THREATNEXIS
CISSP MASTER STUDY GUIDE

All 8 Domains — Free Edition

Think like a Manager. Pass the First Time.

About This Guide

Welcome to the Threatnexis CISSP Master Study Guide — Free Edition. This guide covers all eight CISSP domains with the clarity, depth, and instructor-level insight you need to build real understanding.

This is NOT a brain dump. This is not a list of definitions to memorize. This guide teaches you how to THINK like a CISSP — which is the only way to pass an exam that tests judgment, not just knowledge.

> **HOW TO USE THIS GUIDE** Read each domain with the goal of understanding the WHY behind each concept. Ask yourself: 'How does this help a business manage risk?' That question is the lens through which every CISSP question should be viewed.

Domain	Weight
Domain 1: Security & Risk Management	16%
Domain 2: Asset Security	10%
Domain 3: Security Architecture & Engineering	13%
Domain 4: Communication & Network Security	13%
Domain 5: Identity & Access Management	13%
Domain 6: Security Assessment & Testing	12%
Domain 7: Security Operations	13%
Domain 8: Software Development Security	10%

> **THE GOLDEN RULE** The CISSP is not a technical exam. It is a risk management and governance exam. When in doubt, ask: 'What would a senior security manager recommend here?' That is almost always the right answer.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Overview

Domain 1 is the largest domain on the CISSP exam, carrying 16% of the total weight. Think of it as the foundation that every other domain is built on. If you understand risk management, governance, and the manager's mindset here, the rest of the exam starts making sense.

This domain is NOT about technical security controls. It is about policy, strategy, ethics, legal frameworks, and — above all — how organizations make risk-based decisions.

> □ **THE CORE INSIGHT** Security exists to enable the business, not to prevent it from functioning. Every decision in Domain 1 runs through that filter.

Why This Matters

Every CISSP question, regardless of domain, ultimately tests whether you think like a security manager or a security technician. Domain 1 gives you the language, frameworks, and mindset to answer every other question on the exam correctly.

Key Concepts

The CIA Triad

Everything in information security protects three things:

Property	Meaning
Confidentiality	Only authorized people can access information
Integrity	Information is accurate and has not been tampered with
Availability	Systems and data are accessible when needed

Additional properties you need to know:

Property	Meaning
Authentication	Proving who you claim to be
Non-repudiation	You cannot deny performing an action (digital signatures)
Authorization	Determining what you are allowed to do

Risk Management Core Concepts

Risk management is the heart of Domain 1. Understand these terms deeply — they show up in questions from every domain.

Term	Plain English Definition
Threat	Something that could cause harm (attacker, flood, fire)
Vulnerability	A weakness that a threat could exploit
Risk	The probability a threat exploits a vulnerability × the impact
Asset	Anything of value to the organization
Exposure	The degree of loss when a threat event occurs
Control / Safeguard	Something that reduces risk
Residual Risk	Risk that remains after controls are applied
Total Risk	Risk before any controls are applied

KEY FORMULA Risk = Threat × Vulnerability × Asset Value. Reduce any factor and you reduce the risk.

Risk Treatment Options

When you identify a risk, you have four options. The exam will ask you which is appropriate in a given scenario:

Option	What It Means
Avoid	Stop doing the risky activity entirely
Transfer	Pass the risk to a third party (insurance, contracts)
Mitigate	Reduce probability or impact through controls
Accept	Acknowledge the risk and do nothing (documented decision)

MEMORY TRICK

MATA — Risk Treatment

M — Mitigate (reduce the risk)
A — Accept (acknowledge and document)
T — Transfer (insurance or contract)
A — Avoid (stop the activity)

Security Governance

Governance means establishing who is responsible for security decisions and ensuring accountability. The key governance documents are:

Document	Purpose
Policy	High-level mandatory statement of management intent
Standard	Specific mandatory requirements (what to do)
Guideline	Recommended, non-mandatory advice (how to do it)
Procedure	Step-by-step instructions for a specific task
Baseline	Minimum acceptable security configuration

> □ *Policy is mandatory. Guidelines are optional. This distinction appears on the exam constantly.*

Due Care vs. Due Diligence

These two terms confuse nearly every CISSP student. Here is the clearest way to remember them:

Concept	Meaning
Due Care	Doing the right thing (acting reasonably)
Due Diligence	Investigating and understanding risks before acting

> □ **ANALOGY** Due diligence is researching a used car before you buy it. Due care is maintaining it properly after you own it.

