THREATNEXIS

CISSP Memory Techniques & Mnemonics

FREE EDITION — All 8 Domains

Stop memorizing. Start remembering.

How to Use This Guide

The CISSP exam has 125–175 questions. You cannot memorize your way to a pass — but you CAN build memory systems that make the right answer feel obvious. This guide gives you a mnemonic, analogy, or memory anchor for every major CISSP concept.

Each memory device is designed to do two things: get the answer into your head, and get it back out under exam pressure. Read them. Say them out loud. Teach them to someone else. That's the system.

👔 The One Rule That Beats Every Mnemonic

Think like a manager, not an engineer. Before you recall any formula or model, ask: 'What decision would a senior security executive make here?' That mindset is the master key. Every mnemonic in this guide is a shortcut to that mindset.

DOMAIN 1 | SECURITY & RISK MANAGEMENT

Risk Treatment — MATA

🧠 **The 4 Risk Treatment Options**

MATA

M — Mitigate — reduce probability or impact with a control
A — Accept — formally document and accept the residual risk
T — Transfer — pass risk to a third party (insurance, contract)
A — Avoid — stop the risky activity entirely

> 💡 *EXAM TIP: On the exam: 'formally document' is the key phrase for risk acceptance. Undocumented acceptance = negligence.*

CIA Triad — The Foundation

🧠 **Confidentiality · Integrity · Availability**

CIA

C — Confidentiality — only authorized eyes see it
I — Integrity — nobody changed it without permission
A — Availability — it's there when you need it

🏦 **The Bank Vault Analogy**

CIA is your bank. Confidentiality = only you can open your safe deposit box. Integrity = the contents haven't been tampered with. Availability = the bank is open when you need it.

Policy Hierarchy — PSGPB

🧠 **Policy Hierarchy (Top to Bottom)**

Please Stop Giving People Burdens

P — Policy — the law of the org (mandatory, high-level)

S — Standards — specific requirements (mandatory)
G — Guidelines — helpful suggestions (optional)
P — Procedures — step-by-step how-to (mandatory when used)
B — Baselines — minimum security configurations

💡 *EXAM TIP: Policy and Standards are MANDATORY. Guidelines are OPTIONAL. This distinction appears on virtually every CISSP exam.*

Due Care vs. Due Diligence

🚗 **The Used Car Analogy**

Due Diligence = researching the car's history on CarFax BEFORE you buy it. Due Care = changing the oil, rotating the tires, and maintaining it AFTER you own it. Diligence is research. Care is action.

🧠 **Due Diligence = Doing your Homework. Due Care = Doing it Right.**

DD

Due Diligence — investigating risks BEFORE acting (research phase)
Due Care — acting responsibly AFTER the decision (maintenance phase)

Memory hook: 'Diligence before the Deal. Care after the Contract.'

(ISC)² Ethics Canons — Priority Order

🧠 **Ethics Canon Priority (Highest → Lowest)**

SHAL

S — Society — protect the public first, always (Canon 1)
H — Honor — act honestly and lawfully (Canon 2)
A — Ability — provide competent service (Canon 3)
L — Legacy — advance the profession (Canon 4)

Society beats employer beats client beats profession.

💡 *EXAM TIP: When society conflicts with your employer: society wins. This is the most commonly tested ethics scenario.*

ALE Formula Chain

🧠 **Quantitative Risk Formulas**

ALE = SLE × ARO

AV × EF = SLE (Single Loss Expectancy)
SLE × ARO = ALE (Annualized Loss Expectancy)

AV = Asset Value (what is it worth?)
EF = Exposure Factor (% lost in one event, 0.0–1.0)
ARO = Annualized Rate of Occurrence (events per year)

Memory: 'Assets Exposed = Single Loss. Single Loss × Annual Rate = Annual Loss.'

📐 **Quick Example**

Server worth $100k. Fire destroys 40% of it. SLE = $100k × 0.40 = $40k. Fire happens every 10 years: ARO = 0.10. ALE = $40k × 0.10 = $4,000 per year expected loss.

DOMAIN 2 | ASSET SECURITY

Data Roles — ODES

🧠 Who Does What with Data

ODES

O — Owner — the BUSINESS manager; classifies data; assigns access
D — Downline Custodian — IT staff; IMPLEMENTS controls
E — End User (Subject) — the individual the data is about
S — Steward — manages data quality and governance

Owner decides. Custodian implements. Never confuse them.

