CISSP

VISUAL CHEAT SHEET

25-Page Rapid Review System

All 8 Domains • Visual Mnemonics • Exam Traps • Memory Hooks

D1 Security & Risk Mgmt

D2 Asset Security

D3 Security Architecture

D4 Network Security

D5 IAM

D6 Security Testing

D7 Security Operations

D8 Software Dev Security

CISSP EXAM OVERVIEW

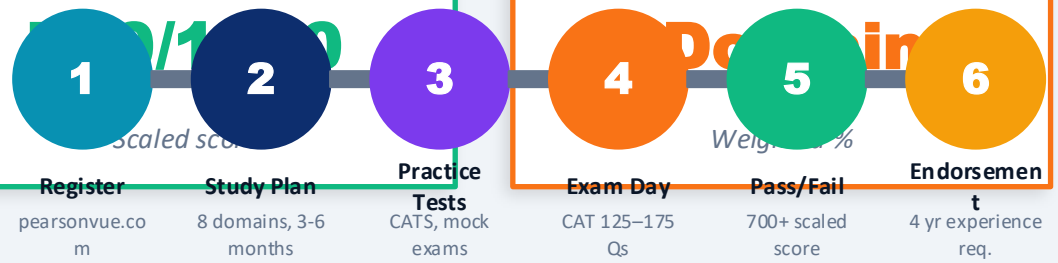
CAT FORMAT

Questions	Time Limit
125–175	**4 Hours**
CAT adaptive	*240 minutes*

DOMAIN WEIGHTS

D1	Security & Risk Management	15%
D2	Asset Security	10%
D3	Security Architecture & Engineering	13%
D4	Communication & Network Security	13%
D5	Identity & Access Management	13%
D6	Security Assessment & Testing	12%
D7	Security Operations	13%
D8	Software Development Security	11%

EXAM LIFECYCLE



EXAM STRATEGY

- Think like a MANAGER, not a technician
- Choose business risk decisions over tech fixes
- Policy/Procedure > Technical controls
- When unsure: select the MOST complete answer
- CAT adapts: harder Qs = on track to pass!
- Eliminate 2 wrong answers first
- Security > Availability (CIA priority)
- 4 yrs exp required (1 yr = 1 domain cert)

THE CISSP MINDSET

🧠 MINDSET

DECISION HIERARCHY

(CISSP prioritizes TOP-DOWN)

🎯 GOLDEN RULES FOR EXAM DAY

- ✓ Security before convenience
- ✓ Risk management is ongoing
- ✓ Management support is critical
- ✓ Least privilege always
- ✓ Defense in depth — never single control

RISK-BASED DECISION FRAMEWORK

Q: Which control to pick?
→ Least costly that manages risk to acceptable level

Q: Security vs Usability?
→ Balance risk — security shouldn't block business

Q: Patch or accept risk?
→ Risk owner decides — document either way

Q: Vendor or in-house?
→ Consider TCO, risk, compliance, support

Q: Incident priority?
→ Contain → Eradicate → Recover → Learn

D1 — SECURITY & RISK MANAGEMENT: CORE CONCEPTS

15% WEIGHT

CIA TRIAD

EXAM TIP

CIA questions: CONFIDENTIALITY = access controls & encryption. INTEGRITY = hashing (SHA). AVAILABILITY = redundancy & backups. Know which attacks target which pillar!

GOVERNANCE FRAMEWORK

POLICY	STANDARD	GUIDELINE	PROCEDURE	BASELINE
High-level management directives 'We shall protect all data'	*Specific mandatory requirements 'AES-256 for all encryption'*	*Recommended, not mandatory 'Consider using VPN remotely'*	*Step-by-step instructions 'How to onboard new user'*	*Minimum security config 'Secure OS baseline'*

↑ MANDATORY ↓ DISCRETIONARY

SECURITY ROLES

Data Owner	Business mgr responsible for data	*Senior management level*
Data Custodian	IT implements security controls	*Sysadmin / DBA*
Data User	Day-to-day access per policy	*Employees*
Privacy Officer	Oversees privacy program	*C-suite level*

D1 — RISK MANAGEMENT

RISK CALCULATION FORMULAS

ALE = SLE × ARO

Annual Loss Expectancy = Single Loss × Annual Rate of Occurrence

SLE = AV × EF

Single Loss Expectancy = Asset Value × Exposure Factor (0.0–1.0)

