify integrity (is data unchanged?)	Protect confidentiality (hide data)
Reversible?	NO — one-way function	YES — can decrypt with key
Examples	SHA-256, MD5, SHA-3	AES, RSA, 3DES
Use Case	Password storage, file verification	Encrypting files, secure communication

Security Models

Model	Focus & Description
Bell-LaPadula	Focuses on CONFIDENTIALITY. No read up, No write down. (Military/Government)
Biba	Focuses on INTEGRITY. No write up, No read down. (Prevents data corruption)
Clark-Wilson	Integrity via well-formed transactions. Used in commercial environments.
Brewer-Nash (Chinese Wall)	Prevents conflicts of interest. Once you work with one company, you can't work with their competitor.

Graham-Denning	Defines how subjects and objects are created/deleted and rights assigned.
Take-Grant	Models how rights can be passed between subjects.

MNEMONIC: Bell-LaPadula = "Write UP, Read DOWN"... WRONG way!
"No Read Up, No Write Down" = guards CONFIDENTIALITY (think: CIA secrets). Biba is the OPPOSITE for INTEGRITY.

Secure Design Principles

Principle	Description
Least Privilege	Give users only the minimum access needed to do their job.
Defense in Depth	Use multiple layers of security — if one fails, another catches the attack.
Fail Secure / Fail Safe	Fail Secure = deny all on failure. Fail Safe = allow all (used for life safety).
Separation of Duties	Split critical tasks between multiple people to prevent fraud.
Need to Know	Access to information only if it is necessary for the job.
Open Design	Security should not rely on secrecy of the design (Kerckhoffs principle).
Economy of Mechanism	Keep security design simple — complex systems have more vulnerabilities.

Physical Security

Control	Purpose
Crime Prevention Through Environmental Design (CPTED)	Design physical environments to deter crime (lighting, visibility, fencing).
Mantrap / Airlock	Double-door system — only one door opens at a time. Prevents tailgating.
Faraday Cage	Metal enclosure that blocks electromagnetic signals. Prevents electronic eavesdropping.
HVAC	Heating/Ventilation/AC — critical for data center temperature control.

Guards + CCTV + Motion Sensors	Layered physical detection and deterrence.
Bollards	Concrete/steel posts — prevent vehicle ramming attacks.

Important Terms & Definitions

Term	Definition
PKI (Public Key Infrastructure)	System for managing digital certificates and public-key encryption.
Digital Certificate	Electronic document that binds a public key to an identity. Issued by a CA.
CA (Certificate Authority)	Trusted entity that issues and manages digital certificates.
TCB (Trusted Computing Base)	All hardware, software, and firmware critical to system security.
Covert Channel	Hidden communication path not intended by system design. Used for data leakage.
Side-Channel Attack	Attack using physical information (power usage, timing, EMF) to extract secrets.
Steganography	Hiding secret data inside ordinary files (images, audio) — "security through obscurity."
Salting	Adding random data to passwords before hashing to prevent rainbow table attacks.

Real-Life Examples

Cloud Security Scenario:
Your company uses AWS (IaaS). Under the Shared Responsibility Model: AWS secures the physical infrastructure, hypervisor, and network. YOU are responsible for OS patches, application security, IAM, and data encryption. Misunderstanding this led to many real-world cloud breaches.

Banking Scenario:
A bank uses the Brewer-Nash (Chinese Wall) model: An analyst who works on Coca-Cola's account is automatically blocked from accessing Pepsi's financial data — preventing conflicts of interest. This is enforced by access control systems that track which "conflict classes" you've accessed.

Exam Tips

 Bell-LaPadula = Confidentiality model (military). Biba = Integrity model (commercial). Know which is which!

- **Trap**: Hashing is NOT encryption. You cannot "decrypt" a hash — it is one-way.
- **Trap**: Fail Secure = deny access (for IT systems). Fail Safe = allow passage (for fire doors).
- **Focus**: Know PKI: CA signs certificates, CRL lists revoked certificates, OCSP provides real-time status.
- **Focus**: Cloud Shared Responsibility — who is responsible in IaaS vs PaaS vs SaaS.
- **Trick**: Asymmetric = "Public locks, Private unlocks" — like a public letterbox.

Quick Revision Notes

- Symmetric = fast, same key; Asymmetric = slow, key pair
- AES = best symmetric; RSA = common asymmetric; SHA-256 = secure hash
- Bell-LaPadula = Confidentiality; Biba = Integrity
- No Read Up + No Write Down = Bell-LaPadula (prevents leaking secrets UP)
- Defense in Depth = multiple security layers
- Least Privilege = minimum access needed
- PKI = CA issues certificates; CRL = revoked certs list
- Mantrap prevents tailgating; Faraday Cage blocks EM signals

Practice Questions

Q1: A system denies all access when a security component fails. This is an example of which principle?

A) Fail Safe

B) Fail Secure

C) Least Privilege

D) Defense in Depth

✓Answer: B | Fail Secure means the system defaults to a denied state on failure, protecting assets. Fail Safe allows access (e.g., fire doors open for life safety).

Q2: An organization needs to ensure that users cannot read information at a higher classification level. Which model enforces this?

A) Biba Model

B) Clark-Wilson Model

C) Bell-LaPadula Model

D) Brewer-Nash Model

✓Answer: C | Bell-LaPadula enforces confidentiality: "No Read Up" prevents subjects from reading data above their clearance level.

Q3: Which encryption type is BEST for encrypting large amounts of data quickly?

A) RSA

B) ECC

C) AES (Symmetric)

D) Diffie-Hellman

✓Answer: C | Symmetric encryption (AES) is much faster than asymmetric for bulk data. Asymmetric is used for key exchange, then symmetric takes over for data.