🏢 The Office Building Analogy

The data owner is the CEO who decides who gets a key card to the executive floor. The data custodian is the facilities manager who programs the key cards and maintains the lock system. The CEO doesn't program the locks; the facilities manager doesn't decide who gets access.

Data States — RUT

🧠 The Three States of Data

RUT

R — Rest — stored data (hard drives, databases, backups)
U — Use — actively in memory (RAM, CPU registers)
T — Transit — moving across a network

Every data state needs its own protection strategy.

State	Where	Primary Control
At Rest	Storage, database	Encryption at rest, access control
In Use	RAM, CPU cache	Access control, memory protection
In Transit	Network, internet	TLS, VPN, encryption in transit

Data Destruction — CPD

🧠 Data Destruction Methods (Increasing Permanence)

CPD

C — Clearing — overwrite; media can be reused WITHIN org
P — Purging — degauss or multiple overwrites; media can leave org
D — Destruction — physical shred/burn; no reuse possible

SSDs: overwriting is unreliable. Use cryptographic erasure or physical destruction.

DOMAIN 3 | SECURITY ARCHITECTURE & ENGINEERING

Security Models — The Big Four

🧠 Security Models Quick Map

B-B-C-B

Bell-LaPadula — Confidentiality — No Read Up, No Write Down
Biba — Integrity — No Write Up, No Read Down
Clark-Wilson — Integrity (commercial) — Separation of duties
Brewer-Nash — Conflict of interest — Chinese Wall

Memory: 'Beautiful Bikinis Cover Bodies'

🔐 Bell-LaPadula — The Classified Document Rule

You are a SECRET-cleared analyst. Bell-LaPadula says: Don't Read Up (you can't read TOP SECRET files — No Read Up). Don't Write Down (you can't paste SECRET data into an UNCLASSIFIED document — No Write Down). Confidentiality flows UPWARD.

✏️ Biba — The Data Quality Rule

You are a surgeon. Biba says: Don't Write Up (don't write instructions to a higher-authority medical board without verification — No Write Up). Don't Read Down (don't take medical advice from an unqualified source — No Read Down). Integrity flows UPWARD.

Model	Protects	Key Rules
Bell-LaPadula	Confidentiality	No Read Up / No Write Down
Biba	Integrity	No Write Up / No Read Down
Clark-Wilson	Integrity	Well-formed transactions + SoD
Brewer-Nash	Conflict of Interest	Dynamic access based on history

Cryptography Mnemonics

🧠 Symmetric vs Asymmetric Quick Test

SAFE

S — Same key for encrypt/decrypt = Symmetric (AES, 3DES)
A — Asymmetric = public/private key PAIR (RSA, ECC)
F — Fast = Symmetric (use for bulk data)
E — Exchange keys safely = Asymmetric (use for key exchange)

Hybrid: Asymmetric to share the symmetric key. Then AES for speed.

📬 The Padlock Analogy

You publish your open padlock to the world (public key). Anyone can click their message shut with your padlock. Only you have the key (private key) to open it. That's asymmetric encryption — confidentiality with public key, open with private key.

🧠 Digital Signatures

SIGN with PRIVATE, VERIFY with PUBLIC

Sign = private key (only you can sign — proves authenticity)
Verify = public key (anyone can verify — proves non-repudiation)

Encryption for confidentiality: OPPOSITE direction
Encrypt = recipient's PUBLIC key | Decrypt = recipient's PRIVATE key

Memory: 'I SIGN with MY key (private). You VERIFY with MY key (public).'

Secure Design Principles — SLIM DOGS

🧠 Core Secure Design Principles

SLIM DOGS

S — Separation of Duties — no solo control over critical processes
L — Least Privilege — minimum necessary access, nothing more
I — Input Validation — validate everything coming in
M — Minimize Attack Surface — disable what you don't need
D — Defense in Depth — multiple independent layers
O — Open Design — security doesn't depend on secret mechanisms
G — Governance — policies drive security, not individuals
S — Simplicity (Economy of Mechanism) — complexity = vulnerability

DOMAIN 4 | COMMUNICATION & NETWORK SECURITY

OSI Model — All People Seem To Need Data Processing

🧠 **OSI Layers 7 → 1**

All People Seem To Need Data Processing

A — Application (7) — HTTP, FTP, DNS, SMTP
P — Presentation (6) — Encryption, compression, encoding
S — Session (5) — Session setup & teardown
T — Transport (4) — TCP/UDP, end-to-end delivery
N — Network (3) — IP, routing, IPSec
D — Data Link (2) — MAC, switches, ARP, VLANs
P — Physical (1) — Cables, hubs, raw bits