Ethics

The CISSP exam tests the (ISC)² Code of Ethics. Know these four canons in order — they are prioritized:

Priority	Canon
1 (Highest)	Protect society, the common good, and the infrastructure
2	Act honorably, honestly, and legally
3	Provide diligent and competent service
4 (Lowest)	Advance and protect the profession

> □ *When society conflicts with your employer, society wins. When your employer conflicts with your client, your employer wins.*

Exam Tips

□ **EXAM FOCUS**

- ➤ Think like a manager — protect the business first, implement technology second
- ➤ Risk acceptance must always be formally documented and approved by senior management
- ➤ Policies are mandatory; guidelines are recommendations
- ➤ The (ISC)² Code of Ethics canons are prioritized — society first, always
- ➤ ALE = SLE × ARO — know this formula for quantitative risk analysis
- ➤ Total Risk vs Residual Risk — you always have residual risk after controls
- ➤ Due care = doing it right; Due diligence = researching before acting

Common Mistakes

- **Thinking technically:** The CISSP asks what a manager would do, not what a sysadmin would do.
- **Confusing risk transfer with mitigation:** Buying insurance transfers risk to the insurer; it does not reduce the risk itself.
- **Forgetting residual risk:** Controls reduce risk but never eliminate it. Residual risk always remains.
- **Mixing up standards and guidelines:** Standards are mandatory. Guidelines are suggestions.

Key Takeaways

- Domain 1 establishes the risk-based, management-focused mindset for the entire exam
- CIA Triad: Confidentiality, Integrity, Availability — the three pillars of everything
- Risk = Threat × Vulnerability × Asset Value — manage each factor
- Four risk treatment options: Avoid, Transfer, Mitigate, Accept
- Policy hierarchy: Policy > Standard > Guideline > Procedure
- (ISC)² Code of Ethics: Society first, profession last

Related Domains

Domain 1 influences every other domain. Key connections:

Domain	Connection to Domain 1
Domain 2 (Asset Security)	Asset classification drives risk prioritization
Domain 3 (Security Engineering)	Secure design principles reflect risk management decisions
Domain 5 (Identity & Access)	Access control is a risk mitigation strategy
Domain 8 (Software Security)	SDLC security is risk management applied to development

DOMAIN 2: ASSET SECURITY

Overview

Domain 2 covers how organizations identify, classify, own, and protect their assets. At 10% of the exam, it is moderately weighted but conceptually important — because you cannot protect what you haven't identified.

The big ideas here are: know what you have, know how sensitive it is, assign responsibility, and protect it proportionally.

> **THE CORE INSIGHT** Protection must be proportional to asset value and sensitivity. You don't put a $10 lock on a $10,000 asset.

Key Concepts

Data Classification

Classification tells everyone how sensitive data is and therefore how carefully it must be handled. Two common classification schemes:

Government Classification	Corporate Classification
Top Secret	Confidential / Proprietary
Secret	Private
Confidential	Sensitive
Unclassified	Public

> *Classification is assigned by the data owner — the person responsible for the data, not the person who created or handles it.*

Data Roles

Role	Responsibility
Data Owner	Senior manager; defines classification and access requirements
Data Custodian	IT/security staff; implements and maintains controls
Data Processor	Processes data on behalf of the owner
Data Subject	The individual the data is about (privacy context)
Data Steward	Manages data quality, governance, and policy compliance

> *The data owner is NOT the most technical person — it's the senior manager who bears business responsibility.*

