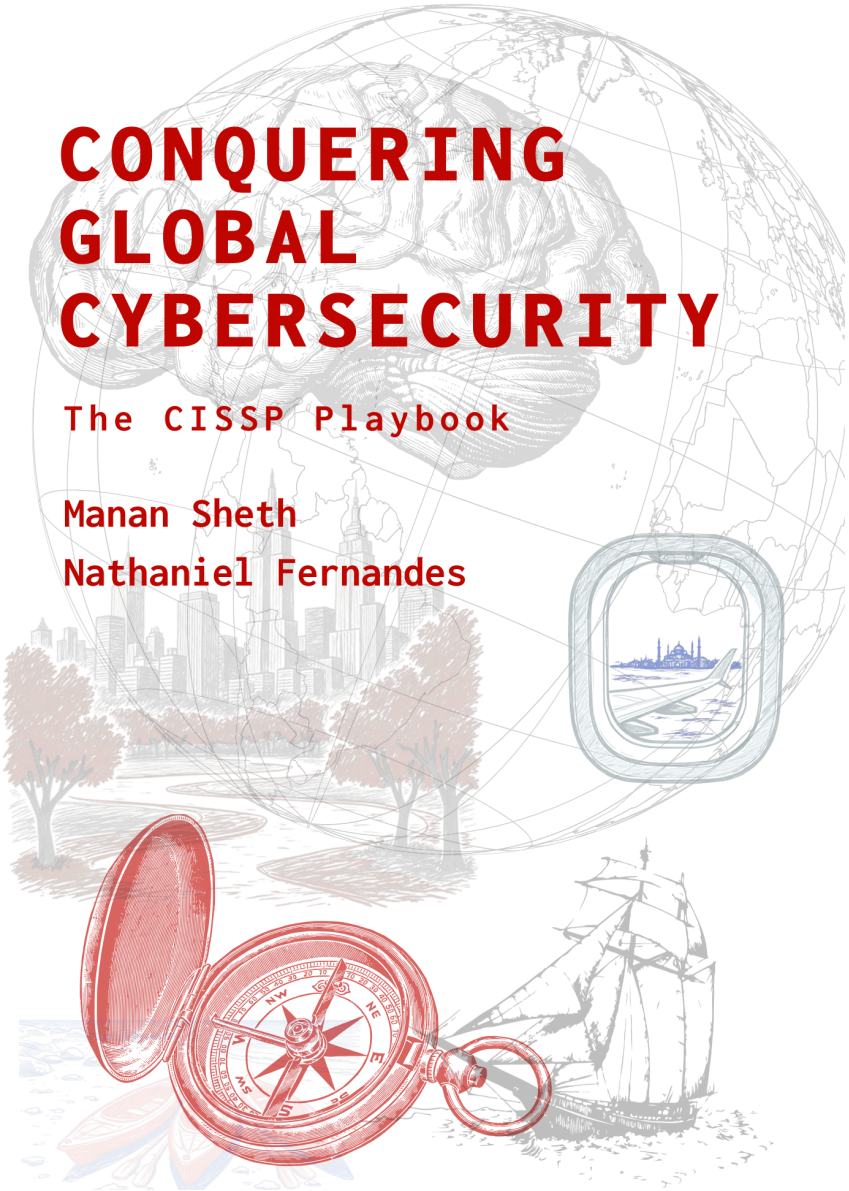
CONQUERING GLOBAL CYBERSECURITY

The CISSP Playbook

Manan Sheth
Nathaniel Fernandes



Conquering global Cybersecurity

The CISSP Playbook

Dedication

This book comes from a learning journey that is still in progress.

It was shaped by curiosity, uncertainty, and a lot of time spent trying to understand things that did not make sense at first, and some still don't.

I did not start with all the answers. Most of what I know came from showing up, getting things wrong, asking better questions over time, and slowly connecting the dots. This book reflects that process in its core.

I am deeply grateful to my family, Mitesh, Vatsala, and Zalak, for their constant support and belief in me during years of change and growth. Their stability made it easier to stay focused when the path felt unclear.

I am also thankful to the people who helped shape my thinking along the way.

I would like to thank my Mentors along my career (Ravindra Gotavade, Burgess Cooper, Burzin Bharucha, Rohit Mathur, Michitaka Arima, and Shweta Tripathi), colleagues, and mentees who challenged my assumptions and shared their experiences with me.

Finally, thank you to every volunteer and reviewer who took the time to contribute.

This book exists because of that shared effort

Manan Sheth

Behind every page of this book are the people who stood by me when life was uncertain - the ones who shaped me, challenged me, and reminded me to keep going when it would have been easier to stop.

Some people believe in you when you're already winning.

Others believe in you while you're still becoming - tired, unsure, and still moving forward anyway. Those people deserve the credit long before success ever arrives.

To my mom and dad - thank you for the love that held me steady through every phase of my life. Thank you for standing beside me even when the direction wasn't clear. This book carries more of you in it than you'll ever know.

To my friends and mentors - thank you for your guidance, honesty, and the push to rise higher than I thought I could. You didn't just support the journey - you helped shape the person who could finish it.

And to Yuvraj Todankar - Thank you. You played a massive role in bringing this book to life. You showed up through the process, pushed me when I needed it, and believed in this work before it was fully built. This book would not be what it is without you, and I will always be grateful.

Nathaniel Fernandes

Acknowledgments

We would like to acknowledge and thank the reviewers who generously shared their expertise and feedback throughout this journey. Your inputs strengthened the quality of this book, and we are grateful for the role you played in shaping the final work.

From Manan Sheth & Nathaniel Fernandes

Ravindra Gotavade

Ravindra Gotavade is an experienced OT Security Architect specialising in cybersecurity for manufacturing Industries, with expertise in regulations such as NIS2, the Cyber Resilience Act, and GDPR. With a strong background in IT/OT security management, risk assessments, and security architecture development.

Lekshmy Iyer

With over a decade of experience in IT and cybersecurity, she has successfully led teams and delivered security assessments across a wide range of industries. Specializing in Vulnerability Assessment and Penetration Testing (VAPT), as well as compliance audits like ISO and PCI, Lekshmy combines technical expertise with a deep understanding of risk management and security protocols. Passionate about safeguarding digital environments, she continues to explore emerging cybersecurity trends and contributes to fostering secure, resilient systems.

Sumir Broota

A pundit of networking and DevSecOps, a Kubestronaut and a moderator of BreachForce, a vibrant, 1200+ member cybersecurity community in Mumbai.

Rehan Shaikh

An Application Security specialist who breaks websites, infiltrates networks, and tinkers with operating system, turning real-world attacks into practical defenses.

Jagdish Mohite

Jagdish Mohite is a experienced cybersecurity and risk management professional specializing in information security governance, risk management, and compliance. He holds ISO 27001 and ISO 31000 certifications and focuses on applying security frameworks, audits, and risk assessments in practical, real-world environments.

Kaustubh Rai

Product security specialist focused on secure design, application security testing, and real-world exploitation. Moderator at BreachForce.

Mahadev Gavas

Mahadev Gavas is a cybersecurity professional with experience in offensive security, enterprise risk assessment, digital forensics,

and incident response. He is also the Organizer of Security BSides Mumbai, founder and former ctf player of team DarkArmy.

About the Authors

Nathaniel Fernandes

Nathaniel Fernandes is a cybersecurity professional who works at the intersection of offensive security, cloud security, and business risk. Known for connecting disciplines that are usually treated separately, he brings together technical depth, real-world incident awareness, and a strategic mindset to help organisations make security decisions that actually hold up in practice. With experience supporting multiple environments and stakeholders, he focuses on building security that is practical, measurable, and aligned with how businesses truly operate.

Manan Sheth

Manan Sheth is an Information Security professional who works at the intersection of technology, risk, and Organisational Resilience. His approach is shaped by hands-on learning and sheer curiosity in how security principles translate into real-world responsibility.

Rather than focusing on tools or trends, Manan's work centres on understanding systems as they exist, identifying what truly matters, and helping managers navigate complexity with the clarity needed for the exam.

He believes in this book as an extension of that mindset. Written for managers and leaders, it aims to make cybersecurity concepts practical, relatable, and usable without losing their depth.

Manan continues to learn, write, and refine his thinking by constantly engaging with local communities and

cybersecurity-focused groups while mentoring new blood in his free time. He aims to make this book a pathway towards CISSP, not as a daunting task, but an enriching journey.

MINDSET

The CISSP mindset is the ability to think like a security leader, not a tool operator. It focuses on risk management, governance, and business impact, choosing the answer that best protects people first, supports the organisation, and aligns with policy, accountability, and long-term strategy over quick technical fixes.

