CISSP EXAM PREP SERIES

Domain 3

Security Architecture & Engineering

The Concepts That Actually Show Up on the Exam

Format	Coverage
Comprehensive Study Guide	10 Core Topic Areas

1. Security Models & Frameworks

Security models provide the theoretical and mathematical foundation for implementing access controls and information security policies. Domain 3 tests your ability to distinguish between these models and understand when each applies.

1.1 Confidentiality Models

Bell-LaPadula Model (BLP)

Developed for the U.S. Department of Defense, BLP is the definitive confidentiality model. Its two core properties govern all information flow:

- Simple Security Property ("no read up")
  - A subject at a lower classification cannot read objects at a higher classification level
  - Prevents unauthorized disclosure of sensitive information
- Star (*) Property ("no write down")
  - A subject at a higher level cannot write to an object at a lower level
  - Prevents information leakage from high to low security domains
- Strong Star Property:
  - Subjects can only read and write at their own classification level

> **EXAM TIP — BLP FOCUS**
> Bell-LaPadula is ONLY about confidentiality — it does NOT address integrity. The exam frequently tests this distinction. If a question mentions 'preventing unauthorized disclosure,' think BLP.

Biba Model

Biba is the integrity counterpart to BLP. It prevents data corruption by lower-integrity subjects:

- Simple Integrity Property ("no read down"):
  - A subject cannot read data at a lower integrity level (preventing contamination)
- Star (*) Integrity Property ("no write up"):
  - A subject cannot write to an object at a higher integrity level

> **KEY CONTRAST — BLP VS. BIBA**
> BLP: no read UP, no write DOWN (preserves confidentiality). Biba: no read DOWN, no write UP (preserves integrity). These are mirror opposites and a frequent exam question pair.

1.2 Integrity Models

Clark-Wilson Model

Clark-Wilson addresses commercial integrity through a more practical, real-world lens than Biba. It introduces two key object types:

- Constrained Data Items (CDIs):
  - Data that must maintain integrity — only modified through controlled procedures
- Unconstrained Data Items (UDIs):
  - Input data from untrusted sources before validation
- Integrity Verification Procedures (IVPs):
  - Ensure CDIs conform to integrity constraints
- Transformation Procedures (TPs):
  - The only authorized methods for modifying CDIs — enforce separation of duties

Brewer-Nash Model (Chinese Wall)

Designed to prevent conflicts of interest in commercial settings, particularly in consulting and financial services. Access decisions are based on prior access history:

- A subject who has accessed data from Company A cannot access conflicting data from Company B
- Dynamically restricts access based on what the subject has already seen
- Commonly tested in scenarios involving auditors, consultants, or investment bankers

1.3 Model Comparison Quick Reference

Model	Primary Goal	Key Rule	Best Applies To
Bell-LaPadula	Confidentiality	No read up / no write down	Government / Military
Biba	Integrity	No read down / no write up	Data accuracy requirements
Clark-Wilson	Commercial Integrity	Transactions via TPs only	Business / Financial
Brewer-Nash	Conflict of Interest	Dynamic access restriction	Consulting / Finance

2. Security Architecture Frameworks

Architectural frameworks provide structured approaches to designing, implementing, and managing security across an enterprise. The exam tests conceptual understanding of each framework's purpose and scope.

2.1 SABSA (Sherwood Applied Business Security Architecture)

SABSA is a risk-driven framework that aligns security architecture with business objectives. It uses a layered model inspired by the Zachman Framework:

- Contextual Layer (Business View):
  - What are the business drivers? Defines WHY security is needed
- Conceptual Layer (Architect's View):
  - What security concepts apply? Defines WHAT needs protecting
- Logical Layer (Designer's View):
  - Security policies and models — HOW will it be protected
- Physical Layer (Builder's View):
  - Technology and infrastructure — WITH WHAT will it be built
- Component Layer (Tradesman's View):
  - Products and standards — WHICH specific tools are used

2.2 TOGAF (The Open Group Architecture Framework)

TOGAF provides a comprehensive approach to enterprise architecture, covering business, data, application, and technology architecture. Its core component is the Architecture Development Method (ADM), a cyclical process ensuring architectural decisions remain aligned with business goals.

2.3 Zachman Framework

The Zachman Framework is an enterprise ontology — a two-dimensional matrix examining an organization from multiple perspectives (Planner, Owner, Designer, Builder, Implementer, Worker) against architectural views (What, How, Where, Who, When, Why). It is descriptive rather than prescriptive.