Risk = Threat × Vulnerability × Impact

Core risk equation — all three factors must exist

Residual Risk = Risk – Controls

What remains after applying controls

EXAMPLE CALCULATION

Asset Value = $100,000 | EF = 0.3 | ARO = 2×/year

`SLE = $100,000 × 0.3 = $30,000 → ALE = $30,000 × 2 = $60,000/yr`

RISK TREATMENT OPTIONS

Risk within tolerance; document and monitor

Low probability, low impact

Eliminate the activity causing the risk

Unacceptably high risk

Insurance, contracts, 3rd party (liability shifts)

Hard to mitigate internally

Implement controls to reduce probability/impact

Most common strategy

RISK TYPES

Inherent Risk
Raw risk before any controls

Residual Risk
Risk remaining after controls

Total Risk
All risk including accepted risks

Control Risk
Risk that controls may fail

D1 — COMPLIANCE, LEGAL & ETHICS

ISC² CODE OF ETHICS (Priority Order)

1 Protect society, the common good, necessary public trust & confidence

🧠 SOCIETY FIRST

2 Act honorably, honestly, justly, responsibly, and legally

🧠 BE HONORABLE

3 Provide diligent and competent service to principals

🧠 SERVE WELL

4 Advance and protect the profession

🧠 GROW THE FIELD

🧠 **MNEMONIC: 'SHIP' = Society, Honorable, Individual (principals), Profession**

When in conflict → always choose SOCIETY (option 1) first!

KEY LAWS & FRAMEWORKS

EU GDPR
EU data privacy regulation; breach notification 72 hrs

CCPA
California consumer privacy

HIPAA
US healthcare data privacy

FISMA
US federal information security

SOX
Financial record integrity for public companies

© DMCA
Digital copyright protection

PCI-DSS
Payment card data security standard

CFAA
Computer fraud & abuse

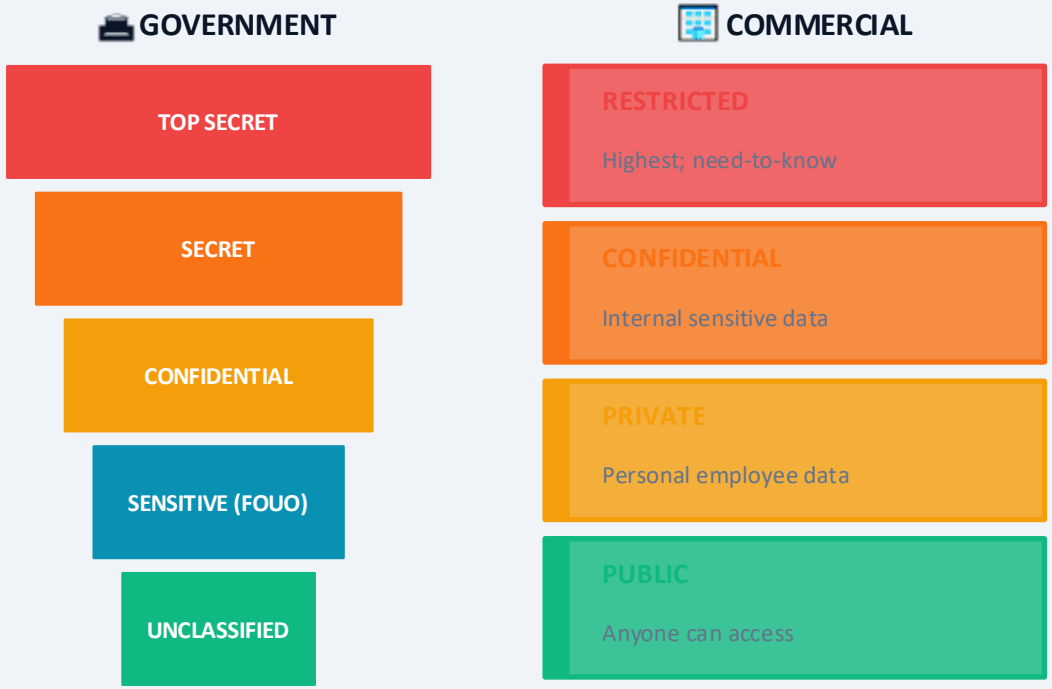
Privacy by Design — 7 Principles

Proactive | Default | Embedded | Full functionality | End-to-end | Visibility | Respect users

D2 — ASSET SECURITY: DATA CLASSIFICATION

10% WEIGHT

CLASSIFICATION PYRAMID



EXAM TIP: The DATA OWNER is always a MANAGEMENT role, never IT! The data custodian (IT) implements the controls that the owner defines.