Hey! I found a mistake in the book!

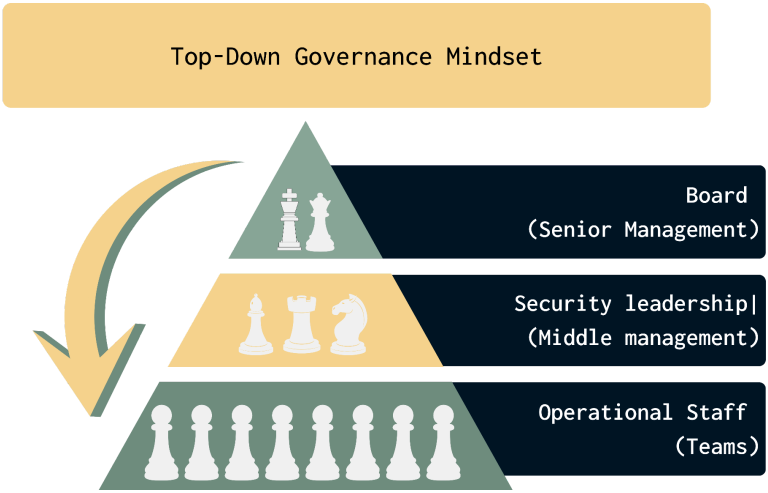
This book was built with care, but we are only human, and no book is ever perfect. If you spot an error, an unclear explanation, or something that can be improved, please reach out and let us know. We genuinely appreciate sharp eyes and honest feedback, and if your suggestion is valid and accepted, we would be happy to acknowledge you by name in a future update. Please email us book@wehost.co.in

Disclaimer

This book has been developed with the Indian ecosystem in mind. It includes analogies and simplified scenarios to improve clarity and understanding. Readers should interpret these examples as teaching tools and focus on the underlying concepts rather than literal or one-size-fits-all applications.

Domain 1: Security and Risk Management

CISSP Exam Mindset



Key Points:

1. Think like a CEO, not a technician - strategic decisions over technical implementations
2. Security as a business enabler, not just a protection mechanism
3. Safety first: Human life > data protection always
4. Policy > procedure in exam questions
5. Comprehensive thinking: broader answers are usually correct
6. Top-down governance: senior management drives security

Exam Tip: When multiple answers seem correct, choose:

1. Policy over procedure
2. Safety over assets
3. More comprehensive option
4. Strategic thinking over immediate action

Core Security Concepts: Subjects & Objects

Subject	Object
Active entities	Passive entities
A subject is a person, process, program, or anything similar that actively tries to access an object	An object is anything that is being passively accessed by a subject, like a file, server, process, or hardware component.

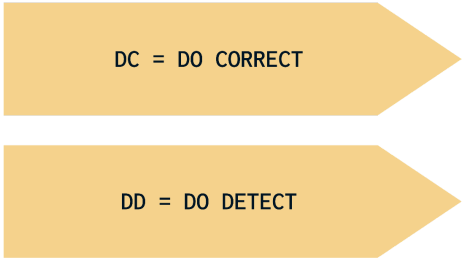
Key Points:

1. Subject: Active entity (users, processes) accessing resources
2. Object: Passive data (files, databases, documents)
3. Tricky Example: iexplore.exe is a subject when running, an object when stored on disk

Exam Tip: Subject performs actions; object receives actions. Any confusion? Ask "who acts" vs "what is acted upon"

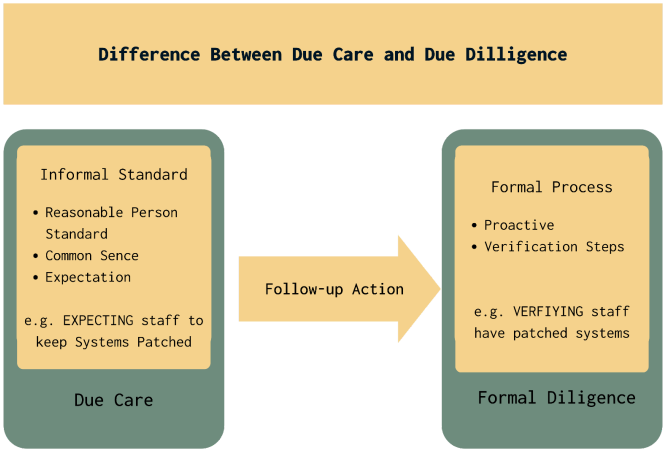
Due Care vs Due Diligence

Due Care v/s Due Diligence



Key Points:

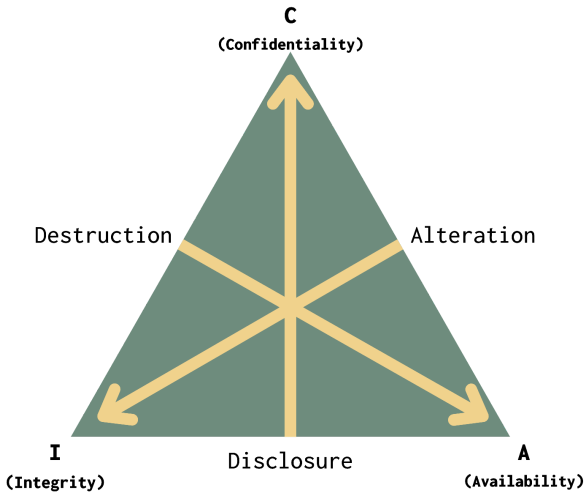
1. Due Care: Doing what a reasonable person would do (prudent man rule)
2. Due Diligence: Managing and verifying due care (process-driven)
3. Due care = informal wisdom; Due diligence = documented verification
4. Example: Expecting staff to patch (care) vs verifying patches (diligence)
5. Gross Negligence: Opposite of due care - legally critical for liability



Exam Tip:

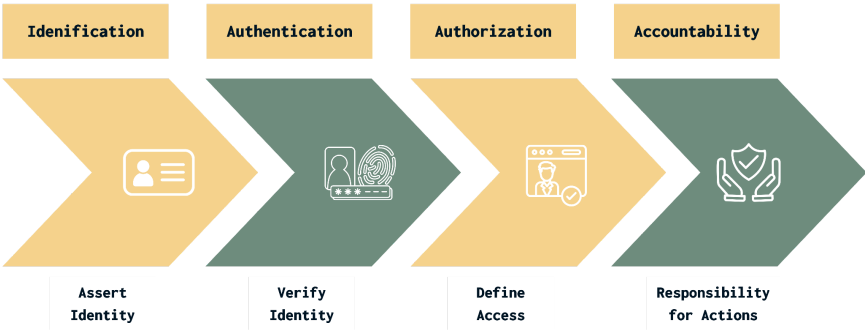
- Due care = what to do
- Due diligence = proving you did it.
- Think "care is action, diligence is evidence"

CIA Triad Extended



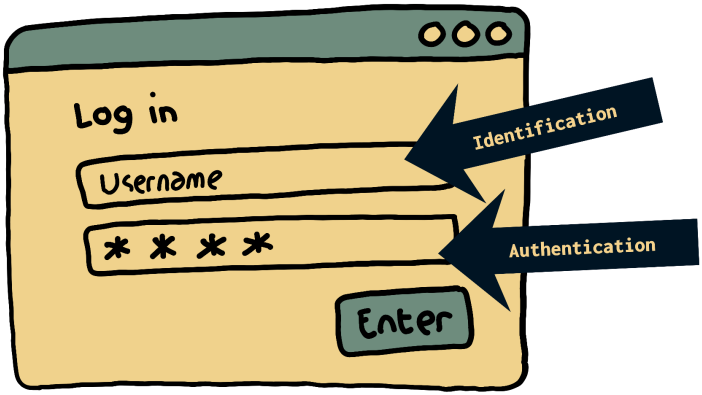
1. CIA: Confidentiality, Integrity, Availability
2. DAD: Disclosure, Alteration, Destruction

Identity & Access Management (IAAA)



Key Points:

1. Identity: Who you claim to be (unique identifier, avoid role-revealing names)
2. Authentication: Proving identity (Type 1: know, Type 2: have, Type 3: are)
3. Authorisation: What you are allowed to do (access control models)
4. Accountability: Tracking actions (logging, auditing, non-repudiation)



Authentication Factors:

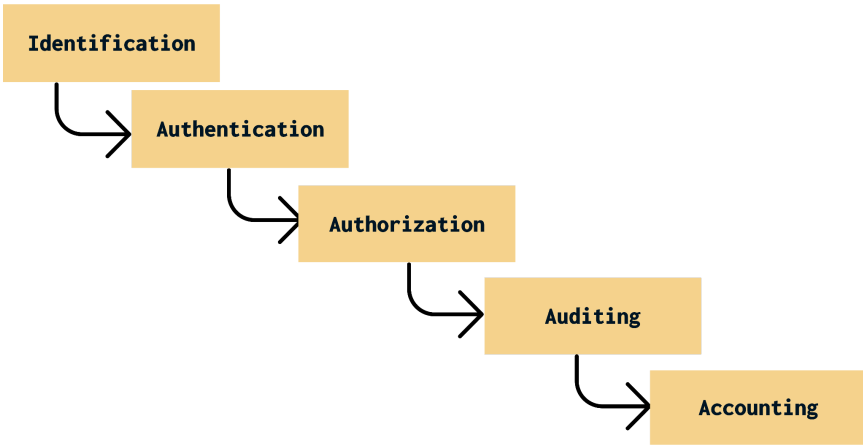
Authentication By Knowledge	Authentication By Ownership	Authentication By Characteristic
Something you know	Something you have	How you behave or your physiology; something you are

1. Type 1 (Something You Know): Passwords, PINs, security questions
2. Type 2 (Something You Have): Smart cards, tokens, mobile OTP
3. Type 3 (Something You Are): Biometrics (fingerprint, iris, facial)
4. National ID covers billions with fingerprint/iris biometrics

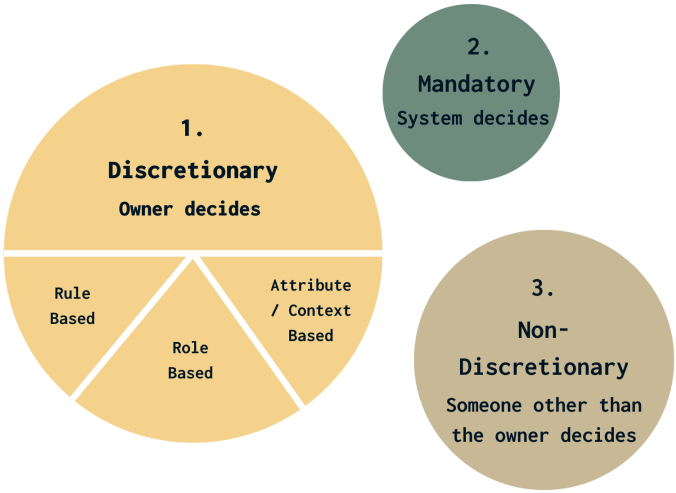
5. Banking uses SMS OTP for high-value transactions (vulnerable to SIM swap)

Exam Tip:

- MFA requires factors from DIFFERENT types. Password + security question = single factor (both Type 1)



Access Control Models



Key Points:

DAC (Discretionary Access Control):

1. The owner decides access permissions
2. Flexible but with potential security gaps
3. Example: Windows file permissions

MAC (Mandatory Access Control):

1. Central authority enforces labels (Top Secret, Secret, Confidential)
2. High security, rigid structure
3. Example: Military/government classified systems

RBAC (Role-Based Access Control):

1. Permissions assigned to roles, users assigned to roles
2. Scalable, most common in enterprise
3. Example: Bank customer service can view but not modify transactions

ABAC (Attribute-Based Access Control):

1. Access based on subject + object + environment attributes

2. Dynamic, context-aware decisions
3. Example: ATM withdrawal is allowed only during business hours from the registered location

Model	Security Level	Flexibility	Complexity	Best Use Case
DAC	Low - Medium	High	Low	Small Organization, File Sharing
MAC	Very High	Low	High	Government, Military, Classified Data
RBAC	Medium - High	Medium	Medium	Enterprise systems, standard workflow
ABAC	High	Very High	Very High	Dynamic environment, fine-grained control

Indian Context:

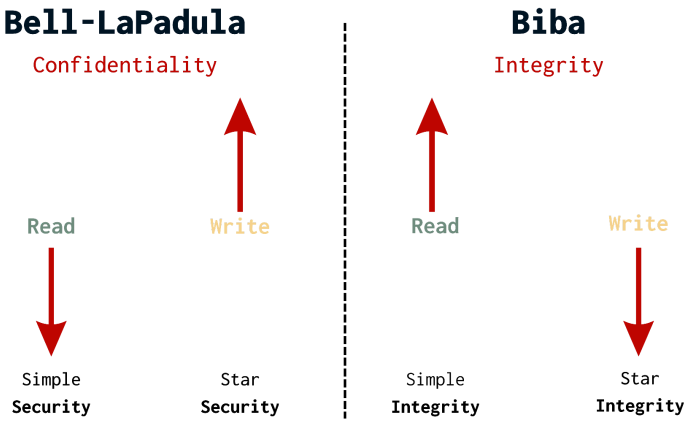
1. Tax systems use RBAC: officers access only the assigned jurisdiction
2. The government implements MAC for classified data and RBAC for unclassified data

Exam Tip: Look for keywords:

1. "owner decides" = DAC,
2. "classification labels" = MAC,
3. "job function" = RBAC,
4. "multiple factors/context" = ABAC

Additional Security Models

Bell-LaPadula Model:

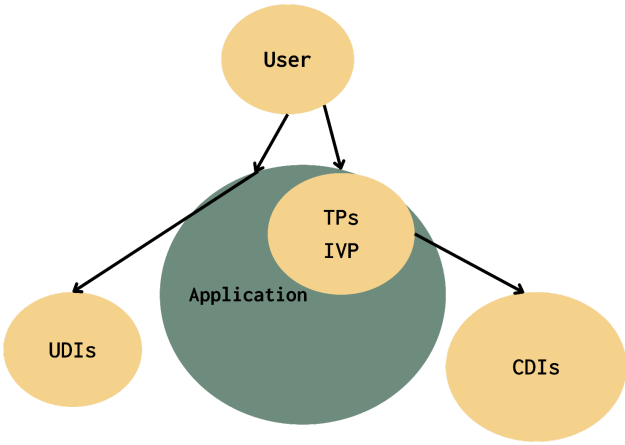


1. Confidentiality-focused (military classification)
2. No Read Up (Simple Security Property) - can't read higher classification
3. No Write Down (★ Star Property) - can't write to lower classification
4. Example: A Secret clearance user can't read Top Secret files

Biba Model:

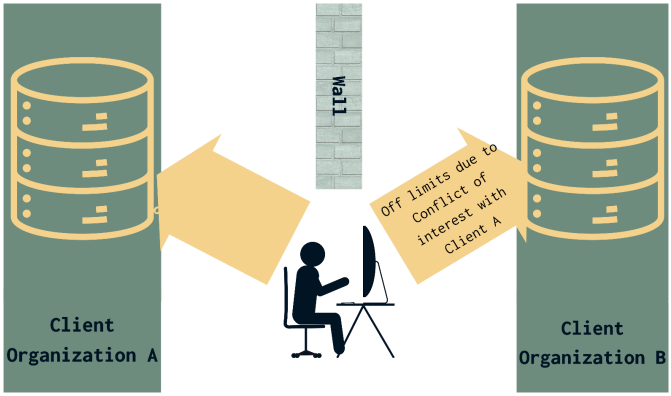
1. Integrity-focused (opposite of Bell-LaPadula)
2. No Write Up (Simple Integrity) - can't write to higher integrity
3. No Read Down (★ Integrity Property) - can't read lower integrity
4. Example: Production system can't read from untrusted development data

Clark-Wilson Model:



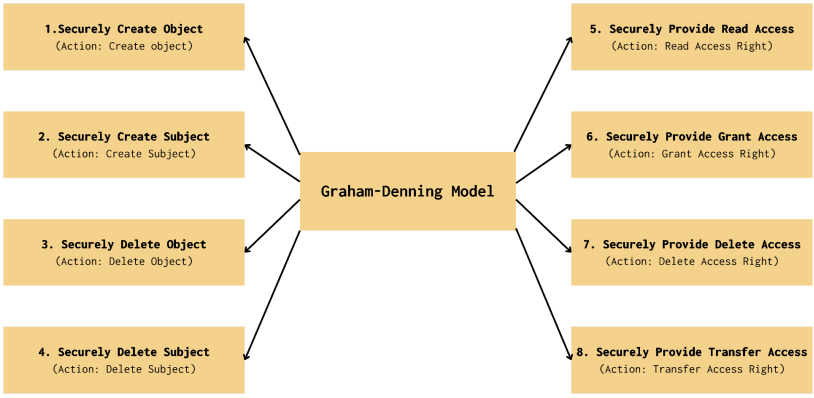
1. Commercial integrity focus
2. Well-Formed Transactions + Separation of Duties
3. CDI (Constrained Data Items), TP (Transformation Procedures), IVP (Integrity Verification)
4. Example: Banking - tellers use transaction programs, can't directly modify balances