💡 *EXAM TIP: Know which layer each attack and control lives on. ARP poisoning = Layer 2. IP spoofing = Layer 3. SQL injection = Layer 7. The layer tells you the countermeasure.*

Attack	OSI Layer	Countermeasure
ARP Poisoning	Layer 2	Dynamic ARP Inspection, VLANs
IP Spoofing	Layer 3	Ingress/Egress filtering, IPSec
TCP SYN Flood	Layer 4	SYN cookies, rate limiting
Session Hijack	Layer 5	Encrypted sessions, re-auth
SQL Injection	Layer 7	Input validation, WAF, parameterized queries

Firewall Types — PSA-NG

🧠 **Firewall Types (Weakest → Strongest)**

PSA-NG

P — Packet Filter — IP/port rules only; stateless; easily spoofed
S — Stateful — tracks connection state; standard today
A — Application (Proxy) — full Layer 7 inspection; protocol-aware

NG — Next-Gen — stateful + IPS + DPI + app awareness

Each level adds intelligence at the cost of performance.

IDS vs IPS — The Detective vs The Bouncer

🕵️ IDS = The Detective (Passive)

The detective WATCHES what happens, takes notes, and files a report. They don't stop anything — they detect and alert. IDS is placed OFF the main traffic path (out-of-band).

🚪 IPS = The Bouncer (Active)

The bouncer stands at the door and physically blocks bad actors from entering. IPS is placed INLINE — traffic passes through it. If something looks wrong, the bouncer stops it.

DOMAIN 5 | IDENTITY & ACCESS MANAGEMENT

IAM Framework — IAAA

🧠 **The Four Steps of Access Control**

IAAA

I — Identification — claiming an identity (username)
A — Authentication — PROVING the identity (password, biometric)
A — Authorization — determining WHAT you can do (permissions)
A — Accountability — tracking WHAT you did (audit log)

Memory: 'I Arrive And Act'

Authentication Factors — 5 Types

🧠 **Authentication Factor Types**

Know Have Are Where Do

Type 1 — Something you KNOW — password, PIN, passphrase
Type 2 — Something you HAVE — smart card, token, phone
Type 3 — Something you ARE — biometrics (fingerprint, retina)
Type 4 — Somewhere you ARE — geolocation, IP address
Type 5 — Something you DO — typing rhythm, signature dynamics

MFA requires DIFFERENT types. Two passwords = NOT MFA.

Access Control Models — DAM RULE

🧠 **Access Control Models**

DAM RULE

D — DAC (Discretionary) — owner controls; flexible; Windows
A — Attribute-Based (ABAC) — dynamic; context-aware; cloud
M — Mandatory (MAC) — system enforces labels; military/govt

R — Role-Based (RBAC) — most common enterprise model
U — User decides = DAC
L — Label decides = MAC
E — Every attribute evaluated = ABAC

Model	Who Controls Access	Typical Environment
DAC	Resource owner	File systems, Windows, home networks
MAC	System (labels)	Military, government classified systems
RBAC	Role assignment	Corporate enterprise (most common)
ABAC	Policy engine	Cloud, modern dynamic environments

Biometric Error Rates — FAR vs FRR

🎯 **False Acceptance vs False Rejection**

FAR (False Acceptance Rate) = the bouncer lets in an impostor. Type 2 Error. BAD for high security. FRR (False Rejection Rate) = the bouncer turns away the real employee. Type 1 Error. BAD for usability. CER/EER = where they cross. Lower CER = better system.

🧠 **Biometric Error Memory**

FAR = Friendly to Attackers. FRR = Frustrating to Real users.

FAR — False ACCEPTANCE — attacker gets in — SECURITY failure
FRR — False REJECTION — real user blocked — USABILITY failure
CER — Crossover Error Rate — where FAR = FRR — the quality metric

Lower CER = more accurate system. High security = minimize FAR.

DOMAIN 6 | SECURITY ASSESSMENT & TESTING

Pen Test Knowledge Levels — BMW

🧠 Penetration Test Knowledge Levels

BMW

B — Black Box — no knowledge (external attacker simulation)
M — Middle (Gray) Box — partial knowledge (most realistic)
W — White Box — full knowledge (most thorough)

Gray box = the sweet spot. Realistic AND efficient.

> 💡 *EXAM TIP: ALWAYS get a signed rules of engagement document before penetration testing. This is non-negotiable. Unauthorized testing is illegal regardless of intent.*

Vulnerability vs. Pen Test

🏠 The House Inspection Analogy

A vulnerability assessment is a home inspector walking through and finding every crack, loose tile, and dripping faucet. A penetration test is a skilled burglar actually trying to break in through those cracks — proving which ones are actually exploitable.