Q4: A security architect wants to prevent an attacker from using previously captured password hashes. What control is MOST effective?

A) Encryption

B) Salting passwords before hashing

C) Using MD5 hashing

D) Multi-factor authentication

✓Answer: B | Salting adds random data to each password before hashing, making rainbow table attacks ineffective since each identical password produces a unique hash.

DOMAIN 4

Communication and Network Security

Domain Overview

This domain covers how data travels across networks and how to protect it in transit. It covers network protocols, firewalls, VPNs, wireless security, and network architecture. It accounts for 13% of the CISSP exam.

Why it matters: Most attacks happen over networks. Understanding how to design secure networks is critical for any cybersecurity professional.

★ Most Important Topics

- **OSI vs TCP/IP Models** — which layer does what
- **Firewalls**: Packet Filter, Stateful, NGFW, WAF
- **VPN Types**: IPsec, SSL/TLS, Site-to-Site, Remote Access
- **Network Segmentation** and DMZ
- **Wireless Security**: WPA2, WPA3, 802.1X, RADIUS
- **Network Attacks**: ARP Spoofing, MITM, DNS Poisoning, DDoS
- **Network Security Devices**: IDS, IPS, NAC, Proxy

Key Concepts

OSI Model — All 7 Layers

Layer	What Happens Here
7 — **Application**	HTTP, FTP, SMTP, DNS — what the user sees
6 — **Presentation**	Encryption/Decryption, Compression, SSL/TLS
5 — **Session**	Establish, manage, terminate sessions (NetBIOS, RPC)
4 — **Transport**	TCP (reliable), UDP (fast) — port numbers here
3 — **Network**	IP addressing, routing — routers work here
2 — **Data Link**	MAC addresses, switches, frames (ARP, Ethernet)
1 — **Physical**	Cables, hubs, bits — physical transmission

MNEMONIC: OSI Layers (Top to Bottom)
"All People Seem To Need Data Processing" — Application, Presentation, Session, Transport, Network, Data Link, Physical

Firewall Types

Type	How It Works
Packet Filter	Checks IP addresses and ports only. Simple, fast, no state. Layer 3.
Stateful Inspection	Tracks connection state. Smarter than packet filter. Layer 4.
Application-Layer (Proxy)	Understands application content. Can block by content type. Layer 7.
NGFW (Next-Gen Firewall)	Combines stateful + deep packet inspection + IPS + app awareness.
WAF (Web Application Firewall)	Protects web apps specifically. Blocks SQLi, XSS, CSRF. Layer 7.

VPN Protocols

Protocol/Type	Description
IPsec	Gold standard for VPNs. Works at Layer 3. Two modes: Transport (encrypts payload) and Tunnel (encrypts entire packet).
SSL/TLS VPN	Works through web browser (HTTPS). Easy for remote workers. Layer 7.
Site-to-Site VPN	Connects two office networks securely over the internet.
Remote Access VPN	Individual user connects to company network from home/travel.
AH (Authentication Header)	IPsec component — provides integrity and authentication. No encryption.
ESP (Encapsulating Security Payload)	IPsec component — provides encryption + integrity.

Network Segmentation & DMZ

Internet → [Firewall 1] → DMZ → [Firewall 2] → Internal Network

- **DMZ (Demilitarized Zone)**: Network segment between two firewalls. Hosts public-facing servers (web, email, DNS).
- **VLAN**: Virtual LAN — logically segments a network. Reduces broadcast domain size.
- **Network Segmentation**: Separate networks for different sensitivity levels. Limits lateral movement by attackers.

- **Air Gap**: Complete physical isolation — no network connection at all. Used for highly classified systems.

Wireless Security

Standard	Description
WEP	BROKEN — 40/104-bit RC4. Easily cracked. Do not use.
WPA	Better than WEP, TKIP encryption, but still vulnerable.
WPA2	Uses AES encryption. Enterprise mode uses 802.1X/RADIUS.
WPA3	Latest. SAE (Simultaneous Authentication of Equals). Forward secrecy.
802.1X	Port-based Network Access Control. Requires authentication before network access.
RADIUS	Remote Authentication Dial-In User Service — centralized authentication server.
Evil Twin	Fake AP with same SSID — MITM attack on wireless users.

Common Network Attacks

Attack	How It Works
ARP Spoofing	Attacker sends fake ARP replies, linking their MAC to a legitimate IP. Enables MITM.
DNS Poisoning	Corrupt DNS cache to redirect users to malicious sites.
MITM (Man-in-the-Middle)	Attacker intercepts communication between two parties.
DDoS	Overwhelm a server with traffic from many sources — makes it unavailable.
Smurf Attack	Ping broadcast amplification DDoS — floods target with ICMP replies.
SYN Flood	Send many TCP SYN packets, exhausting server's connection table.
Replay Attack	Capture and re-send valid authentication data to gain access.

□ Important Terms & Definitions

Term	Definition
IDS (Intrusion Detection System)	Monitors and ALERTS on suspicious activity. Does NOT block.
IPS (Intrusion Prevention System)	Monitors and BLOCKS suspicious activity inline.
NAC (Network Access Control)	Checks device health before allowing network access (posture check).
Proxy Server	Intermediary between client and internet — hides client identity, filters content.
Bastion Host	Hardened server exposed to the internet, with all unnecessary services removed.
Honeypot	Fake system designed to attract attackers — detects and studies attack methods.
SIEM	Security Information and Event Management — collects and correlates security logs.

Real-Life Examples

SOC Scenario:
A SOC analyst notices ARP spoofing alerts from the SIEM. An attacker on the internal network is sending fake ARP replies, redirecting traffic through their machine. The IPS is configured to automatically block such ARP anomalies. The network is also segmented with VLANs, limiting the blast radius to just one department.