Brewer-Nash (Chinese Wall):



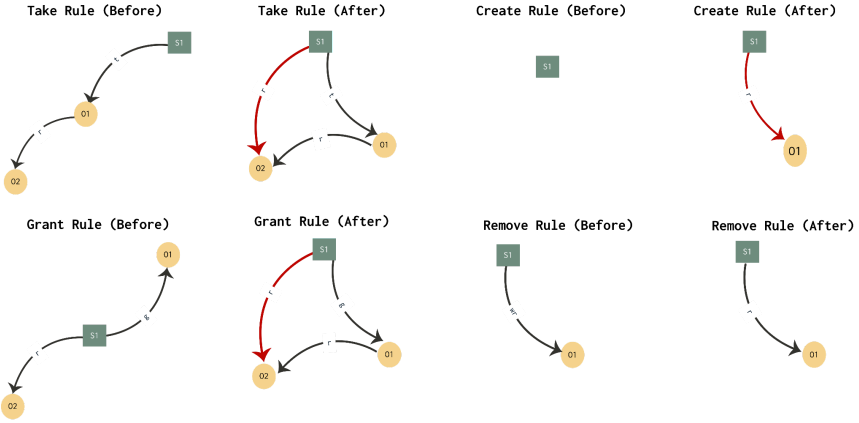
1. Conflict of interest prevention
2. Dynamic separation based on previous accesses
3. Example: Consultant accessing Bank A data blocks, Bank B access

Graham-Denning Model:



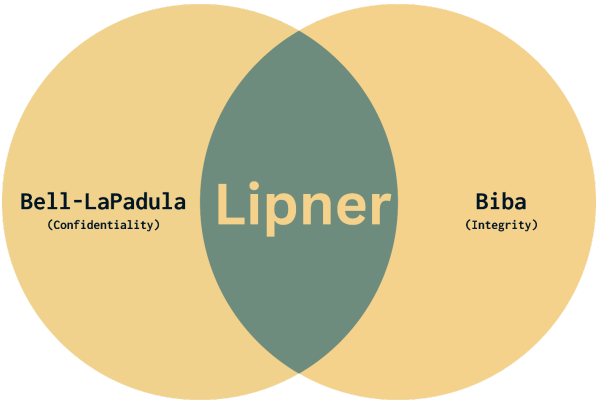
1. Eight protection rights: create/delete objects, subjects, and access rights
2. Example: OS kernel permission management

Take-Grant Model:



1. Access rights transfer via directed graphpadi
2. Four operations: take, grant, create, revoke
3. Example: User delegates file access rights to another user

Lipner Model:

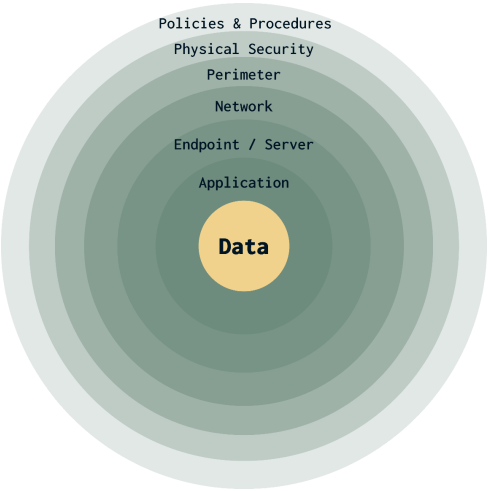


1. Combines Bell-LaPadula (confidentiality) + Biba (integrity)
2. Example: Development vs production environment protection

Exam Tip:

1. Bell-LaPadula = Confidentiality (no read up/write down)
2. Biba = Integrity (no write-up / read-down)
3. Clark-Wilson = Integrity/commercial
4. Chinese Wall = Conflict prevention
5. Graham-Denning = Rights framework
6. Take-Grant = Rights delegation
7. Lipner = Combines Bell-LaPadula + Biba

Defence in Depth Strategy



Key Points:

1. Multiple security layers (no single point of failure)
2. Forces attackers through multiple obstacles
3. Increases detection likelihood

Layers:

1. Physical: Perimeter, guards, biometrics, mantraps
2. Network: Firewalls, IPS, segmentation, VLANs
3. Host: OS hardening, HBIPS, patching, endpoint protection
4. Application: Secure coding, input validation, WAF
5. Data: Encryption (rest/transit), digital signatures, DLP

Indian Context:

1. Data centres: 5 layers (perimeter wall, guards, mantrap, biometric, server cage)
2. Payment platforms encrypt with AES-256-GCM (rest) + TLS 1.3 (transit)

Exam Tip: Physical access defeats all logical controls - always consider physical security first

Governance Structure & Policy Hierarchy

Executive (Senior) Management	Sets the proper tone from the top, promotes the audit process, and provides support where needed.
Audit Committee	Composed of members of the Board/senior stakeholders to provide oversight of the audit program.
Security Officer	Advises on security-related risks to be evaluated in the audit program.
Compliance Manager	Ensures corporate compliance with applicable laws and regulations, professional standards, and company policy.
Internal Auditors	Company employees who provide assurance that corporate internal controls are operating effectively.
External Auditors	Provide an unbiased and independent audit report as they are independent of the entity being audited.

Key Points:

Governance Hierarchy:

1. Board: Ultimate accountability, strategic oversight
2. CEO: Strategy approval, resource allocation
3. CISO: Implementation, compliance monitoring
4. Business Units: Operational compliance
5. All Personnel: Individual responsibilities

Policy Hierarchy (Wedding Menu Analogy):

1. Policy: High-level intent ("We serve vegetarian") - Board/CEO approved, strategic
2. Standards: Mandatory specifications ("Paneer must be 200g") - specific requirements
3. Procedures: Step-by-step instructions ("Heat oil to 180°C, add cumin...") - detailed how-to
4. Guidelines: Recommendations ("Add extra cream for richness") - best practices, optional

Indian Context:

1. RBI mandates board-level IT Strategy Committees for banks
2. DPDP Act 2023 requires data protection policies
3. CERT-In: 6-hour breach reporting, 180-day log retention

Exam Tip: "First step" questions = Policy development. Authority questions = Board/CEO approval. Implementation = Top-down

Risk Management Formulas (CRITICAL)

Quantitative Risk Analysis:

1. Single Loss Expectancy (SLE):

SLE = Asset Value (AV) × Exposure Factor (EF)

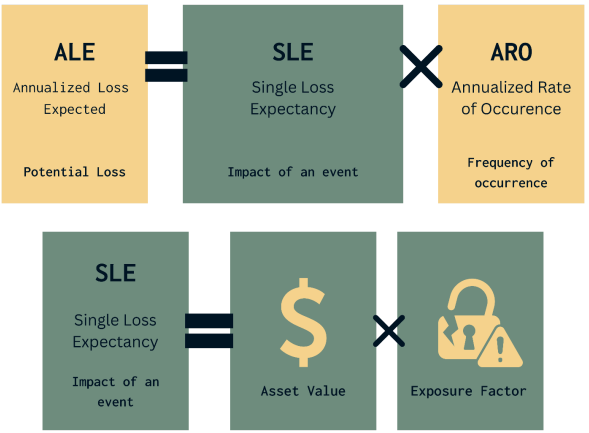
1. Expected loss from ONE incident
2. Example: Server ₹50 lakhs, fire destroys 60% → SLE = ₹30 lakhs

2. Annual Rate of Occurrence (ARO):

ARO = Number of times threat expected per year

1. Example: Ransomware expected 2x/year → ARO = 2.0

3. Annual Loss Expectancy (ALE):



ALE = SLE × ARO

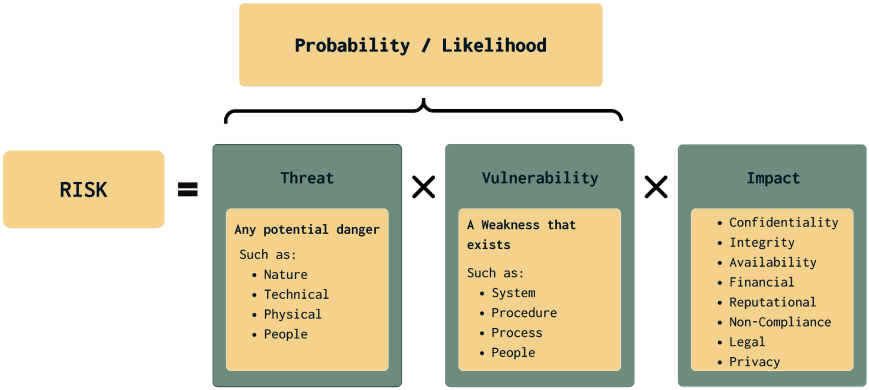
1. Yearly expected loss
2. Example: ₹30 lakhs × 2 = ₹60 lakhs annual loss