	Vulnerability Assessment	Penetration Test
Does it run?	No — scan/detect only	Yes — actively exploits
Goal	Find vulnerabilities	Prove exploitability
Output	Vulnerability list	Exploitation path + impact
Frequency	Continuous/weekly	Annual or after changes

Red / Blue / Purple Teams

🧠 Security Team Colors

RBP

R — Red Team — attackers; full adversary simulation
B — Blue Team — defenders; monitoring, detection, response
P — Purple Team — collaborative; Red + Blue working together

White Team = referees. They set rules of engagement.

DOMAIN 7 | SECURITY OPERATIONS

Incident Response — PICERL

🧠 **Incident Response Phases In Order**

PICERL

P — Preparation — build the team, tools, playbooks BEFORE incidents
I — Identification — detect and confirm an incident has occurred
C — Containment — stop the spread; don't let it grow
E — Eradication — remove root cause; clean the environment
R — Recovery — restore systems; verify integrity; back to normal
L — Lessons Learned — document, analyze, improve

Memory: 'Please I Can Escape Rapidly Learning'

🔥 **The House Fire Analogy**

Preparation = smoke detectors, fire extinguishers, evacuation plan. Identification = the alarm goes off. Containment = close doors to slow the fire. Eradication = fire department puts out the fire. Recovery = repair and rebuild. Lessons Learned = why did it start? How do we prevent it next time?

💡 *EXAM TIP: NEVER skip Containment to rush to Eradication. If the attacker still has a foothold, eradicating malware from one machine only forces them to reinfect it.*

BCP vs DRP — The Twin Siblings

🧠 **Business Continuity vs Disaster Recovery**

BCP vs DRP

BCP — Business Continuity Plan — keep the BUSINESS running
DRP — Disaster Recovery Plan — restore IT SYSTEMS after a disaster

BCP is about people and processes. DRP is about technology.
BCP runs DURING a disaster. DRP brings systems back AFTER.

Memory: 'BCP = Business Continues Please. DRP = Data Returns Please.'

Term	What It Is	Drives…
MTD	Max Tolerable Downtime	Sets the ceiling — RTO must be lower
RTO	Recovery Time Objective	How fast to restore systems
RPO	Recovery Point Objective	How much data loss is acceptable

⏱️ **RTO and RPO — The Clock Analogy**

RPO is how far you can rewind the clock — 'I can afford to lose up to 4 hours of data.' RTO is how quickly you need to get the clock running again — 'I need systems back within 8 hours.' RPO drives backup frequency. RTO drives recovery site choice.

Recovery Sites — The Hotel Analogy

🏨 **Hot / Warm / Cold Sites**

Hot site = a luxury hotel with your belongings already there. Check in immediately. Very expensive. Warm site = a hotel room that's ready but your luggage hasn't arrived yet. Takes a day to settle in. Cold site = an empty property you own. You have to furnish it, move in, and set up utilities before you can live there. Weeks of work.

Site Type	Ready In	Cost
Hot Site	Hours	Highest — fully mirrored and live
Warm Site	Days	Medium — hardware ready, data transfer needed
Cold Site	Weeks	Lowest — facility only, everything must be set up

Digital Forensics — Order of Volatility

🧠 **Order of Volatility (Most → Least)**

Collect Volatile First

1. CPU registers and cache — gone in nanoseconds
2. RAM — gone when system powers off
3. Running processes and network connections
4. Hard disk / SSD storage
5. External storage and removable media

6. Remote logs and archived backups

Memory: 'Really Rapid Hard Drives Exhaust Remote systems'

💡 EXAM TIP: Never shut down a compromised system before capturing RAM if you can help it. Volatile evidence (running processes, RAM contents, network connections) disappears on reboot.

Backup Types — The Weekend Warrior

💾 Full vs Incremental vs Differential

Full backup on Friday. Incremental on Mon/Tue/Wed/Thu — backs up only what changed since YESTERDAY. Differential on Mon/Tue/Wed/Thu — backs up everything changed since last FRIDAY. Incremental is smallest daily files but slowest to restore (need Friday + every day). Differential is bigger daily files but faster to restore (need only Friday + today).