Wireless Scenario:
An employee connects to a hotel Wi-Fi called "Marriott_Free" (Evil Twin attack). The corporate VPN policy requires all traffic to go through the company IPsec VPN — so even if traffic is intercepted, it's encrypted. 802.1X authentication at the office ensures only corporate devices join the internal Wi-Fi.

Exam Tips

IDS = Detect only (passive). IPS = Detect AND Block (inline, active). Know the difference!

- **Trap**: IPsec AH provides integrity but NOT encryption. ESP provides both.
- **Trap**: WEP is broken. WPA2 (AES) is the minimum. WPA3 is best.
- **Focus**: Know each OSI layer and what protocols/attacks apply to it.
- **Focus**: DMZ design — web servers go in DMZ, databases NEVER in DMZ.
- **Trick**: "Stateful = smarter firewall" — it knows if a packet is part of an established session.

Quick Revision Notes

- OSI: Physical, Data Link, Network, Transport, Session, Presentation, Application
- Packet Filter < Stateful < Application < NGFW (complexity = security)
- IPsec: AH = integrity only, ESP = encryption + integrity
- DMZ = between two firewalls; public servers live here
- WEP = broken; WPA2-AES = minimum; WPA3 = best
- IDS = alerts only; IPS = blocks inline
- 802.1X + RADIUS = enterprise wireless authentication
- VLAN = logical segmentation; Air Gap = physical isolation

Practice Questions

Q1: A security engineer wants to protect web applications from SQL injection and XSS attacks. Which device should be deployed?

A) Stateful Firewall

B) IDS

C) Web Application Firewall (WAF)

D) Network IPS

✓Answer: C | WAF operates at Layer 7 and specifically understands HTTP/HTTPS traffic. It can detect and block SQLi, XSS, and other web application attacks.

Q2: An attacker sends a flood of TCP SYN packets to a web server, preventing legitimate connections. What type of attack is this?

A) ARP Spoofing

B) SYN Flood (DDoS)

C) DNS Poisoning

D) Replay Attack

✓Answer: B | A SYN flood exploits the TCP three-way handshake by sending many SYN packets without completing connections, exhausting server resources.

Q3: A company wants to connect two remote offices securely. Which solution is MOST appropriate?

A) Remote Access VPN

B) Site-to-Site IPsec VPN

C) SSL VPN per user

D) WPA3 wireless

✓Answer: B | Site-to-Site IPsec VPN permanently connects two network locations. Remote Access VPN is for individual users, not office-to-office connections.

Q4: Which wireless security protocol provides the strongest protection and is recommended for new deployments?

A) WEP

B) WPA

C) WPA2

D) WPA3

✓Answer: D | WPA3 is the latest standard with SAE (replacing PSK), forward secrecy, and improved protections against offline dictionary attacks. WEP and WPA are insecure.

DOMAIN 5

Identity and Access Management (IAM)

Domain Overview

IAM ensures only the right people, with the right permissions, access the right resources at the right time. This domain accounts for 13% of the CISSP exam and covers identity lifecycle, authentication methods, and access control models.

Why it matters: Most breaches involve compromised credentials or excessive permissions. Strong IAM is your first line of defence.

★ Most Important Topics

- **Authentication Factors**: Something you know/have/are/do/somewhere
- **Access Control Models**: DAC, MAC, RBAC, ABAC, Rule-Based
- **Single Sign-On (SSO)** and Federation
- **Privileged Access Management (PAM)**
- **Zero Trust Architecture**
- **Directory Services**: LDAP, Active Directory
- **OAuth 2.0, SAML, OpenID Connect**

Key Concepts

Authentication Factors

Factor Type	Examples
Something You Know	Password, PIN, passphrase, security questions
Something You Have	Smart card, hardware token (RSA SecurID), OTP app, key fob
Something You Are	Biometrics: fingerprint, retina, face, voice recognition
Something You Do	Typing rhythm, gait analysis, behavioral biometrics
Somewhere You Are	Geolocation-based — access from specific IP or location

MFA (Multi-Factor Authentication) = using 2 or more DIFFERENT factor types. Two passwords = NOT MFA.

Access Control Models

Model	How It Works & Use Case

DAC (Discretionary)	Owner controls access. "I decide who reads my file." Used in most OS (Windows, Linux file permissions).
MAC (Mandatory)	System enforces labels. Owner CANNOT change access. Used in government/military (Top Secret, Secret).
RBAC (Role-Based)	Access based on job role. "Finance team gets finance systems." Most common in corporations.
ABAC (Attribute-Based)	Access based on multiple attributes (time, location, device, user attributes). Very flexible.
Rule-Based	Access based on predefined rules (firewall ACLs — "allow port 443 from any").

MNEMONIC: Access Control Models
"DAC = Discretionary (owner decides), MAC = Mandatory (label decides), RBAC = Role decides, ABAC = Attributes decide" — Think of D-M-R-A as Dear Manager, Rules Apply!

Biometric Accuracy

Metric	What It Means
FAR (False Acceptance Rate)	System lets in an UNAUTHORIZED user. Very dangerous — security risk.
FRR (False Rejection Rate)	System rejects an AUTHORIZED user. Usability problem — inconvenient.
CER/EER (Crossover Error Rate)	Point where FAR = FRR. Lower CER = more accurate biometric system.

When comparing biometric systems, choose the one with the LOWEST CER — it means the best overall accuracy.

SSO, Federation & Identity Protocols

Protocol/Concept	Description
SSO (Single Sign-On)	Log in once, access all systems. Convenient but single point of failure.
SAML	XML-based standard for exchanging authentication data. Used for enterprise SSO.
OAuth 2.0	Authorization framework — allows apps to access resources without sharing passwords. (Login with Google)

OpenID Connect	Authentication layer on top of OAuth 2.0. Provides identity tokens.
Kerberos	Ticket-based authentication. Used in Windows Active Directory. Requires a KDC (Key Distribution Center).
LDAP	Protocol for accessing directory services (like Active Directory). Stores user accounts and groups.
Federation	Trust between organizations — use your company credentials to access a partner's system.