> **EXAM DISTINCTION**
> TOGAF provides a process (ADM) for building architecture. Zachman provides a classification schema for organizing architectural artifacts. SABSA ties security architecture directly to business risk drivers. Know which framework is process-oriented vs. descriptive.

3. Cryptography Fundamentals

Cryptography underpins nearly all security controls. Domain 3 tests both conceptual understanding and applied knowledge of when to use specific algorithms and protocols.

3.1 Symmetric vs. Asymmetric Cryptography

Attribute	Symmetric	Asymmetric
Key count	1 shared key	Key pair (public + private)
Speed	Fast (bulk data)	Slow (key exchange, signatures)
Key distribution	Difficult (secure channel needed)	Public key can be shared openly
Common algorithms	AES, 3DES, ChaCha20	RSA, ECC, Diffie-Hellman
Primary use	Data encryption	Key exchange, digital signatures

3.2 Key Algorithms You Must Know

AES (Advanced Encryption Standard)

The current U.S. government standard for symmetric encryption. Key facts for the exam:

- Block cipher — processes 128-bit blocks
- Key sizes: 128, 192, or 256 bits (256-bit is used in Top Secret applications)
- Replaced DES and 3DES — if a question mentions legacy concerns, it's probably DES

RSA (Rivest-Shamir-Adleman)

- Asymmetric algorithm based on the mathematical difficulty of factoring large prime numbers
- Key sizes: 2048 bits minimum (4096 preferred for long-term security)
- Used for key exchange and digital signatures — NOT for bulk data encryption

Elliptic Curve Cryptography (ECC)

- Provides equivalent security to RSA with significantly smaller key sizes
- 256-bit ECC key ≈ 3072-bit RSA key in security strength
- Preferred for constrained environments: mobile devices, IoT, smart cards

3.3 Hashing Algorithms

Hash functions produce a fixed-length digest (fingerprint) of variable-length input. They are one-way — you cannot reverse a hash to recover the original data.

Algorithm	Output Size	Status	Notes
MD5	128 bits	Broken — do NOT use	Collision vulnerabilities proven
SHA-1	160 bits	Deprecated	Collision found

Algorithm	Output Size	Status	Notes
			(SHAttered, 2017)
SHA-256	256 bits	Current standard	Part of SHA-2 family
SHA-3	Variable	Current (alternative)	Keccak algorithm, different design
bcrypt/Argon2	Variable	Password hashing	Intentionally slow with salting

3.4 Digital Signatures

Digital signatures provide authentication, non-repudiation, and integrity. The signing process is often misunderstood on the exam:

- Sender ENCRYPTS a hash of the message with their PRIVATE key
- Recipient DECRYPTS the signature with the sender's PUBLIC key
- If the decrypted hash matches a fresh hash of the received message, the signature is valid

> **CRITICAL EXAM POINT**
> Private key = used to SIGN (encrypt the hash). Public key = used to VERIFY (decrypt the hash). This is the opposite of how encryption works, where you encrypt with the recipient's PUBLIC key.

3.5 Public Key Infrastructure (PKI)

- **Issues and signs digital certificates** Certificate Authority (CA):
- **Verifies identity before the CA issues certificates** Registration Authority (RA):
- **List of revoked certificates; checked manually** Certificate Revocation List (CRL):
- **Real-time certificate status checking** OCSP (Online Certificate Status Protocol):
- **The standard format for digital certificates** X.509:

4. Secure Design Principles

These foundational principles guide the architecture and design of secure systems. The exam tests your ability to identify which principle applies in a given scenario.

4.1 Core Design Principles

Least Privilege

Subjects (users, processes, systems) should have only the minimum permissions necessary to perform their designated function — nothing more. This limits blast radius when accounts are compromised.

Separation of Duties (SoD)

No single individual should have sufficient access to complete a high-risk transaction or commit fraud alone. A classic example: the person who requests a payment cannot also approve and issue it.

Defense in Depth

Layer multiple security controls so that the failure of one control does not result in total compromise. Also called 'layered security.' Assumes breach is possible and focuses on limiting damage.

Fail Secure / Fail Safe

- **When a system fails, it defaults to a DENIED / locked-down state (door locks, firewall blocks all traffic)** Fail Secure:
- **When a system fails, it defaults to a safe state for people (fire door opens to allow evacuation)** Fail Safe:

> **EXAM DISTINCTION — FAIL SECURE VS. FAIL SAFE**
> Fail Secure = security priority (deny access). Fail Safe = human safety priority (allow exit). A security system on a server room uses fail secure (door stays locked). A physical fire exit uses fail safe (door unlocks).