Data States

State	Description
Data at Rest	Stored data (hard drives, databases, backups)
Data in Transit	Data moving across networks
Data in Use	Data actively being processed in memory

MEMORY TRICK

RUT — Data States
R — Rest (stored)
U — Use (in memory)
T — Transit (on the wire)

Data Handling Requirements

Each classification level requires specific handling procedures:

Activity	What It Means
Marking/Labeling	Physically or digitally identifying classification level
Handling	Procedures for accessing and using classified data
Storage	Secure storage requirements (encryption, access control)
Retention	How long data must be kept
Destruction	Secure methods for disposing of data

Data Destruction Methods

Method	Description
Clearing	Overwriting with non-sensitive data (reuse within org)
Purging	More thorough removal (degaussing, multiple overwrites)
Destruction	Physical destruction — shredding, incineration, disintegration
Sanitization	Making data unrecoverable through any means

Exam Tips

EXAM FOCUS

- ➤ The data owner is a manager, not a technical person — they assign classification
- ➤ Data custodians implement controls but do not define them
- ➤ Know the three data states: at rest, in transit, in use — and appropriate controls for each
- ➤ Clearing allows reuse within org; destruction allows no reuse
- ➤ Retention policies must align with legal and regulatory requirements

Key Takeaways

- Identify, classify, and assign ownership to every asset
- Data owner = business manager; Data custodian = IT implementer
- Three data states: at rest, in transit, in use
- Protection must be proportional to sensitivity and value
- Data destruction options: clear, purge, destroy — increasingly permanent

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Overview

Domain 3 is the most technically diverse domain on the CISSP exam, carrying 13% of the weight. It covers security models, architectural frameworks, cryptography, and physical security.

The CISSP does NOT expect you to engineer these systems. It expects you to understand the principles, know which model applies to which situation, and think about security architecture from a management perspective.

> □ **THE CORE INSIGHT** Security must be designed in from the start — 'security by design' beats 'security by addition'. Retrofitting security is always more expensive and less effective.

Key Concepts

Secure Design Principles

Principle	Plain English
Defense in Depth	Multiple layers of controls — if one fails, others remain
Least Privilege	Give users only the access they need — nothing more
Separation of Duties	No single person controls an entire critical process
Need to Know	Access only to information required for the current task
Fail Secure	When systems fail, they fail in a secure state (deny access)
Open Design	Security doesn't depend on keeping the design secret (Kerckhoffs)
Economy of Mechanism	Keep security mechanisms simple — complexity breeds vulnerabilities
Minimize Attack Surface	Reduce the number of ways an attacker can enter

Security Models

Security models are theoretical frameworks that define rules for how subjects (users, processes) can access objects (files, resources). Know these cold:

Model	Focus
Bell-LaPadula	Confidentiality
Biba	Integrity
Clark-Wilson	Integrity

Brewer-Nash (Chinese Wall)	Conflicts of interest
Take-Grant	Rights propagation

MEMORY TRICK

Bell-LaPadula — Confidentiality

Simple Security Property: No Read Up (don't read data above your level)
Star (*) Property: No Write Down (don't write data below your level)
Think: 'Top Secret agent can't write in the public newspaper'

MEMORY TRICK

Biba — Integrity (Bell-LaPadula flipped)

Simple Integrity: No Read Down (don't read lower-integrity data)
Star (*) Integrity: No Write Up (don't write to higher-integrity objects)
Think: 'A surgeon won't take medical advice from an unqualified source'

Cryptography Fundamentals

Concept	Definition
Symmetric Encryption	Same key used to encrypt and decrypt (fast, but key distribution problem)
Asymmetric Encryption	Public/private key pair — encrypt with public, decrypt with private
Hashing	One-way transformation creating a fixed-length fingerprint of data
Digital Signature	Hash encrypted with sender's private key — proves authenticity + integrity
Certificate	Digital ID — binds a public key to an identity, issued by a CA
PKI	Infrastructure for managing digital certificates and key pairs