Privileged Access Management

- **PAM**: Tools and processes to manage, monitor, and control privileged accounts (admin, root, service accounts).
- **Principle of Least Privilege**: Give minimum access needed. Review regularly.
- **Just-In-Time (JIT) Access**: Grant privileged access only when needed, automatically revoke after.
- **Separation of Duties**: No single person should have complete control over a critical process.
- **Account Lifecycle**: Provisioning → Use → Review → Deprovision (remove when no longer needed).

Zero Trust Architecture

"Never Trust, Always Verify"

- Assume breach — treat every request as if it comes from an untrusted network.
- Verify explicitly — always authenticate and authorize based on all available data.
- Use least privilege access — limit user access with just-in-time and just-enough-access.
- Microsegmentation — granular perimeters to contain breach impact.

Important Terms & Definitions

Term	Definition
Identification	Claiming an identity ("I am Krishna")
Authentication	Proving the claimed identity ("Here is my password")
Authorization	What you are allowed to do after authentication ("You can read files")
Accountability	Tracking actions to an individual — requires unique identities

Non-repudiation	Cannot deny an action was taken — digital signatures provide this
Provisioning	Creating and setting up a user account with appropriate access
Deprovisioning	Removing access when a user leaves or changes roles

Real-Life Examples

Corporate IAM Scenario:
A new employee joins the Finance department. HR triggers provisioning: Active Directory creates an account, RBAC assigns the "Finance" role (read-only to accounting systems). MFA is enforced via Microsoft Authenticator. When the employee leaves, deprovisioning removes all access within 24 hours. PAM tools ensure admin accounts are only used with approval and full session recording.

Exam Tips

Identification → Authentication → Authorization — this ORDER is always the same. Never skip steps.

- **Trap**: OAuth is for AUTHORIZATION, not authentication. OpenID Connect adds authentication.
- **Trap**: Two passwords = single-factor (both are "something you know"). MFA needs DIFFERENT factor types.
- **Focus**: Know which access control model fits which scenario (MAC = military, RBAC = corporate, DAC = files).
- **Focus**: CER — lower is better for biometrics.
- **Trick**: Kerberos uses TICKETS, not passwords, for subsequent authentication after initial login.

Quick Revision Notes

- Authentication factors: Know, Have, Are, Do, Somewhere
- MFA = different factor types; 2 passwords = NOT MFA
- DAC = owner controls; MAC = labels/system controls; RBAC = roles
- SSO = once login; SAML = enterprise SSO standard
- OAuth 2.0 = authorization; OpenID Connect = authentication
- Kerberos = tickets, KDC; LDAP = directory protocol
- CER/EER — lower = better biometric accuracy
- Zero Trust = Never trust, always verify
- Identification → Authentication → Authorization → Accountability

Practice Questions

Q1: A user swipes a badge AND scans their fingerprint to enter a data center. This is an example of:

A) Single-factor authentication

B) Multi-factor authentication

C) Two-factor identification

D) Biometric identification

✓Answer: B | Badge = Something You Have. Fingerprint = Something You Are. Two different factor types = Multi-Factor Authentication (MFA).

Q2: A military system automatically assigns access based on classification labels that users cannot change. This is:

A) DAC

B) RBAC

C) MAC

D) ABAC

✓Answer: C | MAC (Mandatory Access Control) uses system-enforced labels. Users cannot modify access permissions. Common in government and military environments.

Q3: You compare two biometric systems. System A has a CER of 5%, System B has a CER of 12%. Which is more accurate?

A) System B — higher CER means better detection

B) System A — lower CER means better overall accuracy

C) They are equivalent

D) Cannot determine without FAR data

✓Answer: B | Lower CER (Crossover Error Rate) = better accuracy. System A (5%) is more accurate than System B (12%).

Q4: A company uses "Login with Google" on their partner portal. Which protocol enables this WITHOUT sharing the user's Google password with the partner site?

A) LDAP

B) Kerberos

C) SAML

D) OAuth 2.0 with OpenID Connect

✓Answer: D | OAuth 2.0 enables authorization (access delegation) without sharing passwords. OpenID Connect adds identity verification (who the user is).

DOMAIN 6

Security Assessment and Testing

Domain Overview

This domain covers how organizations test and verify that their security controls are working. It includes penetration testing, vulnerability assessments, audits, and security metrics. It accounts for 12% of the CISSP exam.

Why it matters: Controls that are never tested may not work. Regular testing finds gaps before attackers do.

★ Most Important Topics

- **Vulnerability Assessment vs Penetration Testing**
- **Pen Testing Types**: Black Box, White Box, Gray Box
- **Security Audits** and review types
- **Testing Methodologies**: OWASP, PTES, NIST
- **Code Review**: SAST vs DAST
- **Log Reviews & SIEM**
- **Key Metrics**: MTTD, MTTR, MTTF, MTBF

Key Concepts

Vulnerability Assessment vs Penetration Testing

Feature	Vulnerability Assessment	Penetration Testing
Feature	**Vulnerability Assessment**	**Penetration Testing**
Goal	Find weaknesses	Actively exploit weaknesses
How	Automated scanning + manual review	Simulate real attacks step by step
Tools	Nessus, Qualys, OpenVAS	Metasploit, Burp Suite, Nmap
Risk	Low risk	Higher risk (could disrupt systems)
Output	List of vulnerabilities	Proof of exploitation + business impact
Frequency	Regular (monthly/quarterly)	Less frequent (annually)
Authorization	Required	MUST have written authorization

Penetration Testing Types

Type	Description
Black Box	Tester has NO prior knowledge. Simulates external attacker. Realistic.
White Box	Tester has FULL knowledge (source code, architecture). Thorough but not realistic.
Gray Box	Tester has PARTIAL knowledge. Balance of realism and depth.
Crystal Box	Another name for White Box testing.