Cost-Benefit Analysis:

Control Cost ≤ Risk Reduction Value

If Annual Safeguard Cost > (ALE_before - ALE_after) → ACCEPT RISK

Risk Calculation:



Total Risk = Threats × Vulnerabilities × Asset Value

Residual Risk = Total Risk - Control Effectiveness

Example Problem:

1. Risk: Data breach (ALE = ₹5 crores)
2. Control: DLP solution (₹50 lakhs initial + ₹10 lakhs/year)
3. Risk Reduction: 80% (new ALE = ₹1 crore)
4. Annual Benefit: (₹5 crores - ₹1 crore) - ₹10 lakhs = ₹3.9 crores
5. Decision: IMPLEMENT (benefit > cost)

Exam Tip: If safeguard cost > risk reduction, ACCEPT THE RISK. Residual risk always remains - can only be reduced, never eliminated.

Term	Description
Threat Agent	Entity that has the potential to cause damage to an asset (e.g., external attackers, internal attackers, disgruntled employees).
Threat	Any potential danger.
Attack	Any harmful action that exploits a vulnerability.
Vulnerability	A weakness in an asset that could be exploited by a threat.
Risk	Significant exposure to a threat or vulnerability (a weakness that exists in an architecture, process, function, technology, or asset).
Asset	Anything that is valued by the organization.
Exposure / Impact	Negative consequences to an asset if the risk is realized (e.g., loss of life, reputational damage, downtime, etc.).
Countermeasures and Safeguards	Controls implemented to reduce threat agents, threats, and vulnerabilities and reduce the negative impact of a risk being realized.
Residual Risk	The risk that remains after countermeasures and safeguards (controls) are implemented.

Risk Treatment Strategies

Four Risk Responses:

1. Risk Avoidance (Eliminate):
    1. Don't engage in risky activity

2. Complete risk elimination, but may limit business opportunities
3. Example: Not accepting credit cards avoids PCI-DSS but limits payment options

2. Risk Mitigation (Reduce):

1. Implement controls to reduce the likelihood or impact
2. Preventive controls (reduce probability): firewalls, MFA, training
3. Detective/Corrective controls (reduce impact): IDS, backups, incident response
4. Example: MFA reduces account compromise likelihood

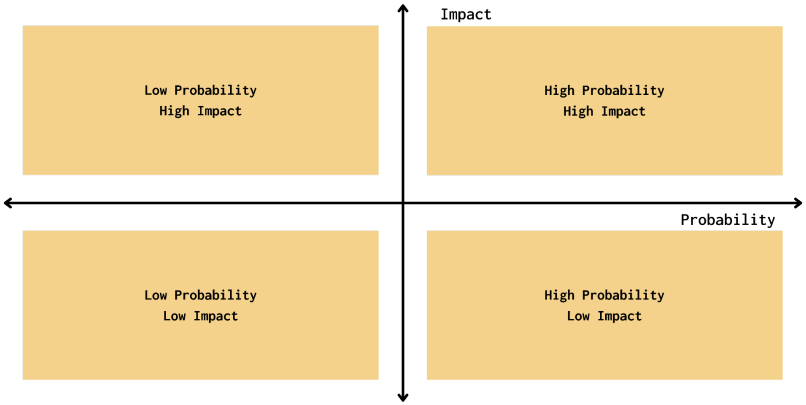
3. Risk Acceptance (Accept):

1. Acknowledge risk, take no action
2. Appropriate for low-impact, low-probability risks
3. Must be documented, management-approved decision
4. Regular review as threat landscape changes
5. Example: Advanced persistent threats for small businesses

4. Risk Transference (Share):

1. Shift financial impact to a third party
2. Cyber insurance, contractual indemnification, SLAs
3. Doesn't eliminate organisational responsibility
4. Example: Cyber insurance for breach costs

Risk Prioritisation Matrix:



Impact/Likelihood	High Likelihood	Low Likelihood
High Impact	Priority 1: Immediate mitigation	Priority 2: Prepare/ensure
Low Impact	Priority 3: Efficient controls	Priority 4: Accept/minimal

Exam Tip: Mitigation reduces risk; Avoidance eliminates it. Spending millions to protect thousands rarely makes business sense.

Threat Intelligence Integration

Three Intelligence Levels:

Strategic Intelligence (Executive):

1. Geopolitical trends, nation-state activities
2. Industry-wide attack patterns
3. Long-term threat evolution

4. Example: APT groups targeting the South Asian financial sector

Tactical Intelligence (Management):

1. Threat actor TTPs (Tactics, Techniques, Procedures), often tracked on MITRE framework
2. Campaign details, attack methodologies
3. Indicator patterns
4. Example: Banking trojans using Indian language phishing

Operational Intelligence (Technical):

1. IOCs (Indicators of Compromise): IPs, domains, file hashes
2. Vulnerability information, exploit availability
3. Real-time threat feeds
4. Example: Malicious IPs attacking payment gateways now

Sources:

1. Commercial: Recorded Future, ThreatConnect, vendor feeds
2. Government: CERT-In advisories, ISACs (industry-specific)
3. OSINT: Security blogs, dark web monitoring (verify credibility)

Indian Context:

1. CERT-In provides national cybersecurity threat advisories
2. Financial sector ISACs share threat intelligence

Exam Tip: Intelligence drives risk assessment, informs control selection, feeds incident response planning

(ISC)² Code of Ethics (PAPA)

(ISC)² Code of Professional Ethics	**(ISC)² Code of Ethics Canons:** 1. Protect society, the common good, necessary public trust and confidence, and the infrastructure. 2. Act honorably, honestly, justly, responsibly, and legally. 3. Provide diligent and competent service to principals. 4. Advance and protect the profession.

Four Canons (Priority Order):

1. Protect society, the common good, public trust, and infrastructure

    1. Public interest above all (including the employer)
    2. Critical for infrastructure (power, transportation, digital identity)

2. Act honourably, honestly, justly, responsibly, and legally

    1. Follow laws AND maintain high ethics
    2. Report breaches even if it reflects poorly on the organisation
    3. Resist pressure for inadequate security

3. Provide diligent and competent service to principals

    1. Maintain professional competence (continuous learning)
    2. Accurately represent capabilities/limitations
    3. Avoid conflicts of interest
    4. Balance with higher-priority canons

4. Advance and protect the profession

    1. Mentor juniors, contribute knowledge
    2. Report Code violations

3. Improve the profession's reputation

Exam Tip: Remember "PAPA" for priority. Canon conflicts resolve in order: Society > Honour> Principals > Profession

Professional Development

Emerging Technologies:

1. Cloud Security: Multi-cloud, containers, serverless, shared responsibility models
2. AI/ML Security: Adversarial attacks, algorithmic bias, model integrity
3. Quantum Computing: Post-quantum cryptography, cryptographic agility planning

CISSP Requirements:

1. 120 CPE credits over 3 years (40 Group A minimum)
2. 5 years experience (or 4 years + degree)

Career Progression Skills:

Junior → Mid Level (Technical Focus):

1. Deep tool expertise, architectures, and incident response
2. CISSP domains: 3, 4, 6, 8

Mid → Senior Level (Management Integration):

1. Business process understanding, risk assessment
2. Project management, vendor management
3. CISSP sweet spot: technical + management balance

Senior → Executive Level (Strategic Leadership):

1. Executive communication, board presentations
2. Business strategy, organisational change management
3. CISSP domains: 1, 2, 5, 7

Indian Context:

1. Bank CISOs often have MBAs, report to Risk Committees
2. IT companies require CISO candidates to have P&L experience

Exam Tip: CISSP tests management mindset, not just technical skills. Balance business needs with security requirements.