Economy of Mechanism (Keep It Simple)

Security mechanisms should be as simple as possible. Complexity is the enemy of security — complex systems have more failure points, are harder to audit, and are more likely to contain vulnerabilities.

Open Design

Security should not rely on the secrecy of the design (Kerckhoffs's Principle). The algorithm should be publicly known; only the key should be secret. This enables public scrutiny and peer review.

Complete Mediation

Every access to every resource must be checked against the access control policy — no caching of authorization decisions that could become stale. Every single access request must be validated.

4.2 Trusted Computing Base (TCB)

The TCB is the totality of protection mechanisms within a computer system — hardware, software, and firmware — that enforce the security policy. Key concepts:

- **The abstract concept of an access control component that mediates ALL access between subjects and objects** Reference Monitor:
- **The hardware, firmware, and software that implement the reference monitor concept** Security Kernel:
- TCB properties: Must be tamper-resistant, always invoked, and verifiable

4.3 Evaluation Assurance Levels (EAL)

Common Criteria (ISO/IEC 15408) defines EAL levels for product evaluation:

EAL	Level Name	Description
EAL1	Functionally Tested	Basic assurance; developer's testing
EAL2	Structurally Tested	Gray-box testing; vulnerability analysis
EAL3	Methodically Tested	Dev environment controls; review
EAL4	Methodically Designed	Most common commercial level
EAL5–7	Semiformal to Formal	Military / high-security systems

5. System Vulnerabilities & Threats

Understanding common vulnerability categories and how attackers exploit them is essential for Domain 3. This section covers the threat types most likely to appear on the exam.

5.1 Memory & Software Vulnerabilities

Buffer Overflow

Occurs when a program writes more data to a buffer than it can hold, overwriting adjacent memory. This can overwrite return addresses, allowing an attacker to redirect execution to malicious code.

- Stack overflow: Targets the call stack; can overwrite saved return addresses
- Heap overflow: Targets dynamically allocated memory
- Mitigation: ASLR (Address Space Layout Randomization), DEP/NX (Data Execution Prevention), SafeStack, input validation

Race Conditions & TOCTOU

A Time-of-Check to Time-of-Use (TOCTOU) attack exploits the window between when a security check is performed and when the action is executed. An attacker races to change the state in that interval.

5.2 Covert Channels

A covert channel communicates information using a mechanism not intended for communication, bypassing mandatory access controls:

- **Uses attributes of a shared resource (file permissions, disk space) to transmit data** Covert Storage Channel:
- **Uses timing of events (response delays, resource availability) to encode information** Covert Timing Channel:

> **EXAM NOTE — COVERT CHANNELS**
> Covert channels are extremely difficult to eliminate entirely. The goal is to reduce their bandwidth (the amount of data they can leak per unit time) to an acceptable level, not to achieve perfect elimination.

5.3 Malware Classification

Type	Definition	Key Characteristic
Virus	Attaches to host files; requires execution	Needs human action to spread
Worm	Self-replicating; spreads autonomously	No host file required
Trojan	Disguised as legitimate software	No self-replication
Ransomware	Encrypts data; demands payment	Extortion via crypto

Type	Definition	Key Characteristic
Rootkit	Hides malicious activity at OS/kernel level	Difficult to detect
Logic Bomb	Triggers on specific condition/date	Often planted by insiders

6. Secure Network Architecture

Network architecture decisions directly impact the security posture of an organization. Domain 3 focuses on the concepts behind segmentation, traffic control, and network security designs.

6.1 Network Segmentation & Zones

DMZ (Demilitarized Zone)

A DMZ is a network segment that sits between the internal trusted network and the external untrusted internet. Servers accessible from the internet (web servers, mail relays) are placed here. The architecture uses two firewalls:

- Outer firewall: Filters traffic between internet and DMZ
- Inner firewall: Filters traffic between DMZ and internal network
- A compromised DMZ server does NOT grant direct access to internal systems

Zero Trust Architecture

Zero Trust is a security model based on 'never trust, always verify.' Core principles:

- Verify explicitly: Authenticate and authorize every request — no implicit trust based on network location
- Use least privilege access: Limit user access with Just-In-Time (JIT) and Just-Enough-Access (JEA)
- Assume breach: Minimize blast radius, segment access, verify end-to-end encryption

6.2 Firewall Types

Type	Operates At	Inspects	Limitation
Packet Filter	Network (L3)	IP/port headers only	No stateful tracking
Stateful Inspection	Transport (L4)	Connection state tables	No application layer
Proxy / App-layer	Application (L7)	Full content inspection	Higher latency/cost
NGFW	Application (L7+)	Identity, apps,	More complex to