Penetration Testing Phases

Planning → Reconnaissance → Scanning → Exploitation → Post-Exploitation → Reporting

Phase	What Happens
Planning	Define scope, rules of engagement, authorization. Get written permission!
Reconnaissance	Gather information passively (OSINT) and actively (port scans).
Scanning	Port scanning (Nmap), vulnerability scanning (Nessus), service fingerprinting.
Exploitation	Use findings to gain access. Metasploit, Burp Suite, custom scripts.
Post-Exploitation	Privilege escalation, lateral movement, data exfiltration, persistence.
Reporting	Document findings, business impact, and remediation recommendations.

SAST vs DAST

Feature	SAST	DAST
Feature	**SAST (Static Analysis)**	**DAST (Dynamic Analysis)**
When	Before code runs (source code)	While application is running
How	Analyze code for vulnerabilities	Test running app by sending inputs

Tools	Fortify, Checkmarx, SonarQube	OWASP ZAP, Burp Suite, Acunetix
Finds	Logic flaws, insecure code patterns	Runtime issues, injection, auth flaws
Developer Access	Yes — needs source code	No — treats app as black box
Speed	Fast — done in CI/CD pipeline	Slower — needs running instance

Security Metrics

Metric	Definition
MTTD (Mean Time To Detect)	Average time to detect a security incident.
MTTR (Mean Time To Respond)	Average time to respond and contain an incident.
MTTF (Mean Time To Failure)	Average time before a system fails (non-repairable).
MTBF (Mean Time Between Failures)	Average time between failures for a repairable system.
RTO (Recovery Time Objective)	Target time to restore after an incident.
RPO (Recovery Point Objective)	Maximum acceptable data loss in time.

Audit Types

Type	Description
Internal Audit	Done by internal staff. Less independent but more frequent.
External Audit	Done by independent third party. More credible and objective.
First-Party Audit	Organization audits itself (self-assessment).
Second-Party Audit	Customer audits supplier/vendor.
Third-Party Audit	Independent auditor. Most credible (ISO 27001 certification).
SOC 2 Report	Independent audit of service organization's controls (security, availability, privacy).

□ MNEMONIC: SAST vs DAST

"SAST = Sleeping app (static code review). DAST = Dancing app (running, dynamic testing)."

Real-Life Examples

Security Assessment Scenario:
At Bridgestone America, before every major release, the security team runs Fortify SAST on the source code (finding SQLi patterns), then OWASP ZAP DAST on the staging environment (finding authentication bypass). A quarterly Nessus scan checks for known CVEs. Once a year, an external pen test team is hired for black-box testing. All findings go into a risk register and tracked for remediation.

Exam Tips

Always get WRITTEN AUTHORIZATION before penetration testing. This is legally critical — unauthorized testing is a crime.

- **Trap**: Vulnerability assessment finds vulnerabilities. Pen test EXPLOITS them. Different goals!
- **Focus**: Know SAST = source code review; DAST = running application testing.
- **Focus**: Know all key metrics — MTTD, MTTR, MTTF, MTBF — and what they measure.
- **Trick**: Black Box = most realistic but misses deep issues. White Box = most thorough but least realistic.
- **Exam Trap**: "First thing in pen testing" = always PLANNING and getting written authorization.

Quick Revision Notes

- VA = find vulnerabilities; Pen Test = exploit them (written auth required!)
- Black Box = no knowledge; White Box = full knowledge; Gray Box = partial
- SAST = static/code; DAST = dynamic/running
- Fortify = SAST tool; Burp Suite/ZAP = DAST tools; Nessus = scanner
- MTTD = detect; MTTR = respond; MTBF = between failures; MTTF = to failure
- Internal audit = less credible; Third-party = most credible
- Pen test phases: Plan > Recon > Scan > Exploit > Post-Exploit > Report

Practice Questions

Q1: A security team wants to test if attackers can actually steal customer data from their web app. What is the MOST appropriate approach?

A) Run a Nessus vulnerability scan

B) Conduct a black-box penetration test

C) Review application source code with SAST

D) Perform a log review

✓Answer: B | Penetration testing simulates actual attacks to prove exploitability. A black-box test most realistically simulates an external attacker. Vulnerability scans only identify — they don't exploit.

Q2: A developer wants to find SQL injection vulnerabilities in source code BEFORE deployment. Which tool type is MOST appropriate?

A) DAST tool

B) IDS

C) SAST tool

D) Fuzzer

✓Answer: C | SAST (Static Application Security Testing) analyzes source code without running it. It's ideal for early detection in the development pipeline before deployment.

Q3: The FIRST thing a penetration tester should do before starting any test is:

A) Run Nmap to discover hosts

B) Obtain written authorization from the client

C) Check for known CVEs

D) Interview system administrators

✓Answer: B | Written authorization is legally required before any penetration testing activity. Without it, the tester is committing an unauthorized access crime.

Q4: A security manager wants to measure how quickly the team identifies incidents. Which metric is MOST relevant?

A) MTTR

B) MTBF

C) MTTD

D) RPO

✓Answer: C | MTTD (Mean Time To Detect) measures the average time to identify a security incident. MTTR measures response time after detection.

DOMAIN 7
Security Operations

Domain Overview

Security Operations is the day-to-day work of keeping an organization secure. It covers incident response, monitoring, disaster recovery, and operational security controls. This is the second-largest domain at 13% of the exam.