Intellectual Property Protection

Type	Protects	Disclosure Required
Trade Secret	Business information	No
Patent	Functional innovations; novel ideas/inventions	Yes
Copyright	Expression of an idea embodied in a fixed medium (books, movies, songs, etc.)	Yes
Trademark	Color, sound, symbol, etc. used to distinguish one product/company from another	Yes

Four IP Types:

1. Trademarks:

1. Protect brand names, logos, slogans
2. India: Trade Marks Act, 1999
3. Process: Search → File → Register → Monitor → Enforce
4. Example: PayTM searched 45 countries before launch

2. Patents:

1. Protect inventions, innovative processes

2. India: Patents Act, 1970 - software needs technical effect
3. Example: IT services companies hold hundreds of AI/automation patents

3. Copyright:

1. Protect original works (software, content, training materials)
2. India: Copyright Act, 1957 - software = literary works
3. Automatic protection, registration strengthens enforcement
4. Example: EdTech companies protect video lessons, interactive content

4. Trade Secrets:

1. Protect confidential business information
2. No registration, requires: identification, documentation, access control, NDAs
3. Example: Algorithms, customer lists, pricing strategies

Indian Context:

1. IT Act 2000: Digital signatures are legally valid
2. DPDP Act 2023: India's GDPR equivalent
3. Madrid Protocol: International trademark filing

Exam Tip: Copyright is automatic; patents require filing. Trade secrets are protected through controls, not registration.

Supply Chain Risk Management

Key Points:

1. Third-party vendors extend the attack surface
2. SolarWinds/Log4j demonstrate supply chain compromise risks

Vendor Assessment:

1. Pre-contract: ISO 27001, SOC 2 reviews, security audits

2. Depth matches vendor's data access and criticality
3. Continuous monitoring throughout the relationship

Service Requirements Agreement (SRA):

1. Customer's security expectations for vendors
2. Technical controls (encryption standards)
3. Operational requirements (incident response times)
4. Compliance certifications

Service Level Agreement (SLA):

1. Vendor's commitments to service levels
2. Vulnerability remediation times, incident notification
3. Availability targets, penalties for non-compliance
4. Note: Penalties compensate but don't undo breach damage

Software Supply Chain:

1. SBOM (Software Bill of Materials): component transparency
2. Code signing: verify software integrity/authenticity
3. Third-party components: track usage, monitor vulnerabilities
4. Example: Log4Shell affected countless apps via the logging library

Indian Context:

1. Payment banks face significant penalties for KYC violations
2. IT services companies invest heavily in vendor GDPR compliance

Exam Tip: Financial penalties don't prevent security breaches - focus on preventive controls, not just contractual penalties.

Indian Regulatory Landscape

Key Regulations:

IT Act 2000:

1. Foundation of Cyber Law in India
2. Digital signatures, electronic records legal validity
3. Cybercrime definitions and penalties

DPDP Act 2023:

1. India's data protection law (GDPR equivalent)
2. Data fiduciary responsibilities, consent requirements
3. Cross-border transfer provisions

CERT-In Mandate (2022):

1. 6-hour breach reporting (from discovery)
2. 180-day log retention minimum
3. Covers 20 types of security incidents
4. Example: Telecom companies created 24/7 incident response teams

Sector-Specific:

1. RBI (Banking): IT Strategy Committees, cybersecurity frameworks
2. SEBI (Securities): Listed company compliance requirements
3. IRDAI (Insurance): Insurance sector security mandates
4. TRAI (Telecom): DOT guidelines, telecom regulations
5. HIPAA: Affects Indian companies processing US healthcare data
6. ECPA: US electronic communication privacy (cloud providers)

Global Impact:

1. GDPR: Affects Indian companies with EU data (72-hour breach notification, up to 4% global revenue fines)
2. PCI DSS: Payment card industry security (Level 1 for high-volume processors)
3. SOX: Financial reporting controls for US-listed companies
4. Basel III: Banking capital and risk management

Compliance Challenges:

1. Multiple jurisdictions with varying requirements

2. Understanding applicable regulations
3. Demonstrating compliance through audits
4. Example: Payment gateways manage PCI DSS Level 1 for trillions processed

GRC Platforms:

1. Track compliance across 50+ regulations
2. Map requirements to controls, identify gaps
3. Automated evidence collection for audits
4. Example: Multinational banks use GRC for global compliance

Exam Tip: Compliance is a journey, not a destination. Focus on continuous monitoring, not one-time certification.

Continuous Risk Monitoring

Key Risk Indicators (KRIs):

1. Early warning of increasing risk levels
2. Leading indicators (predict future problems)
3. Examples: Unpatched critical vulnerabilities, failed auth attempts, security incidents
4. Threshold values trigger escalation

Key Performance Indicators (KPIs):

1. Measure security control effectiveness
2. Examples: Mean time to patch, % systems hardened, training completion rates
3. Identify areas needing improvement

Risk Register:

1. Document identified risks, analysis, treatment, and status
2. Living document - regularly updated
3. Supports management decision-making
4. Provides a comprehensive risk landscape view

Exam Tip: KRIs predict problems (leading), KPIs confirm effectiveness (lagging). Both are needed for complete risk visibility.

Domain 1 Exam Strategy

Domain Weight:

1. 15% of CISSP exam
2. ~23 questions (out of ~150)

High-Priority Topics:

1. Risk management formulas (SLE, ARO, ALE, cost-benefit)
2. Access control models (DAC, MAC, RBAC, ABAC)
3. CIA Triad extended (5 pillars)
4. (ISC)² Code of Ethics (PAPA priority order)
5. Policy hierarchy (Policy > Standards > Procedures > Guidelines)
6. Risk treatment strategies (Mitigate, Transfer, Accept, Avoid)

Exam Question Patterns:

"First Step" Questions:

1. Answer: Usually, policy development or risk assessment
2. Think strategic before tactical

Authority Questions:

1. Answer: Board/CEO approval required
2. Top-down governance

Cost-Benefit Scenarios:

1. Calculate: Annual safeguard cost vs ALE reduction
2. If cost > benefit → Accept risk

Ethics Scenarios:

1. Apply PAPA priority: Society > Honor > Principals > Profession
2. Public safety is always first

Access Control Questions:

1. Keywords: "owner decides" = DAC, "labels" = MAC, "role" = RBAC, "context" = ABAC

Common Traps:

1. Choosing a technical fix over policy/governance
2. Ignoring human safety for asset protection
3. Bottom-up security instead of top-down
4. Eliminating risk (impossible) vs reducing to an acceptable level

Exam Tip: When stuck between two answers:

1) Choose policy over procedure

2) Choose safety over assets

3) Choose strategic over tactical

4) Choose comprehensive over limited scope

Quick Formula Reference Card

Risk Calculations:

SLE = AV × EF

ARO = Expected occurrences per year

ALE = SLE × ARO

Total Risk = Threats × Vulnerabilities × Asset Value

Residual Risk = Total Risk - Control Effectiveness

Control Justified if: Annual Cost < (ALE_before - ALE_after)

Availability:

Five nines (99.999%) = 5.26 minutes downtime/year

Calculate: 365 days × 24 hrs × 60 min × (100% - uptime%)

Exam Tip: Memorise these formulas - they appear in multiple domains and scenario questions.

Critical Concepts Summary

Think Like a CEO:

1. Strategic over tactical decisions
2. Business enablement over pure protection
3. Policy before procedure
4. Safety before assets

CIA+A+NR:

1. Confidentiality, Integrity, Availability (foundation)
2. Authenticity, Non-repudiation (modern additions)
3. DAD Triad = failures (Disclosure, Alteration, Destruction)

Access Control:

1. DAC = owner decides (flexible, less secure)
2. MAC = system enforces (rigid, high security)
3. RBAC = role-based (scalable, enterprise standard)
4. ABAC = attribute-based (dynamic, complex)

Governance:

1. Board → CEO → CISO → Business Units → All Personnel
2. Policy → Standards → Procedures → Guidelines
3. Top-down, not bottom-up

Risk Management:

1. Four responses: Mitigate, Transfer, Accept, Avoid
2. Quantitative: SLE, ARO, ALE formulas
3. Residual risk always remains
4. Cost-benefit drives decisions

Ethics:

1. PAPA: Protect society > Act honorably > Provide service > Advance profession
2. Public interest above all

Indian Context:

1. CERT-In: 6-hour reporting, 180-day logs
2. DPDP Act 2023: India's data protection law
3. Sector regulators: RBI, SEBI, IRDAI, TRAI
4. National ID: Billions enrolled, biometric authentication

Exam Strategy:

1. 15% of the exam (~23 questions)
2. Master formulas, access models, and ethics priority
3. Think governance and management, not just technical
4. "First step" = policy; "Authority" = Board/CEO