Type	Operates At	Inspects	Limitation
		threats	manage

6.3 VPN Protocols

- **Operates at Layer 3; two modes: Transport (encrypts payload) and Tunnel (encrypts entire IP packet including header)** IPSec:
- **Operates at Layer 7; uses web browser; easier client deployment** SSL/TLS VPN:
- **Provides integrity and authentication but NOT confidentiality — does not encrypt payload** AH (Authentication Header):
- **Provides confidentiality, integrity, and authentication** ESP (Encapsulating Security Payload):

> **EXAM TIP — AH VS. ESP**
> AH = Authentication only, no encryption. ESP = Encryption + Authentication. If NAT is involved, AH breaks (NAT changes IP headers that AH protects). Use ESP in NAT environments.

7. Physical Security Controls

Physical security is foundational — all logical controls fail if an attacker gains physical access to hardware. Domain 3 includes physical security as part of a complete architecture.

7.1 Defense in Depth: Physical Layers

Physical security applies the same layered defense principle as logical security:

- **Fences, walls, vehicle barriers, lighting, CCTV at property boundary** Layer 1 — Perimeter:
- **Reinforced doors, window security, exterior access control** Layer 2 — Exterior Building:
- **Mantrap/airlock entry, badge readers, visitor management** Layer 3 — Interior Zones:
- **Server rooms, data centers with biometrics and two-person integrity** Layer 4 — Secure Areas:
- **Cable locks, full disk encryption, asset tags, RFID tracking** Layer 5 — Assets:

7.2 Access Control Mechanisms

Mantrap (Airlock)

A mantrap uses two interlocked doors to prevent tailgating. Only one door can be open at a time. The person must be authenticated in the secure vestibule before the inner door unlocks. Used for high-security data centers.

Biometric Authentication

Biometric systems have two critical error rates:

- **Probability of accepting an unauthorized person — a TYPE II error** FAR (False Acceptance Rate):
- **Probability of rejecting an authorized person — a TYPE I error** FRR (False Rejection Rate):
- **The point where FAR = FRR; lower CER = more accurate system** CER/EER (Crossover Error Rate):

> **EXAM FORMULA — BIOMETRIC ACCURACY**
> CER (Crossover Error Rate) = the point at which FAR equals FRR. A system with CER of 1% is more accurate than a system with CER of 5%. Lower CER = better biometric system. This is the primary accuracy comparison metric.

7.3 Environmental Controls

Control	Purpose	Key Standard/Note
Hot/Cold Aisles	Datacenter cooling efficiency	Cold aisle faces server fronts
Halon Alternatives	Fire suppression (no water)	FM-200, Inergen — safe for equipment
UPS	Short-term power continuity	Bridges gap to generator start
Generator	Long-term power backup	Requires fuel supply management
HVAC Controls	Temperature & humidity	40-60% humidity; 64-80°F typical

8. Cloud & Virtualization Security

Cloud and virtualization technologies introduce unique security challenges and shared responsibility models that are heavily tested in Domain 3.

8.1 Cloud Service Models

Model	Provider Manages	Customer Manages	Example
IaaS	Hardware, hypervisor,	OS, apps, data, IAM	AWS EC2, Azure VMs

Model	Provider Manages	Customer Manages	Example
	networking		
PaaS	IaaS + OS + runtime + middleware	Applications, data	Heroku, Google App Engine
SaaS	Everything including app	Data, user access config	Office 365, Salesforce

8.2 Cloud Deployment Models

- **Resources owned and operated by a third-party provider; multi-tenant** Public Cloud:
- **Dedicated infrastructure for a single organization; on-premises or hosted** Private Cloud:
- **Combination of public and private; data and apps portable between** Hybrid Cloud:
- **Shared by organizations with common concerns (compliance, mission)** Community Cloud:

8.3 Virtualization Security Threats

VM Escape

The most critical virtualization threat. An attacker exploits a vulnerability in the hypervisor to break out of a virtual machine and access the hypervisor or other VMs on the same host. If successful, all VMs on the host are compromised.

Hypervisor Types

- **Runs directly on hardware (VMware ESXi, Hyper-V, Xen). More secure — smaller attack surface. Used in data centers.** Type 1 (Bare Metal):
- **Runs on top of an OS (VirtualBox, VMware Workstation). Larger attack surface. Used for development/testing.** Type 2 (Hosted):

> **SHARED RESPONSIBILITY REMINDER**
> In ALL cloud models, the customer is ALWAYS responsible for their data and user access management. The provider's responsibility increases as you move from IaaS to PaaS to SaaS — but the customer never fully delegates data security.