Why it matters: A great security design fails without proper operational execution. This domain covers what happens after systems are deployed.

★ Most Important Topics

- **Incident Response Lifecycle** (NIST)
- **Logging & Monitoring** — SIEM, log management
- **Change Management** process
- **Configuration Management**
- **Vulnerability Management** lifecycle
- **DRP & BCP** (tested here too)
- **Security Controls**: Preventive, Detective, Corrective, Compensating

Key Concepts

Incident Response Lifecycle (NIST)

Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned

Phase	What Happens
Preparation	Build IR team, tools, playbooks, train staff BEFORE incidents happen.
Detection & Analysis	Identify the incident — use SIEM, IDS/IPS, user reports. Determine scope.
Containment	Stop the spread. Short-term (isolate system) and long-term (patch).
Eradication	Remove the root cause — delete malware, close vulnerability.
Recovery	Restore systems to normal operations. Monitor closely.
Lessons Learned	Post-incident review — what happened? How to prevent next time? Update playbooks.

MNEMONIC: Incident Response = PDCEER-L
"Please Don't Call Every Emergency Response Late" — Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned

Security Control Types

Control Type	Purpose & Examples
Preventive	STOP an incident before it happens. Firewall, Access Control, Training.
Detective	FIND an incident when it occurs. IDS, CCTV, Audit Logs.
Corrective	FIX the damage after an incident. Patching, Restoring backups.
Deterrent	DISCOURAGE attackers. Warning signs, penalties, visible cameras.
Compensating	Alternative control when primary isn't possible. Used for compliance workarounds.
Recovery	RESTORE operations after incident. DRP, hot/warm/cold sites.
Directive	GUIDE behavior through policies, rules, contracts.

Logging and Monitoring

- **SIEM (Security Information & Event Management)**: Collects, normalizes, correlates logs. Generates alerts.
- **Log Sources**: Firewalls, servers, endpoints, applications, network devices.
- **Log Integrity**: Logs must be tamper-proof. Send to centralized, protected SIEM.
- **Retention**: Logs must be kept for required period (depends on compliance — PCI-DSS requires 1 year).
- **NTP (Network Time Protocol)**: Synchronize all system clocks — critical for log correlation and forensics.

Change Management Process

Request → Review → Approval (CAB) → Testing → Implementation → Documentation → Review

- **CAB (Change Advisory Board)**: Group that reviews and approves changes before implementation.
- **Emergency Change**: Expedited process for critical fixes — still requires documentation and post-review.

- **Rollback Plan**: Every change must have a plan to undo it if something goes wrong.

Recovery Site Types

Site Type	Description
Hot Site	Fully operational duplicate. Can switch in MINUTES. Most expensive.
Warm Site	Partially equipped. Takes HOURS to days. Middle cost.
Cold Site	Empty building with power/network. Takes DAYS to weeks. Cheapest.
Mobile Site	Portable/trailer-based recovery facility.
Reciprocal Agreement	Two organizations agree to host each other in an emergency. Inexpensive but risky.
Cloud Recovery	Use cloud infrastructure for DR. Increasingly common — fast and scalable.

Vulnerability Management Lifecycle

Discover → Prioritize → Assess → Report → Remediate → Verify

- **CVSS Score**: Common Vulnerability Scoring System. 0–10. 9–10 = Critical, 7–8.9 = High.
- **CVE**: Common Vulnerabilities and Exposures — unique IDs for known vulnerabilities.
- **Patch Management**: Regular patching cycle — critical patches within 24-72 hours ideally.

Important Terms & Definitions

Term	Definition
Chain of Custody	Documentation tracking evidence handling from collection to court.
Order of Volatility	Collect most volatile evidence first: RAM > Swap > Disk > Logs.
IOC (Indicator of Compromise)	Evidence of a breach: suspicious IP, malware hash, unusual login.
TTPs (Tactics, Techniques, Procedures)	How attackers operate — used to understand and detect threats.
Threat Hunting	Proactive search for hidden threats not caught by automated tools.

SOC (Security Operations Center)	24/7 team monitoring and responding to security events.
CSIRT	Computer Security Incident Response Team — handles incident management.

Real-Life Examples

Incident Response Scenario:
A SOC analyst at a SaaS company sees an alert in ArcSight SIEM: unusual outbound data transfer at 2 AM. Detection phase confirms ransomware. Containment: network segment is immediately isolated. Eradication: malware removed, systems rebuilt from clean backups. Recovery: services restored in 6 hours (within RTO). Lessons learned meeting identifies that the initial phishing email was not caught by email filters — controls are updated.

Exam Tips

In forensics, ALWAYS preserve evidence first before analyzing. Never work on original evidence — work on a forensic copy.

- **Trap**: In incident response, CONTAINMENT comes before ERADICATION. Stop the spread first.
- **Focus**: Order of evidence volatility: RAM first (most volatile), then disk, then logs, etc.
- **Trap**: A "cold site" is NOT secure by itself — it's just a facility. You must bring everything.
- **Focus**: Change Management — CAB must APPROVE before implementation. Never skip this.
- **Trick**: Detective + Preventive + Corrective = the core control triad to remember.

Quick Revision Notes

- IR phases: Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned
- Preventive = stop; Detective = find; Corrective = fix; Compensating = alternative
- Hot site = minutes; Warm = hours; Cold = days
- SIEM = collect + correlate logs + alert
- NTP = synchronize clocks for accurate log correlation
- Chain of Custody = evidence documentation trail
- Order of volatility: RAM > Swap > Disk > Logs
- CVSS: 9-10 = Critical, 7-8.9 = High

Practice Questions

Q1: During an active ransomware attack, what is the MOST important immediate action?