DATA STATES & CONTROLS

DATA AT REST

Stored on disk, DB, backup

Controls: Encryption (AES), ACLs, FDE

DATA IN TRANSIT

Moving over network

Controls: TLS, IPSec, VPN, HTTPS

DATA IN USE

Being processed in memory

Controls: RAM encryption, trusted execution

KEY EXAM FACTS

• Data owner = accountable for classification • Data custodian = implements controls • Scoping = removing inapplicable controls • Tailoring = adjusting controls to environment

D2 — DATA LIFECYCLE & RETENTION

1. CREATE

Generate or acquire data

Classification, labeling, ownership assignment

2. STORE

Persist to storage systems

Encryption at rest, access controls, backup

3. USE

Process or view data

Least privilege, DLP, logging/monitoring

4. SHARE

Transfer or distribute

Encryption in transit, NDA, sharing agreements

5. ARCHIVE

Long-term retention

Immutable storage, retention policies, compliance

6. DESTROY

Permanent deletion

Degaussing, shredding, crypto-erasure

DESTRUCTION METHODS: Overwriting | Degaussing | Physical destruction | Cryptographic erasure | Sanitization (NIST 800-88)

D3 — SECURITY MODELS

13% WEIGHT

Bell-LaPadula — 1973

FOCUS: CONFIDENTIALITY

- No Read Up (Simple Security)
- No Write Down (*-Property)
- Strong Tranquility

BLP = NO READING UP (government/military)

Biba — 1977

FOCUS: INTEGRITY

- No Read Down (Simple Integrity)
- No Write Up (*-Integrity)
- Invocation Property

Biba = NO WRITING UP (corporate data integrity)

Clark-Wilson — 1987

FOCUS: INTEGRITY

- Well-formed transactions only
- Separation of duties enforced
- CDI/UDI/TP/IVP concepts

Clark-Wilson = Transactions + SoD (banking/ERP)

Brewer-Nash — 1989

FOCUS: CONFIDENTIALITY

- Chinese Wall model
- Once accessed, conflicts blocked
- Prevents conflict of interest

Brewer-Nash = Chinese Wall (consulting firms)

Graham-Denning — 1972

FOCUS: ACCESS CONTROL

- 8 basic protection rights
- Create/Delete objects & subjects
- Read/Grant/Delete/Transfer

Graham-Denning = 8 rules for object access

Take-Grant — 1976

FOCUS: ACCESS CONTROL

- Directed graph model
- Take = gain rights
- Grant = give rights to others

Take-Grant = rights propagation via graphs

D3 — CRYPTOGRAPHY FUNDAMENTALS

SYMMETRIC vs ASYMMETRIC

SYMMETRIC

Same key encrypt/decrypt

⚡ Fast | Key Mgmt: 😰 Hard ($n^2/2$ keys)

ALGORITHMS

- DES (56-bit, BROKEN)
- 3DES (168-bit, deprecated)
- AES (128/192/256-bit) ✅
- RC4 (stream, deprecated)
- Blowfish/Twofish

USE: Bulk data encryption

ASYMMETRIC

Public key encrypts, Private decrypts

🐢 Slow | Key Mgmt: 😊 Easy (2n keys)

ALGORITHMS

- RSA (2048+ bit) ✅
- ECC (smaller keys)
- Diffie-Hellman (key exchange)
- DSA (digital signatures)
- ElGamal

USE: Key exchange, digital signatures

HASHING (ONE-WAY)

MD5	128-bit	BROKEN - collision attacks
SHA-1	160-bit	DEPRECATED - collision found
SHA-256	256-bit	✅ Widely used (SHA-2)
SHA-3	256/512-bit	✅ Keccak algorithm
HMAC	Variable	Message Authentication Code

PKI KEY CONCEPTS

- CA = Certificate Authority (issues certs)
- CRL = Certificate Revocation List
- OCSP = Online cert status checking
- CSR = Cert Signing Request

D3 — HARDWARE & PHYSICAL SECURITY

SECURE HARDWARE STACK

HSM – Hardware Security Module

Dedicated crypto processor; stores keys in tamper-evident hardware; FIPS 140-2 Level 3+

TPM – Trusted Platform Module

Chip on motherboard; stores keys/certs; enables Secure Boot; measured boot chain

Secure Enclave / TEE

Isolated CPU execution environment; protects keys in use; ARM TrustZone, Intel SGX