Algorithm	Type & Key Detail
AES	Symmetric block cipher — 128/192/256-bit keys. NIST standard.
RSA	Asymmetric — based on difficulty of factoring large numbers
SHA-256	Hashing — produces 256-bit digest. Current standard.
3DES	Symmetric — legacy, uses DES 3 times. Being phased out.
ECC	Asymmetric — uses elliptic curves, smaller keys, same strength as RSA
Diffie-Hellman	Key exchange protocol — establishes shared secret over untrusted

	channel

Physical Security

Physical security is the last domain students study and the first line of defense in reality. The CISSP tests concepts, not implementations:

Control Type	Examples
Deterrent	Security cameras, warning signs, guards — discourage attackers
Preventive	Locks, fences, bollards — physically prevent access
Detective	Motion sensors, CCTV recording, audit logs — detect intrusions
Corrective	Fire suppression, incident response — respond and recover

Exam Tips

EXAM FOCUS

- Bell-LaPadula = Confidentiality; Biba = Integrity — opposite rules
- Fail secure = deny access on failure (bank vault); fail safe = allow egress on failure (fire exit)
- Symmetric encryption: fast, good for bulk data; Asymmetric: slow, good for key exchange
- A digital signature uses your PRIVATE key to sign, recipient uses your PUBLIC key to verify
- Defense in depth is always preferred over relying on a single control

Key Takeaways

- Design security in from the beginning — 'bolt-on' security is weak and expensive
- Bell-LaPadula protects confidentiality; Biba protects integrity
- Symmetric = same key; Asymmetric = public/private key pair
- Hashing is one-way; encryption is two-way
- Physical security layers: deterrent → preventive → detective → corrective

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Overview

Domain 4 covers how data moves across networks and how those networks are secured. At 13% of the exam, it is technically rich but — consistent with the CISSP mindset — the exam tests your ability to choose the right network security control for a given business situation, not configure routers.

> **THE CORE INSIGHT** Networks are attack pathways. Every connection is a potential entry point. The goal is to control what can communicate with what, and to ensure that communication is confidential, authenticated, and integrity-protected.

Key Concepts

OSI Model

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

MEMORY TRICK

Remember OSI from top to bottom

All People Seem To Need Data Processing

A = Application, P = Presentation, S = Session, T = Transport, N = Network, D = Data Link, P = Physical

Key Network Security Devices

Device	What It Does
Firewall	Filters traffic based on rules (stateless or stateful)
IDS	Intrusion Detection System — monitors and alerts (passive)
IPS	Intrusion Prevention System — monitors and blocks (active)

Proxy	Acts as intermediary — hides internal network from external
VPN	Encrypted tunnel over public network for remote access
WAF	Web Application Firewall — filters HTTP/HTTPS traffic
SIEM	Security Information and Event Management — centralized logging/alerting

Network Attacks

Attack	Description
DoS / DDoS	Flood a system with traffic to deny service to legitimate users
Man-in-the-Middle	Attacker intercepts communications between two parties
ARP Poisoning	Fake ARP replies link attacker MAC to victim IP (Layer 2)
DNS Spoofing	Falsify DNS records to redirect traffic to malicious sites
Session Hijacking	Steal a valid session token to impersonate an authenticated user
Replay Attack	Capture valid credentials/tokens and retransmit to authenticate

Network Security Protocols

Protocol	Purpose
TLS/SSL	Encrypts web traffic (HTTPS) — authenticate server, encrypt data
IPSec	Encrypts at the network layer — used for VPNs
SSH	Encrypted remote administration (replaces Telnet)
SFTP / SCP	Secure file transfer over SSH
HTTPS	HTTP over TLS — encrypted web browsing
DNSSEC	DNS with cryptographic validation — prevents DNS spoofing