A) Eradicate the malware

B) Notify law enforcement

C) Contain the affected systems

D) Perform forensic analysis

✓Answer: C | Containment stops the spread. Before eradicating, you must contain. Forensics and notifications come after the immediate threat is controlled.

Q2: A forensic investigator must collect evidence from a compromised server. What should be collected FIRST?

A) Hard drive image

B) Network logs

C) RAM contents

D) Application logs

✓Answer: C | Order of volatility: RAM is most volatile (lost when power off). It must be captured FIRST. Hard drive data persists longer.

Q3: An organization needs to recover operations within 15 minutes of a disaster. Which recovery site is MOST appropriate?

A) Cold Site

B) Warm Site

C) Mobile Site

D) Hot Site

✓Answer: D | Hot sites are fully operational and can take over in minutes. Cold sites take days; warm sites take hours. 15-minute RTO requires a hot site.

Q4: A security guard watching CCTV cameras is an example of which type of control?

A) Preventive

B) Detective

C) Corrective

D) Compensating

✓Answer: B | CCTV + a guard watching it is a detective control — it detects incidents while they occur. A fence or lock would be preventive.

DOMAIN 8

Software Development Security

Domain Overview

This domain covers integrating security into the software development process — from design to deployment. It ensures that security is built into code, not patched in later. It accounts for 10% of the CISSP exam.

Why it matters: Vulnerabilities in software are the #1 entry point for attackers. Secure development practices save enormous costs — fixing a bug in production costs 30x more than fixing it in design.

★ Most Important Topics

- **SDLC (Software Development Lifecycle)** phases
- **Secure Coding Practices** & OWASP Top 10
- **DevSecOps** — integrating security in CI/CD
- **SAST, DAST, SCA** — types of code testing
- **Database Security**: SQL Injection prevention
- **API Security**
- **Software Supply Chain Security**

Key Concepts

SDLC Phases

Phase	Security Activities
Planning	Define requirements, scope, and security objectives.
Requirements	Gather functional AND security requirements. Threat modelling starts here.
Design	Architect secure systems. Apply security design principles (least privilege, defense in depth).
Development / Coding	Write code following secure coding standards. Peer code reviews.
Testing	SAST, DAST, SCA, pen testing, code review. QA and security testing.
Deployment / Release	Secure deployment. Configuration management. Change control.
Maintenance / Operations	Patch management, vulnerability scanning, monitoring.

Decommission	Secure disposal — sanitize data, remove access, document.

SDLC Models

Model	Description
Waterfall	Linear. Each phase completes before next. Hard to go back. Less flexible.
Agile	Iterative sprints. Continuous delivery. Security must be in each sprint.
Spiral	Risk-driven. Good for high-risk projects. Prototyping + testing each loop.
DevOps / DevSecOps	Dev + Ops + Security working together. Continuous integration and delivery with security built in.
RAD (Rapid Application Development)	Focus on quick prototyping, less formal planning.

OWASP Top 10 — Most Common Web Vulnerabilities

Vulnerability	Description
A01: Broken Access Control	Users access data/functions beyond their permissions.
A02: Cryptographic Failures	Weak or missing encryption (e.g., storing passwords in plain text).
A03: Injection	SQL injection, OS command injection — untrusted data sent to interpreter.
A04: Insecure Design	Security not considered in design phase — no threat modelling.
A05: Security Misconfiguration	Default passwords, open cloud storage, unnecessary services enabled.
A06: Vulnerable Components	Using outdated libraries with known CVEs (supply chain risk).
A07: Auth Failures	Broken authentication — weak passwords, no MFA, session management issues.
A08: Software/Data Integrity Failures	Untrusted code updates, insecure deserialization.
A09: Logging Failures	Insufficient logging means breaches go undetected.

A10: SSRF	Server-Side Request Forgery — server makes unintended requests.

Secure Coding Practices

- **Input Validation**: Never trust user input. Validate on the server side, not just client side.
- **Parameterized Queries**: Prevent SQL injection — use prepared statements instead of string concatenation.
- **Output Encoding**: Encode output to prevent XSS attacks.
- **Error Handling**: Don't reveal internal system details in error messages.
- **Principle of Least Privilege**: Code should run with minimum required permissions.
- **Secure Defaults**: Systems should be secure out of the box — insecurity requires effort to enable.
- **Defense in Depth**: Multiple validation layers — don't rely on a single check.

Database Security

Concept	Description
SQL Injection	Attacker injects malicious SQL via input. Prevented by parameterized queries.
Polyinstantiation	Multiple copies of data with different classifications shown based on clearance.
Database Encryption	Encrypt sensitive columns or entire database. Protects at-rest data.
Views	Restrict what columns/rows a user can see — enforces least privilege in DB.
Stored Procedures	Encapsulate business logic; can reduce SQL injection surface.
Aggregation Attack	Combining non-sensitive data to derive sensitive info.
Inference Attack	Deducing sensitive info from non-sensitive query responses.

DevSecOps & CI/CD Security

- **Shift Left**: Move security testing earlier in SDLC — catch bugs in code, not production.
- **CI/CD Pipeline Security**: Integrate SAST, SCA, secrets scanning automatically in every commit.
- **SCA (Software Composition Analysis)**: Scan open-source libraries for known vulnerabilities.
- **Secrets Management**: Never hardcode API keys, passwords in source code. Use Vault, AWS Secrets Manager.
- **Container Security**: Scan Docker images for vulnerabilities. Use minimal base images.

MNEMONIC: OWASP Top 3 = BAI
"Bad Access Is Insecure" — Broken Access Control, Cryptographic failures (A02), Injection (A03) — the top 3 most critical.