UEFI Secure Boot

Validates OS bootloader signature; prevents boot-level rootkits

Hardware Root of Trust

Immutable foundation for trust chain; starting point of measured boot

⚡ SIDE-CHANNEL ATTACKS

Timing Attack	Analyzes computation time to infer keys ✓ Constant-time algorithms
Power Analysis	SPA/DPA monitors power consumption during crypto ops ✓ Power leveling, noise injection
EM Emanation	Captures electromagnetic radiation from device (TEMPEST) ✓ Faraday cages, shielding
Acoustic Attack	Sound from CPU/fan reveals computations ✓ Sound insulation, noise
Cache Timing	CPU cache access patterns leak info (Spectre/Meltdown) ✓ Microcode patches, isolation

🏗 PHYSICAL CONTROLS: Mantraps/Airlocks | Biometric access | CCTV monitoring | Guards & patrols | Bollards (vehicle) | Turnstiles | Faraday cage | Clean desk policy

D4 — OSI MODEL & TCP/IP

13% WEIGHT

#	LAYER NAME	PDU	PROTOCOLS/TECH	DEVICE
7	APPLICATION	Data	HTTP, FTP, DNS, SMTP, HTTPS	—
6	PRESENTATION	Data	SSL/TLS, JPEG, MPEG, ASCII	—
5	SESSION	Data	NetBIOS, RPC, SQL, NFS	—
4	TRANSPORT	Segment	TCP, UDP, TLS, SCTP	—
3	NETWORK	Packet	IP, ICMP, ARP, BGP, OSPF	Router
2	DATA LINK	Frame	Ethernet, WiFi, PPP, HDLC	Switch/Bridge
1	PHYSICAL	Bit	Cables, Hubs, NIC, Fiber	Hub/Repeater

🧠 MNEMONIC (Top→Bottom): 'All People Seem To Need Data Processing' | (Bottom→Top): 'Please Do Not Throw Sausage Pizza Away'

TCP/IP MODEL

Application
OSI: L5-7

Transport
OSI: L4

Internet
OSI: L3

Network Access
OSI: L1-2

TCP vs UDP

TCP	Connection-oriented Reliable, ordered, slow	*HTTP, FTP, SMTP*
UDP	Connectionless Fast, no guarantee	*DNS, VoIP, Video*

D4 — NETWORK DEVICES & ARCHITECTURE

Firewall

L3-L7

Packet filter, stateful inspection, or NGFW. Controls traffic based on rules.

IDS

Passive

Intrusion Detection System. Monitors & ALERTS only. Passive device.

IPS

Inline

Intrusion Prevention System. Monitors & BLOCKS inline. Active device.

Proxy

L7

Intermediary for requests. Forward proxy = outbound; Reverse = inbound.

WAF

L7

Web App Firewall. Protects against SQLi, XSS, CSRF. L7 HTTP.

SIEM

Monitoring

Security Info & Event Mgmt. Log aggregation + correlation + alerting.

VPN

L3/L7

Encrypted tunnel. IPSec (L3), SSL/TLS (L7). Site-to-site or remote.

NAC

L2-L3

Network Access Control. Verifies endpoint compliance before granting access.

- Signature-based IDS: Matches known attack patterns (low FP, misses 0-days)
- Anomaly-based IDS: Detects deviations from baseline (high FP, catches 0-days)
- Host IDS (HIDS): Monitors individual host
- Network IDS (NIDS): Monitors network traffic

D4 — SECURE PROTOCOLS

PROTOCOL	INSECURE (AVOID)	PORT	SECURE REPLACEMENT	PORT	USE CASE
HTTP	✗ HTTP	80	✓ HTTPS (TLS)	443	Web traffic
Remote Shell	✗ Telnet	23	✓ SSH v2	22	Remote admin
File Transfer	✗ FTP	21	✓ SFTP / FTPS	22/990	File transfer
Email Send	✗ SMTP	25	✓ SMTPS / STARTTLS	465/587	Email outbound
Email Read	✗ POP3	110	✓ POP3S / IMAPS	995/993	Email client
Directory	✗ LDAP	389	✓ LDAPS	636	Auth/directory
DNS	✗ DNS	53	✓ DNSSEC / DoH / DoT	53/443/853	Name resolution
SNMP	✗ SNMPv1/v2	161	✓ SNMPv3	161	Network mgmt
Time	✗ NTP	123	✓ NTPsec	123	Time sync
Remote Desktop	✗ RDP (unencrypted)	3389	✓ RDP over TLS/VPN	3389	Windows remote

🧠 KEY PORTS TO MEMORIZE: 20/21=FTP 22=SSH/SFTP 23=Telnet 25=SMTP 53=DNS 80=HTTP 110=POP3 143=IMAP 389=LDAP 443=HTTPS 636=LDAPS 993=IMAPS 995=POP3S