DOMAIN 8 | SOFTWARE DEVELOPMENT SECURITY

STRIDE — Threat Modeling

🧠 **Six Threat Categories**

STRIDE

S — Spoofing — impersonating a user or system
T — Tampering — unauthorized data modification
R — Repudiation — denying an action was performed
I — Information Disclosure — unauthorized data access
D — Denial of Service — making a system unavailable
E — Elevation of Privilege — gaining more access than authorized

Memory: 'Some Trusted Relationships Identify Dark Enemies'

SDLC Security — Shift Left

🧠 **SDLC Security Phases**

RDT-DM

R — Requirements — define security requirements upfront
D — Design — threat model; secure architecture review
T — Testing — SAST, DAST, fuzz testing
D — Deployment — hardening; change control; configuration management
M — Maintenance — patching; vulnerability scanning; monitoring

Memory: 'Requirements Define The Deployment Mindset'

🏗️ **The Construction Analogy**

You don't build a house and then add fire exits after inspection fails. You design fire exits into the blueprint before the first brick is laid. Security in software works the same way — design it in during Requirements and Design phases. Retrofitting security costs 10-100x more.

SAST vs DAST

🧠 **Code Testing Methods**

SAST = Source. DAST = Dynamic.

SAST — Static Application Security Testing
Analyzes SOURCE CODE without running the app
Like proofreading a recipe before cooking

DAST — Dynamic Application Security Testing
Tests the RUNNING application from the outside
Like tasting the food while it's cooking

Use BOTH: SAST finds code issues; DAST finds runtime/config issues.

Top Injection Defenses — IPV

🧠 **Defending Against Injection Attacks**

IPV

I — Input Validation — validate ALL input on the server side
P — Parameterized Queries — use prepared statements; never concatenate SQL
V — Validate on Server — client-side validation is supplemental only

The #1 mistake: trusting client-side input validation alone.
Attackers bypass client-side controls trivially — always validate server-side.

QUICK-REFERENCE MASTER SHEET — ALL 8 DOMAINS

All Mnemonics at a Glance

Use this page as your rapid-review sheet in the final days before your exam.

Domain	Mnemonic	Stands For
D1	MATA	Mitigate · Accept · Transfer · Avoid
D1	CIA	Confidentiality · Integrity · Availability
D1	SHAL	Society · Honor · Ability · Legacy (Ethics)
D1	ALE=SLE×ARO	AV×EF=SLE; SLE×ARO=ALE
D2	ODES	Owner · Custodian · End User · Steward
D2	RUT	Rest · Use · Transit (data states)
D2	CPD	Clearing · Purging · Destruction
D3	B-B-C-B	Bell-LaPadula · Biba · Clark-Wilson · Brewer-Nash
D3	SAFE	Same=Symmetric · Asymmetric · Fast=Sym · Exchange=Asym
D3	SLIM DOGS	Sep.Duties · Least Priv · Input Val · Min Surface · Defense Depth · Open Design · Gov · Simplicity
D4	APSTNDP	OSI Layers 7→1 (All People Seem To Need Data Processing)
D4	PSA-NG	Packet · Stateful · Application · Next-Gen Firewall
D5	IAAA	Identify · Authenticate · Authorize · Account
D5	DAM RULE	DAC · ABAC · MAC | Role · User · Label · Every attribute
D5	FAR/FRR	False Acceptance · False Rejection · Crossover Error Rate
D6	BMW	Black · Middle (Gray) · White box testing
D6	RBP	Red · Blue · Purple teams
D7	PICERL	Prep · Identify · Contain · Eradicate · Recover · Learn
D7	MTD>RTO	MTD ceiling; RTO must be shorter
D7	Volatility	RAM → Disk → External → Remote (collect volatile first)
D8	STRIDE	Spoof · Tamper · Repudiate · Disclose · DoS · Elevate
D8	SAST/DAST	Static=Source Code · Dynamic=Running Application
D8	IPV	Input Validation · Parameterized Queries · Validate Server-Side

🚀 Continue Your CISSP Journey

The Premium Threatnexis Memory Toolkit includes:

- ✓ Memory Palace System — room-by-room walkthrough for all 8 domains
- ✓ Full visual concept maps — color-coded relationship diagrams
- ✓ Advanced acronym banks — 80+ mnemonics with story hooks
- ✓ Chaining mnemonics — link concepts across domains
- ✓ 500+ scenario practice questions with manager mindset explanations
- ✓ Rapid-review one-pagers for exam day
- ✓ 30, 60, 90-day study planners
- ✓ Flashcard decks (300+ cards) for every domain

[Unlock the Premium CISSP Toolkit — ThreatNexis.com]

[Book a CISSP Coaching Session]

[Subscribe Free — CISSP Insider Newsletter]