Final Exam Reminders

1. CISSP tests management decisions, not technical implementation
2. Human safety > data protection - always
3. Policy > procedure - strategic over tactical
4. Top-down governance - Board/CEO drives security
5. Risk cannot be eliminated - only reduced to acceptable levels
6. Controls must be cost-justified - cost ≤ benefit
7. Public interest first - (ISC)² Code Canon 1
8. Physical access defeats logical controls - consider physical security
9. Defence in depth - multiple layers, no single point of failure

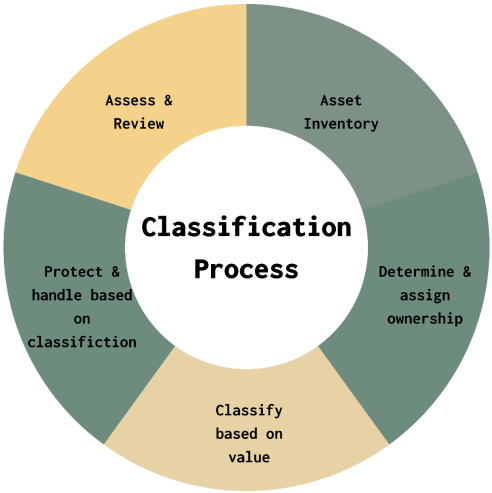
10. Residual risk remains - even with perfect controls

Pass Strategy:

1. Read the question carefully (what is being asked?)
2. Eliminate obviously wrong answers.
3. Apply the CISSP mindset (CEO, not technician)
4. Choose strategic over tactical
5. Choose comprehensive over limited
6. Trust your preparation

Domain 2: Asset Security

Overview

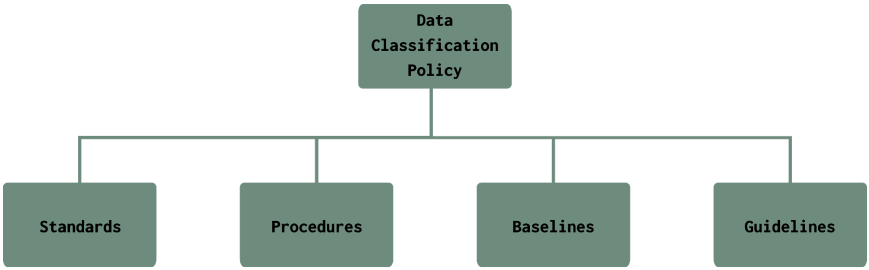


Key Points:

- 10% of the CISSP exam (13-15 questions)
- Focus: Identifying, classifying, and protecting information assets throughout the lifecycle
- Critical regulatory compliance: DPDP Act 2023, RBI guidelines, SEBI requirements, GDPR, EU AI.
- Data is a valuable asset requiring protection from creation to destruction
- Indian Context:
- DPDP Act 2023: India's comprehensive data protection law
- IT Act 2000 Sections 43, 66: Digital data security and penalties
- RBI Cybersecurity Framework: Financial sector mandates
- CERT-In directives: Logging and incident reporting requirements

Exam Tip: Remember "Asset Security = Data Lifecycle + Classification + Controls." Questions test strategic understanding, not technical implementation details.

Data Classification Systems



Government Classification

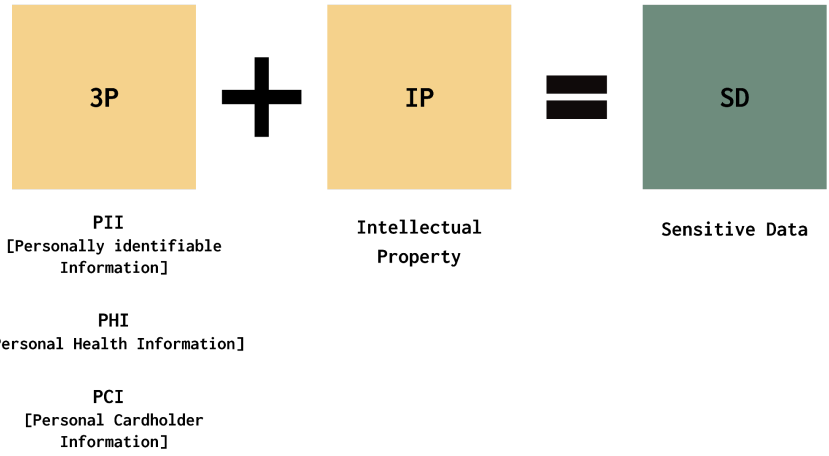
Key Points:

- Top Secret: Exceptionally grave national security damage (e.g., INS Arihant blueprints, RAW operative lists)
- Secret: Serious damage possible (e.g., LAC Army movement plans, IB surveillance operations)
- Confidential: Would cause damage but is manageable (e.g., diplomatic communications, defence procurement)
- Unclassified: No national security implications, but may need privacy protection
- Special Categories:
- FOUO (For Official Use Only): Sensitive but unclassified

- SBU (Sensitive But Unclassified): Needs protection without classification overhead

Exam Tip: Government classification carries LEGAL consequences under the Official Secrets Act. Unauthorised disclosure = prosecution and imprisonment.

Private Sector Classification



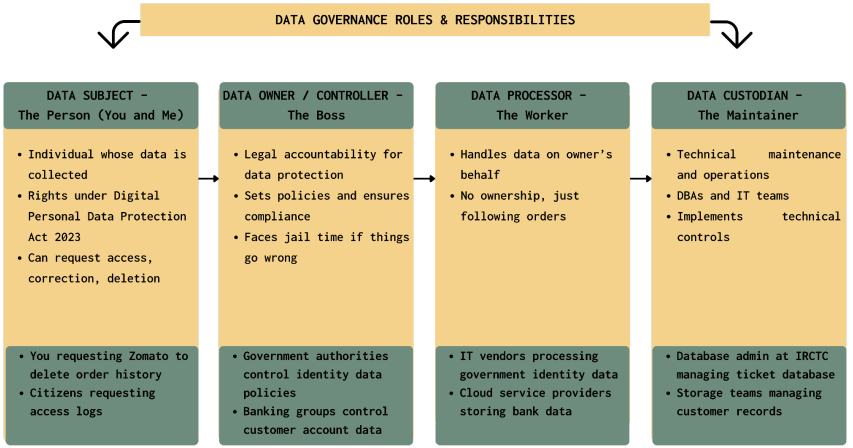
Key Points:

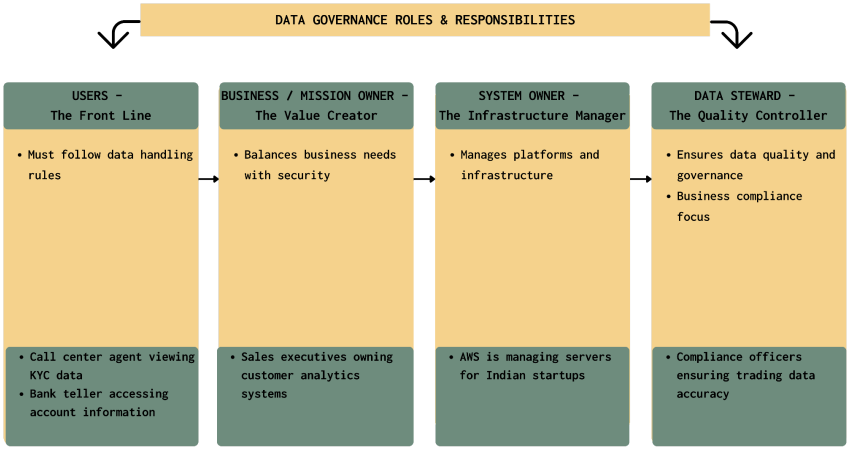
Data Classification	Minimum Method	Recommended Method	Verification Required
Public	Simple Deletion	Overwriting (1 pass)	None
Internal Use	Overwriting (1 pass)	Overwriting (3 passes)	Witness / Log
Confidential	Overwriting (3 passes)	Physical Shredding	Certificate
Secret / Top Secret	Physical Shredding	Incineration	Multiple Witnesses
Special Access	Incineration	Chemical Dissolution	Government Oversight

- Confidential/Proprietary: Trade secrets, M&A details, source code, strategic plans
- Private: PII, PHI, financial records, identity numbers (DPDP Act protected)
- Sensitive: System architectures, network diagrams, internal procedures (often subdivided: Sensitive-HR, Sensitive-Finance)
- Public: Marketing materials, press releases, annual reports (still needs integrity/availability protection)

Exam Tip: Classification vs Categorisation - Classification = creating the system/blueprint. Categorisation = sorting data into categories. CISSP tests this distinction!