D5 — IAM: AUTHENTICATION

13% WEIGHT

Type 1

Something YOU KNOW

- Password
- PIN
- Passphrase
- Security questions
- Cognitive passwords

⚠ *Weakest (can be shared/guessed)*

Type 2

Something YOU HAVE

- Smart card
- Hardware token
- OTP device
- Authenticator app
- USB security key

⚠ *Medium (can be lost/stolen)*

Type 3

Something YOU ARE

- Fingerprint
- Retina/Iris scan
- Voice recognition
- Facial recognition
- Vein pattern

⚠ *Strongest (hard to fake)*

🔐 MULTI-FACTOR AUTHENTICATION (MFA)

Combines 2+ DIFFERENT factors. Two passwords = NOT MFA!

Type 1+2: Password + Token | Type 1+3: Password + Biometric | All three = Strongest

D5 — ACCESS CONTROL MODELS

DAC — Discretionary AC

Who controls: Resource OWNER decides

How: ACLs, file permissions

✓ Flexible, easy to implement

✗ Weak; owner may mis-assign

📌 **Windows NTFS file permissions**

MAC — Mandatory AC

Who controls: SYSTEM enforces based on labels

How: Sensitivity labels (TS, S, C)

✓ Very strong, no user discretion

✗ Inflexible, admin-heavy

📌 **Military systems, SELinux**

RBAC — Role-Based AC

Who controls: ROLE determines access

How: User → Role → Permission

✓ Easy admin, scalable

✗ Role explosion risk

📌 **Corporate AD groups, cloud IAM**

ABAC — Attribute-Based AC

Who controls: ATTRIBUTES determine access

How: User/object/env attributes

✓ Very granular, flexible

✗ Complex to manage

📌 **XACML policies, Zero Trust**

Rule-BAC — Rule-Based AC

Who controls: RULES applied to all

How: IF condition THEN action

✓ Automated, consistent

✗ Less fine-grained

📌 **Firewall ACLs, router rules**

PBAC — Policy-Based AC

Who controls: POLICY engine decides

How: Centralized policy evaluation

✓ Unified, auditable

✗ Policy design complexity

📌 **Okta, AWS IAM policies**

💡 **EXAM: MAC = most secure (military). DAC = most flexible. RBAC = most common in enterprise. ABAC = most granular. 'Need-to-know' = MAC concept.**

D5 — FEDERATION, SSO & IDENTITY PROTOCOLS

SAML 2.0

Authentication + Authorization

Format: XML tokens

Flow: IdP → SP assertion

📌 Enterprise SSO, cloud apps (Office 365, Salesforce)

OAuth 2.0

Authorization ONLY (not authn)

Format: Access tokens (JWT)

Flow: Resource owner → Auth server → Client

📌 API access delegation ('Login with Google' scopes)

OpenID Connect

Authentication (built on OAuth 2.0)

Format: ID tokens (JWT)

Flow: Auth code flow + ID token

📌 Modern federated identity (Google, Facebook login)

Kerberos

Authentication (tickets)

Format: Tickets (TGT, Service)

Flow: KDC → TGT → Service ticket

📌 Active Directory, Windows domain auth

RADIUS

Authentication + Authz + Accounting

Format: UDP datagrams

Flow: Client → RADIUS server → Response

📌 Network device auth, VPN, WiFi 802.1X

TACACS+

Authentication + Authz + Accounting

Format: TCP (encrypted)

Flow: Full packet encryption

📌 Cisco network device admin auth

🧠 **REMEMBER: OAuth = AUTHORIZATION (not authentication). OpenID Connect ADDS authentication to OAuth. SAML = XML = enterprise. Kerberos = tickets = AD.**

D6 — SECURITY ASSESSMENT & TESTING

12% WEIGHT

PENETRATION TEST PHASES

1. **PLANNING**
   Define scope, rules of engagement, legal authorization, goals
2. **RECONNAISSANCE**
   OSINT, passive scanning, info gathering (no active contact)
3. **SCANNING**
   Active scanning, port scans, vulnerability enumeration (Nmap, Nessus)
4. **EXPLOITATION**
   Gain access, escalate privileges, pivot to other systems
5. **POST-EXPLOITATION**
   Establish persistence, data exfiltration, lateral movement
6. **REPORTING**
   Document findings, PoC, risk ratings, remediation recommendations

TEST TYPES COMPARISON

Black Box
No prior knowledge. Simulates external attacker.

White Box
Full knowledge (code, architecture, credentials).

Gray Box
Partial knowledge. Most realistic internal attacker.

Vuln Assessment
Identify and quantify vulnerabilities. NO exploitation.