9. Site & Facility Security Planning

Facility security begins before construction. Domain 3 includes Crime Prevention Through Environmental Design (CPTED) and site selection considerations.

9.1 CPTED Principles

Crime Prevention Through Environmental Design uses architectural and environmental features to deter criminal activity:

- **Design spaces to maximize visibility — open sightlines, adequate lighting, eliminating concealment areas** Natural Surveillance:
- **Guide movement through design — pathways, landscaping, and structures that channel traffic through controlled entry points** Natural Access Control:
- **Create a sense of ownership — clear boundaries between public and private spaces discourage unauthorized presence** Territorial Reinforcement:
- **Physical security measures — locks, reinforced glass, fencing (the traditional approach)** Target Hardening:

9.2 Site Selection Criteria

Factor	Consideration
Natural Disaster Risk	Flood plains, seismic zones, tornado/hurricane corridors
Proximity to Hazards	Distance from airports, rail lines, chemical plants, military bases
Utility Reliability	Redundant power feeds, fiber routes from separate providers
Accessibility	Access for emergency responders vs. single-entry-point security
Visibility	High-profile buildings attract attention; low-profile sites are harder to target

9.3 Media Sanitization & Disposal

Before physical media leaves control, it must be properly sanitized to prevent data recovery:

- **Overwriting data — protects against standard recovery tools but not forensic lab analysis** Clearing:
- **Degaussing (magnetic media) or cryptographic erasure — protects against lab-grade forensics** Purging:
- **Physical destruction (shredding, incineration, disintegration) — the only guaranteed method** Destruction:

> **NIST GUIDANCE**
> NIST SP 800-88 (Guidelines for Media Sanitization) defines these three methods. For SSDs and flash media, degaussing is ineffective — use cryptographic erasure or physical destruction. The exam may test this SSD-specific exception.

10. High-Frequency Exam Topics & Strategy

Based on domain weightings and common question patterns, these are the areas most likely to appear on your CISSP exam from Domain 3.

10.1 Top 10 Must-Know Concepts

- **Know the properties by name and which direction (up/down) each allows** Bell-LaPadula vs. Biba:
- **Private key signs, public key verifies — know the order** Digital Signature Process:
- **128/192/256-bit; 256-bit for Top Secret; replaced DES/3DES** AES Key Sizes:
- **Security state vs. human safety state on failure** Fail Secure vs. Fail Safe:
- **Most common commercial evaluation level; know the scale direction** EAL4:
- **Goal is reduction, not elimination** Covert Channel Bandwidth:
- **Race condition between check and use — timing attack** TOCTOU:
- **Lower CER = more accurate; the crossover point** CER in Biometrics:
- **ESP encrypts; AH only authenticates; AH breaks NAT** ESP vs. AH:
- **Hypervisor breach affecting all tenant VMs on the host** VM Escape:

10.2 Common Question Traps

TRAP 1 — BELL-LAPADULA AND INTEGRITY

BLP only addresses confidentiality. It does nothing to protect data integrity. If a question mentions data corruption or modification controls, BLP is NOT the answer.

TRAP 2 — SYMMETRIC KEY COUNT

With n parties, symmetric key exchange requires n(n-1)/2 unique keys. With 100 people, that's 4,950 keys. This is why asymmetric cryptography (PKI) scales better for large groups.

TRAP 3 — DIGITAL CERTIFICATES

A digital certificate binds a public key to an identity. It does NOT contain the private key. The certificate is public; the private key is always kept secret by its owner.

10.3 Domain 3 Weight & Approach

Domain 3 (Security Architecture and Engineering) represents approximately 13% of the CISSP exam. With 125-175 questions on the CAT exam, expect 16-23 questions from this domain.

Study strategy recommendations:

- Prioritize security models (BLP, Biba, Clark-Wilson) — highest return on study time

- Master cryptography fundamentals — hash algorithms, key exchange, PKI
- Understand secure design principles conceptually — exam tests application, not memorization
- Review physical security controls — often seen as easy points but contain traps
- Practice elimination: for architecture questions, eliminate answers that confuse confidentiality and integrity controls first

FINAL REMINDER

The CISSP is a managerial/practitioner exam — questions ask what a CISO or senior security professional would do, not what a technician would configure. When in doubt, choose the answer that aligns with risk management, policy, and governance over the purely technical answer.