Exam Tips

EXAM FOCUS

- IDS detects and alerts; IPS detects and blocks — IPS is placed inline
- Stateful firewalls track connections; stateless filter by packet attributes only
- VPN provides confidentiality over public networks; IPSec operates at Layer 3
- TLS provides confidentiality AND integrity for web traffic
- The OSI model: know which layer each protocol and device operates at
- Defense in depth for networks: perimeter firewall → IPS → internal segmentation → host

controls

Key Takeaways

- OSI model: 7 layers from Physical (1) to Application (7)
- IDS = passive monitor; IPS = active block
- VPNs create encrypted tunnels over untrusted public networks
- Always think in layers — perimeter, network, host, application
- Network segmentation limits blast radius when a breach occurs

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT (IAM)

Overview

Domain 5 covers who can access what, how they prove it, and how those decisions are made. At 13% of the exam, IAM is one of the most tested areas. It connects directly to risk management — because unauthorized access is one of the top business risks.

> □ **THE CORE INSIGHT** Identification says who you are. Authentication proves it. Authorization determines what you can do. Accountability ensures we can track what you did.

Key Concepts

The IAM Framework

Step	Concept
1	Identification
2	Authentication
3	Authorization
4	Accountability

Authentication Factors

Factor	Type
Something You Know	Type 1
Something You Have	Type 2
Something You Are	Type 3
Somewhere You Are	Type 4
Something You Do	Type 5

> □ *Multi-factor authentication (MFA) uses TWO DIFFERENT factor types. Two passwords is NOT MFA — it's two Type 1 factors.*

Access Control Models

Model	How Access Is Granted
DAC (Discretionary)	Data owner decides who gets access

MAC (Mandatory)	System enforces based on labels/classifications
RBAC (Role-Based)	Access based on job role
ABAC (Attribute-Based)	Access based on attributes (dept, time, location)
Rule-Based	Fixed rules (e.g., firewall rules)

 ANALOGY RBAC is like a job title — if you're a nurse, you can access patient records. MAC is like a military clearance — your label determines your access, regardless of role.

Biometric Performance Metrics

Metric	Definition
FRR (False Rejection Rate)	Type 1 Error — legitimate user denied (too strict)
FAR (False Acceptance Rate)	Type 2 Error — unauthorized user accepted (too lenient)
CER / EER	Crossover Error Rate — where FRR and FAR are equal; lower CER = better biometric

 Higher security needs = lower FAR (you'd rather annoy legitimate users than accept attackers). Lower CER = more accurate system.

Exam Tips

 EXAM FOCUS

- DAC = owner controls access; MAC = system controls access based on labels
- MFA requires factors from DIFFERENT types — not two passwords
- Least privilege: give only the minimum access needed for the job
- CER/EER: lower is better; the sweet spot where FAR and FRR are equal
- Provisioning and de-provisioning: access must be removed promptly when no longer needed
- Single Sign-On (SSO) improves user convenience but creates a single point of failure

Key Takeaways

- Identify → Authenticate → Authorize → Account for actions
- MFA = two different factor types, not two of the same type
- RBAC is most common in enterprise; MAC is used in classified environments
- Least privilege and need-to-know limit damage from compromised accounts
- Biometric accuracy measured by CER/EER — lower is better

DOMAIN 6: SECURITY ASSESSMENT AND TESTING

Overview

Domain 6 covers how organizations validate that their security controls actually work. At 12% of the exam, this domain bridges strategy (Domain 1) and operations (Domain 7) by providing the verification mechanisms that confirm the security program is effective.

> **THE CORE INSIGHT** You can't manage what you don't measure. Security assessments answer the critical question: 'Are our controls actually working?'

Key Concepts

Assessment Types

Assessment Type	What It Is
Vulnerability Assessment	Identifies vulnerabilities — does NOT exploit them
Penetration Test	Simulated attack — actively exploits vulnerabilities to test defenses
Security Audit	Formal review of controls against a standard or policy
Security Review	Informal check of security posture
Risk Assessment	Identifies and prioritizes risks to the organization

> *Vulnerability assessments find holes; penetration tests prove they can be exploited. They serve different purposes.*

Penetration Testing Types

Type	Tester Knowledge
Black Box	No prior knowledge
White Box	Full knowledge
Gray Box	Partial knowledge