Pen Test
Actually exploit vulnerabilities. Authorized attacks.

Red Team
Full adversary simulation. Physical + social + cyber.

Blue Team
Defenders. Detect, respond, improve security posture.

Purple Team
Red + Blue cooperating. Share TTPs, improve both sides.

SAST = Static Application Security Testing (analyze SOURCE CODE, no execution) | DAST = Dynamic AST (test RUNNING app, black box) | IAST = Combines both in runtime

D6 — SECURITY METRICS & ANALYSIS

DETECTION CONFUSION MATRIX

	ACTUAL POSITIVE	ACTUAL NEGATIVE
PREDICTED POSITIVE	✅ **TRUE POSITIVE** — Alert fired, attack real	⚠️ **FALSE POSITIVE** — Alert fired, no attack (false alarm)
PREDICTED NEGATIVE	💀 **FALSE NEGATIVE** — No alert, attack real (MOST DANGEROUS)	✅ **TRUE NEGATIVE** — No alert, no attack (correct silence)

BIOMETRIC ERROR RATES

FAR — False Accept Rate	Accepts unauthorized user (Type II error)	✓ *Low FAR = more secure*
FRR — False Reject Rate	Rejects authorized user (Type I error)	✓ *Low FRR = more convenient*
CER / EER — Crossover Error Rate	Point where FAR = FRR = benchmark	✓ *Lower CER = better biometric*

KEY SECURITY METRICS (KPIs)

MTTD

Mean Time to Detect

Average time to detect an incident

Formula: Σ detection times / # incidents

MTTR

Mean Time to Respond

Average time to respond/contain

Formula: Σ response times / # incidents

MTTF

Mean Time to Failure

Expected time until system fails

Formula: Total up-time / # failures

MTBF

Mean Time Between Failures

Time between failures (reliability)

Formula: Total up-time / (# failures - 1)

RTO

Recovery Time Objective

Max acceptable downtime after disaster

Formula: Business sets this value

RPO

Recovery Point Objective

Max data loss tolerated

Formula: Time between backups

🧠 RTO > RPO means more data loss is acceptable than downtime. If RTO=4hrs, systems must recover in 4hrs. If RPO=1hr, max 1hr of data loss allowed.

D7 — INCIDENT RESPONSE

13% WEIGHT

PHASE 1: PREPARATION

Build IRP, train team, set up SIEM, establish communication channels, create playbooks

PHASE 2: DETECTION & ANALYSIS

Monitor alerts, correlate events, determine scope, classify severity, create ticket

PHASE 3: CONTAINMENT

Short-term: isolate affected systems. Long-term: patch & harden. Preserve evidence!

PHASE 4: ERADICATION

Remove malware, close vulnerabilities, reset compromised credentials, clean systems

PHASE 5: RECOVERY

Restore systems, verify functionality, monitor for re-infection, gradual return to ops