Important Terms & Definitions

Term	Definition
Threat Modelling	Identify potential threats early in design. STRIDE is a common methodology.
STRIDE	Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation of Privilege.
Code Review	Manual or automated review of source code to find security issues.
Fuzzing	Send random/unexpected inputs to find crashes or unexpected behavior.
Penetration Testing	Simulate attacks on a live system to find exploitable vulnerabilities.
Software Supply Chain	All components, libraries, and tools used to build software — must be verified.
SBoM (Software Bill of Materials)	List of all components in software — helps identify vulnerable dependencies.

Real-Life Examples

DevSecOps Scenario:
At OpenText, every code commit triggers: (1) Fortify SAST scan for insecure code patterns, (2) SCA scan for vulnerable open-source libraries (e.g., Log4Shell CVE), (3) Secrets scanner to find hardcoded API keys. The results are reviewed before the PR is approved. DAST runs nightly on the staging environment using OWASP ZAP. This "shift left" approach catches 80% of vulnerabilities before they reach production.

Database Security Scenario:
A login form uses string concatenation: SELECT * FROM users WHERE username = input. An attacker enters: admin OR 1=1, which bypasses authentication. Fix: use parameterized queries so input is never executed as SQL code.

Exam Tips

OWASP Top 10 A01 (Broken Access Control) is the #1 vulnerability. Injection (A03) is the classic CISSP exam topic.

- **Focus**: Know ALL SDLC phases and what security activities happen in each.
- **Trick**: "Shift Left" = move security testing earlier = cheaper to fix.
- **Trap**: Validation on client-side only is useless — attackers bypass browsers. Always validate server-side.
- **Focus**: STRIDE for threat modelling — know each letter.
- **Trick**: Aggregation attack = combining non-sensitive pieces to learn sensitive info (like putting puzzle together).

Quick Revision Notes

- SDLC: Plan > Require > Design > Code > Test > Deploy > Maintain > Decommission
- OWASP Top 3: Broken Access Control, Cryptographic Failures, Injection
- SQL Injection prevention: Parameterized queries / Prepared statements
- Shift Left = find bugs early = cheaper fixes
- SAST = source code; DAST = running app; SCA = open-source components
- DevSecOps = security integrated into every CI/CD step
- STRIDE: Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation
- Never hardcode secrets — use secret management tools
- Aggregation: combining non-sensitive data to find sensitive info

Practice Questions

Q1: A developer uses string concatenation to build SQL queries with user input. What vulnerability is MOST likely?

A) Cross-Site Scripting

B) SQL Injection

C) Broken Access Control

D) Buffer Overflow

✓**Answer: B | String concatenation with user input directly into SQL queries is the classic cause of SQL Injection. Fix: use parameterized queries / prepared statements.**

Q2: An attacker combines employee names, departments, and salary ranges from multiple non-confidential reports to infer individual salaries. This is:

A) Inference Attack

B) Aggregation Attack

C) SQL Injection

D) Data Mining

✓Answer: B | Aggregation attack = combining multiple non-sensitive pieces of information to derive sensitive information that shouldn't be accessible.

Q3: Security testing is integrated into every CI/CD pipeline commit. This approach is called:

A) Agile Security

B) Waterfall Testing

C) DevSecOps (Shift Left)

D) Penetration Testing

✓Answer: C | DevSecOps (Shift Left) means integrating security into every phase of development, including automated testing in CI/CD pipelines at every code commit.

Q4: During threat modelling, the team identifies a risk of an attacker denying they sent a malicious request. Which STRIDE category is this?

A) Spoofing

B) Repudiation

C) Tampering

D) Info Disclosure

✓Answer: B | Repudiation (the R in STRIDE) = attacker denies performing an action. Countermeasure: audit logs and non-repudiation controls like digital signatures.

Q5: An organization is concerned about vulnerabilities in third-party libraries used in their application. What is the MOST effective control?

A) SAST scanning of own code

B) SCA (Software Composition Analysis)

C) DAST testing

D) Code review of internal functions

✓Answer: B | SCA specifically scans third-party and open-source components for known CVEs. SAST only analyzes first-party source code.

ALL 8 DOMAINS — MASTER CHEAT SHEET

Last-Day Revision Summary

Domain	Key Exam Points
Domain 1 — Security & Risk Management (15%)	CIA Triad | ALE=SLE×ARO | Accept/Transfer/Mitigate/Avoid | BCP vs DRP | RTO/RPO | Policy>Standard>Guideline
Domain 2 — Asset Security (10%)	Owner classifies, Custodian protects | Govt: TS>S>C>U | Lifecycle: Create→Destroy | Degauss=magnetic only | Crypto Erasure
Domain 3 — Security Architecture (13%)	BLP=Confidentiality, Biba=Integrity | AES=fast symmetric | SHA=hash | Fail Secure=deny | Defense in Depth
Domain 4 — Network Security (13%)	OSI 7 layers | IDS=detect, IPS=block | IPsec AH=auth, ESP=encrypt | WPA3=best | DMZ=between 2 firewalls
Domain 5 — IAM (13%)	DAC=owner, MAC=labels, RBAC=roles | MFA=different factors | SSO+SAML | CER lower=better | Zero Trust
Domain 6 — Assessment & Testing (12%)	VA=find, PenTest=exploit | Written auth FIRST | SAST=code, DAST=running | MTTD=detect, MTTR=respond
Domain 7 — Security Operations (13%)	IR: Prep>Detect>Contain>Eradicate>Recover>Lessons | Hot=minutes, Cold=days | RAM first (volatility) | SIEM
Domain 8 — Software Dev Security (10%)	SDLC phases | OWASP Top 10 | SQL Injection=param queries | Shift Left | DevSecOps | STRIDE

✨You've got this! Best of luck on your CISSP exam! ✨

Krishna Chandra Muduli, CISSP | krishnamuduli.co.in/learning_hub.html