Penetration Testing Phases

Phase	Activity
1. Planning & Reconnaissance	Define scope, rules of engagement, gather intelligence
2. Scanning & Enumeration	Discover live hosts, open ports, services, vulnerabilities

3. Exploitation	Attempt to exploit identified vulnerabilities
4. Post-Exploitation	Assess impact, move laterally, escalate privileges
5. Reporting	Document findings, risk ratings, and remediation recommendations

Log Management and SIEM

Concept	Purpose
Log Review	Periodic review of security logs for anomalies
SIEM	Aggregates and correlates logs from multiple sources in real time
NTP (Time Sync)	Accurate timestamps are critical for log correlation and forensics
Log Retention	Retain logs long enough to support investigations (often 1+ years)

Exam Tips

EXAM FOCUS

- Vulnerability assessment = identify; Penetration test = exploit and prove
- Always get written authorization before conducting any penetration test
- Gray box testing is most realistic for most enterprise scenarios
- Continuous monitoring outperforms point-in-time assessments for detecting threats
- SIEM provides real-time correlation; logs alone do not provide correlation

Key Takeaways

- Assessments validate that controls work — do them regularly
- Pen test requires written permission — unauthorized testing is illegal
- Black box: no knowledge; White box: full knowledge; Gray box: partial
- SIEM aggregates logs and provides real-time alerting
- Metrics and KPIs let management track security program effectiveness

DOMAIN 7: SECURITY OPERATIONS

Overview

Domain 7 is the largest operational domain on the CISSP exam at 13%. It covers incident response, disaster recovery, forensics, patch management, and the day-to-day running of security operations. If Domain 1 is strategic, Domain 7 is tactical.

> **THE CORE INSIGHT** Security operations is about maintaining confidentiality, integrity, and availability on an ongoing basis — and responding quickly and correctly when something goes wrong.

Key Concepts

Incident Response Phases

Phase	Key Activities
1. Preparation	Build the IRT, create policies, set up tools, train staff
2. Identification	Detect that an incident has occurred; determine scope
3. Containment	Stop the bleeding — limit damage spread
4. Eradication	Remove the root cause (malware, attacker foothold)
5. Recovery	Restore systems to normal operation
6. Lessons Learned	Document, analyze, and improve — post-incident review

MEMORY TRICK

PICERL — Incident Response

P — Preparation
I — Identification
C — Containment
E — Eradication
R — Recovery
L — Lessons Learned

Business Continuity vs. Disaster Recovery

Concept	Focus
BCP (Business Continuity)	Keeping business functions running during a disaster
DRP (Disaster Recovery)	Restoring IT systems after a disaster

Metric	Definition
RTO (Recovery Time Objective)	Maximum acceptable downtime — how fast must systems be restored?
RPO (Recovery Point Objective)	Maximum acceptable data loss — how much data can we afford to lose?
MTD (Max Tolerable Downtime)	Longest a business function can be unavailable before permanent harm

> □ *RTO is about TIME to recover. RPO is about DATA you can afford to lose. MTD must be longer than RTO — if it isn't, your RTO is unachievable.*

Recovery Site Types

Site Type	Description
Hot Site	Fully operational duplicate — data mirrors in real time
Warm Site	Partially equipped — hardware ready, needs data loaded
Cold Site	Empty facility — infrastructure only, everything must be set up
Mobile Site	Portable, self-contained facility

Digital Forensics Principles

Principle	Why It Matters
Preserve Evidence	Never work on original evidence — always work on verified copies
Chain of Custody	Document every person who handles evidence from collection to court
Order of Volatility	Collect most volatile (RAM) to least volatile (archival storage) first
Legal Hold	Suspend data destruction for data relevant to litigation or investigation

□ **MEMORY TRICK**

Order of Volatility — Most to Least

1. CPU registers and cache (gone in microseconds)
2. RAM / memory (gone when system powers off)
3. Running processes and network connections
4. Hard disk storage
5. Remote logs and backups