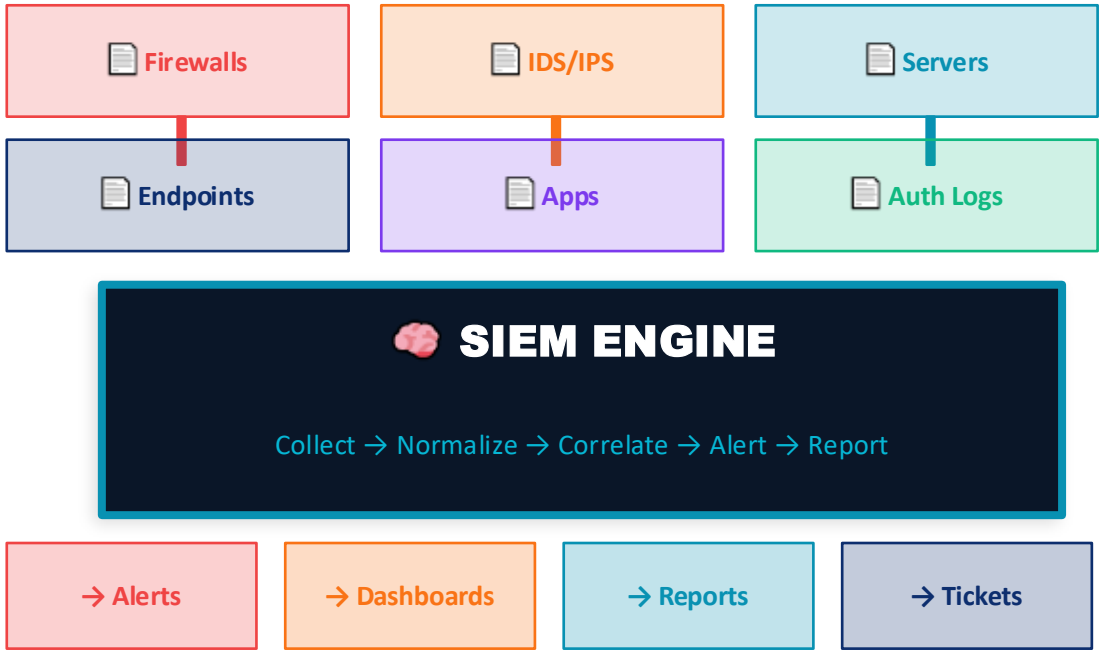
PHASE 6: LESSONS LEARNED

Post-incident review (PIR), update IRP, document timeline, train staff, report metrics

⚠ **EVIDENCE HANDLING: Order of Volatility (most → least): CPU registers & cache → RAM → Swap → Disk → Remote logs → Archived backups. Collect most volatile FIRST!**

D7 — LOGGING, MONITORING & SIEM

SIEM ARCHITECTURE



LOG MANAGEMENT BEST PRACTICES

- Centralize logs to tamper-proof storage
- Enable NTP — time synchronization is critical
- Log: authentication events, privilege use, config changes
- Retain logs per compliance (PCI=1yr, HIPAA=6yr)
- Protect log integrity (digital signatures, append-only)
- Review logs regularly — automated alerts + manual review

SOC TIERS & OPERATIONS

Tier 1 Alert Analyst	Monitor dashboards, triage alerts, basic analysis, escalate
Tier 2 Incident Responder	Deep dive investigations, containment, forensics, remediation
Tier 3 Threat Hunter	Proactive threat hunting, advanced forensics, threat intelligence
Tier 4 SOC Manager	Metrics, resource management, strategy, stakeholder communication

KEY TERMS

- SOAR = Security Orchestration, Automation & Response
- TTP = Tactics, Techniques & Procedures (adversary behavior)
- IOC = Indicator of Compromise (evidence of attack)
- UEBA = User & Entity Behavior Analytics

D7 — BUSINESS CONTINUITY & DISASTER RECOVERY

BCP — Business Continuity Plan

FOCUS: PREVENTION & SUSTAINING

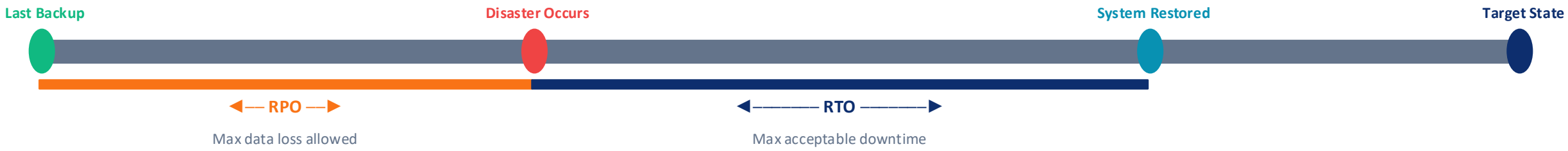
Ensures critical business functions continue during/after disaster. Broader than DRP. Covers people, process, facilities.

DRP — Disaster Recovery Plan

FOCUS: RECOVERY (IT/SYSTEMS)

Restores IT systems and data after disruption. Subset of BCP. Technical focus on getting systems back online.

RECOVERY TIMELINE: RTO & RPO VISUALIZATION



BACKUP STRATEGIES COMPARISON

FULL

Data: ALL data

Slowest backup | Fastest restore

Storage: Most storage

INCREMENTAL

Data: Changes since LAST backup

Fastest backup | Slowest restore (chain)

Storage: Least storage

DIFFERENTIAL

Data: Changes since LAST FULL

Medium backup | Medium restore (2 sets)

Storage: Medium storage

D8 — SECURE SDLC

11% WEIGHT

REQUIREMENTS

1 Security Activities:

Security requirements gathering, privacy impact assessment, compliance mapping

DESIGN

2 Security Activities:

Threat modeling (STRIDE/PASTA), security architecture review, attack surface analysis

DEVELOPMENT

3 Security Activities:

Secure coding standards, code review, SAST tools, developer security training

TESTING

4 Security Activities:

DAST scanning, penetration testing, fuzzing, vulnerability assessment

DEPLOYMENT

5 Security Activities:

Hardening, configuration management, change control, secrets management

MAINTENANCE

6 Security Activities:

Patch management, continuous monitoring, incident response, EOL planning

Waterfall: Sequential, rigid, security at end | Agile: Iterative sprints, security integrated | DevSecOps: Shift-left, security in pipeline (CI/CD) | SAFe: Scaled agile for enterprise

D8 — APPLICATION SECURITY

OWASP TOP 10 (2021)

A01	**Broken Access Control**	Improper enforcement of access restrictions	✓ Proper authz checks, least privilege
A02	**Cryptographic Failures**	Weak or missing encryption of sensitive data	✓ TLS, strong algos, key management
A03	**Injection**	SQLi, XSS, command injection via untrusted input	✓ Parameterized queries, input validation
A04	**Insecure Design**	Security not considered in architecture phase	✓ Threat modeling, secure design principles
A05	**Security Misconfiguration**	Default passwords, unnecessary features enabled	✓ Hardening, config management
A06	**Vulnerable Components**	Using outdated libraries with known vulns	✓ SCA tools, patch management, SBOM
A07	**Auth Failures**	Broken authentication, weak passwords	✓ MFA, secure session management
A08	**Software Integrity Failures**	Untrusted code/updates, CI/CD pipeline attacks	✓ Code signing, integrity verification
A09	**Logging Failures**	Insufficient logging and monitoring	✓ Centralized logging, alerting, SIEM
A10	**SSRF**	Server-Side Request Forgery — internal access	✓ Input validation, network segmentation

SECURE CODING PRINCIPLES

Input Validation

Never trust input. Whitelist > blacklist. Server-side always.

Least Privilege

Code runs with minimal permissions needed for function.

Defense in Depth

Multiple security layers — no single point of failure.

Fail Securely

Failures default to DENY, not permit. Log errors safely.

Separation of Privilege

Two conditions required to grant access (like 2-man rule).

Economy of Mechanism

Keep it simple. Complexity = more attack surface.

Open Design

Security through obscurity alone is NOT sufficient.

Psychological Acceptability

Security controls must be usable or users will bypass

🧠 **SALTZER & SCHROEDER: 8 design principles coined in 1975 — still core to secure development today. Know them all for the exam!**

🚀 ULTIMATE EXAM BLITZ — MUST-KNOW FACTS

D1 RISK

- ALE = SLE × ARO
- SLE = AV × EF
- Ethics: Society → Honorable → Serve → Profession
- Risk = Threat × Vulnerability × Impact
- Due Care = do it | Due Diligence = check it
- Qualitative = subjective | Quantitative = $$$

D2 ASSET

- Data Owner = MGMT role
- Data Custodian = IT role
- Destroy: degauss → shred → overwrite
- 3 data states: rest, transit, use
- Classification: Top Secret → Unclassified
- Scoping removes inapplicable controls

D3 ARCH

- BLP = Confidentiality (no read up)
- Biba = Integrity (no write up)
- Clark-Wilson = Transactions + SoD
- AES = symmetric, RSA = asymmetric
- MD5/SHA-1 = BROKEN
- TPM = on motherboard, HSM = external

D4 NETWORK

- OSI: App→Presentation→Session→Transport→Network→Data→Physical
- TCP = reliable | UDP = fast
- TLS replaces SSL (SSL is dead)
- 22=SSH | 443=HTTPS | 389=LDAP
- VLAN ≠ security boundary
- NAT ≠ firewall

D5 IAM

- MFA = 2+ DIFFERENT factors
- MAC = most secure (mandatory)
- DAC = resource owner decides
- RBAC = most common enterprise
- OAuth = authorization only
- SAML = XML | OIDC = JWT

D6 TEST

- Pen test ≠ vulnerability scan
- Black box = no knowledge
- White box = full knowledge
- CER/EER = biometric accuracy
- FAR = false accept (dangerous)
- SAST = source code | DAST = running app

D7 OPS

- IR: Prep→Detect→Contain→Eradicate→Recover→Lessons
- Order of volatility: RAM first!
- RTO = max downtime | RPO = max data loss
- Full backup = slowest; Incremental = fastest
- SIEM = collect + correlate + alert
- Kerberos = tickets in AD

D8 DEVSEC

- Shift-left = security early in SDLC
- OWASP #1 = Broken Access Control
- SQL injection = parameterized queries
- Never trust input (validate server-side)
- Fail securely = deny by default
- DevSecOps = security in CI/CD pipeline

⚠ EXAM TRAPS: 'Most secure' ≠ 'best answer' (consider cost/risk balance) • OAuth ≠ authentication • IDS alerts, IPS blocks • Two passwords ≠ MFA • Think manager first!