Exam Tips

EXAM FOCUS

- Incident Response order: PICERL — never skip containment to go straight to eradication
- RPO drives backup frequency; RTO drives recovery system design
- Hot site = highest cost, fastest recovery; Cold site = lowest cost, slowest recovery
- Forensics: document everything, work on copies, maintain chain of custody always
- Separation of duties in operations: no single person should approve AND implement changes
- Change management: all changes must be approved before implementation

Key Takeaways

- Incident response: Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned
- BCP = keeping the business running; DRP = restoring IT systems
- RTO = time to recover; RPO = data you can afford to lose
- Hot/Warm/Cold sites: speed and cost trade-offs
- Forensics: preserve, copy, document, maintain chain of custody

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY

Overview

Domain 8 covers how to build security into software from the very beginning. At 10% of the exam, it is the final domain but no less critical — because insecure software is the root cause of the majority of security breaches.

> **THE CORE INSIGHT** Security must be built into software during design — not tested in at the end. A vulnerability found in design costs $1 to fix; the same vulnerability found in production costs $100 to $1,000.

Key Concepts

SDLC Security Integration

SDLC Phase	Security Activity
Requirements	Define security requirements alongside functional requirements
Design	Threat modeling, security architecture review
Development	Secure coding standards, code review
Testing	Security testing, penetration testing, SAST/DAST
Deployment	Hardening, configuration management, change control
Maintenance	Patch management, ongoing vulnerability scanning

Common Software Vulnerabilities

Vulnerability	Description
Buffer Overflow	Writing data beyond allocated memory — can overwrite code/data
SQL Injection	Injecting malicious SQL into input fields to manipulate databases
Cross-Site Scripting (XSS)	Injecting scripts into web pages viewed by other users
Cross-Site Request Forgery (CSRF)	Tricking authenticated users into performing unintended actions
Race Condition (TOCTOU)	Exploiting time gap between checking a condition and using it
Insecure Direct Object Reference	Manipulating IDs in URLs to access unauthorized resources

Testing Types

Test Type	What It Does
SAST (Static Analysis)	Analyzes source code without running it — finds vulnerabilities in code
DAST (Dynamic Analysis)	Tests running application — simulates attacks
IAST	Hybrid — instruments the application from inside during testing
Fuzzing	Sends random/malformed input to find unexpected failures
Code Review	Manual review of code by developers or security experts

Change and Configuration Management

Concept	Purpose
Change Management	Formal process to evaluate, approve, and implement changes
Configuration Management	Track and control how systems are configured
Baseline Configuration	Known-good configuration used as reference and rollback point
Versioning	Track changes to code over time; enables rollback

Exam Tips

EXAM FOCUS

- Security is 100x cheaper when built in during design versus retrofitted in production
- Input validation is the primary defense against injection attacks (SQLi, XSS, command injection)
- SAST = source code analysis; DAST = running application testing
- Separation of environments: dev, test, staging, production — never test in production
- Change management must be approved before implementation — emergency changes too
- Threat modeling (STRIDE) identifies threats during design phase

Key Takeaways

- Build security in during requirements and design — not as an afterthought
- Common vulnerabilities: buffer overflow, SQL injection, XSS, CSRF
- SAST tests code; DAST tests running application
- Input validation prevents most injection attacks
- Change management: approve first, implement second — always

Continue Your CISSP Journey

The Premium Threatnexis CISSP Toolkit includes:

- ✓ Complete domain mastery guides (100+ pages each)
- ✓ Full visual memory maps and concept diagrams
- ✓ Advanced mnemonics and memory palace systems
- ✓ 500+ scenario-based practice questions
- ✓ Manager mindset coaching frameworks
- ✓ Flashcard decks for every domain
- ✓ Rapid review and exam-day sheets
- ✓ 30, 60, and 90-day study plans
- ✓ Cross-domain relationship maps
- ✓ Exam strategy and question dissection guides

[Unlock the Premium CISSP Toolkit — ThreatNexis.com]

[Book a CISSP Coaching Session]

[Subscribe Free — CISSP Insider Newsletter]