Data Roles and Responsibilities





Key Points:

- Data Subject: Individual whose data is collected (rights under DPDP Act: access, correction, deletion)
- Data Owner/Controller: Legal accountability, sets policies, faces jail time if failures occur
- Data Processor: Handles data on the owner's behalf, no ownership (e.g., cloud providers, IT vendors)

- Data Custodian: Technical maintenance (DBAs, IT teams), implements technical controls
- Data Steward: Ensures data quality and governance, business compliance focus
- System Owner: Manages platforms and infrastructure
- Business/Mission Owner: Balances business needs with security
- Users: Must follow data handling rules

Indian Context:

- DPDP Act 2023 defines Data Fiduciary (Controller) and Data Processor roles
- Clear liability: Data Fiduciary is responsible for compliance violations
- Example: Aadhaar - UIDAI = Controller, enrollment centers = Processors

Exam Tip: Owner = ACCOUNTABILITY (owner decides the level of controls to be implemented). Custodian = IMPLEMENTATION (implements those controls). Processor = NO OWNERSHIP. Questions test who bears legal responsibility.

Data Labeling and Marking

Labeling	Marking
System-readable	Human-readable
Association of security attributes with subjects and objects represented by internal data structures	Association of security attributes with objects in a human-readable form
Enables system-based enforcement	Enables process-based enforcement

Critical Distinction for Exam: Labeling (For Machines):

- System-readable metadata
- Enables automated controls and enforcement
- Triggers automatic protection (encryption, DLP, access controls)
- Example: Aadhaar record labelled with sensitivity markers triggers auto-encryption

Marking (For Humans):

- Human-readable indicators (stamps, watermarks, headers/footers)
- Visual cues for proper handling
- Example: RBI documents stamped "CONFIDENTIAL" in red ink

Implementation:

- Digital documents: Embedded metadata + visible headers
- Physical documents: Clear markings on every page

- Removable media: Classification labels on USB/CD
- Email systems: Auto-append tags based on content

Exam Tip: Label = automated security. Mark = human awareness. The board needs defence-in-depth.

Data States and Protection

Data at REST	Data in TRANSIT	Data in USE
Inactive data that is stored (resting) on media: hard disks, tapes, databases, spreadsheets, etc.	Data flowing across a network, such as the internet.	Data being used in computational activities.
Protection: • Encryption • Access Control • Backup and Restoration	Protection: • Access Control • Network Encryption • End-to-end • Link • Onion	Protection: • Homomorphic Encryption • RBAC • DRP • DLP

Data at Rest

Key Points:

- Stored in databases, file systems, archives
- Protection: AES-256 encryption (256-bit KEY size, 128-bit BLOCK size always)
- Access control lists, physical security
- Example: Banks store customer accounts with AES-256-GCM encryption

AES Modes - Critical for CISSP:

- ECB (Electronic Codebook): INSECURE - DO NOT USE. Identical plaintext = identical ciphertext (reveals patterns)
- CBC (Cypher Block Chaining): Common, but requires HMAC for authentication, vulnerable to padding oracle attacks
- GCM (Galois/Counter Mode): RECOMMENDED - provides encryption AND authentication (AEAD), industry standard for TLS 1.3, IPsec
- CTR (Counter Mode): Parallelizable but needs HMAC (or use GCM)

Exam Tip: AES-256 = 256-bit KEY, NOT block size. Block size = always 128 bits. GCM mode is the modern best practice. ECB is always the wrong answer.

Data in Transit

Key Points:

- Moving across networks between systems
- Protection: TLS 1.2 , TLS 1.3 HTTPS, VPNs, IPsec
- Multiple encryption layers during movement
- Example: Every UPI transaction (1000+ crore monthly) uses multiple encryption layers

Data in Use

Key Points:

- Exists in active memory during processing
- Traditionally vulnerable when decrypted for processing

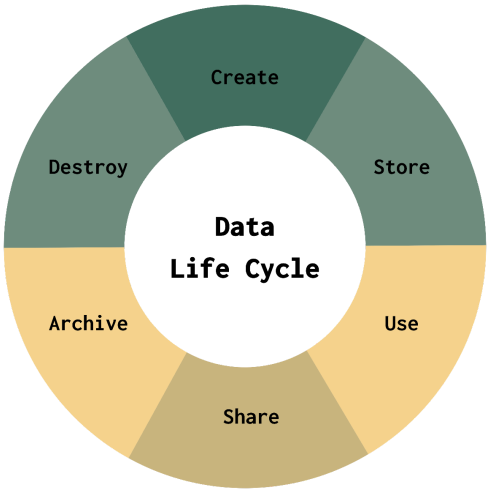
- Modern solutions: Homomorphic encryption, secure enclaves, memory encryption

Advanced Protection Technologies:

- Homomorphic Encryption: Compute on encrypted data without decryption (100-1000x slower but preserves privacy)
- Intel SGX: Encrypted memory regions (enclaves) isolated from OS/hypervisor
- AMD SEV: VM memory encryption with dedicated AES engine
- ARM TrustZone: Secure world vs normal world separation (used for UPI PIN processing in India)
- TME/MKTME: Total memory encryption protecting against cold boot attacks

Exam Tip: Data in use is the MOST vulnerable state.

Data Lifecycle Phases



Key Points:

Create	Generation of new digital content, or the alteration/updating/modifying of existing content
Store	Committing digital data to some sort of storage repository, which typically occurs nearly simultaneously with creation
Use	Data viewed, processed, or otherwise used in some sort of activity, not including modification
Share	Information made accessible to others, such as company users, customers, and partners
Archive	Data leaves active use and enters long-term storage
Destroy	Data is permanently destroyed using physical or digital means (e.g., crypto shredding)

- Creation/Acquisition: Classify immediately, enforce at creation point, attach proper metadata
- Storage/Maintenance: Encryption based on sensitivity, backup and recovery, and maintain classification accuracy
- Use/Processing: Maintain security while enabling access, enforce least privilege, monitor and log all usage
- Sharing/Dissemination: DRM for sensitive content, audit trails, and enforcing distribution restrictions
- Archival: Long-term retention with minimal active system risks, maintain decryption capabilities for the retention period along with Integrity and availability
- Destruction: Complete and verifiable elimination, deletion ≠ , destruction (CRITICAL for exam!)

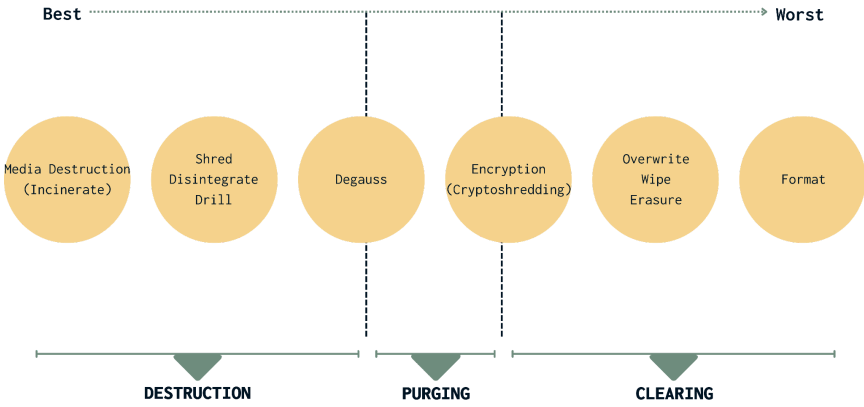
Indian Context:

- RBI: Banks store transaction data for 10 years, encrypted
- DOT: Telecom call records 2 years
- GST: Invoice data 6 years with encryption

- DPDP Act: Right to erasure requires defensible destruction

Exam Tip: DELETION removes file pointers - data remains recoverable. DESTRUCTION makes data unrecoverable. Know the difference!

Data Sanitization Methods (NIST SP 800-88)



NIST SP 800-88 Rev. 1 - Authoritative Standard

Clear:

- Logical techniques to sanitise user-addressable storage
- One pass overwriting is sufficient for modern HDDs
- Protects against simple non-invasive recovery

- Use case: Media reuse within the same organisation

Purge:

- Renders data recovery infeasible using state-of-the-art lab techniques
- Methods: Cryptographic erase (destroy keys), block erase (SSDs), degaussing (magnetic media)
- Use case: Media leaving organisational control

Destroy:

- Physical destruction rendering media unusable
- Methods: Disintegration, pulverisation, melting, incineration, shredding (2mm particle size per NSA)
- Highest assurance, completely unrecoverable

DoD 5220.22-M (Deprecated):

- 3-pass overwrite (zeros, ones, random)
- Officially withdrawn in 2014, superseded by NIST SP 800-88
- Still referenced in older tools and some compliance requirements

Key Methods by Media Type:

Method	HDDs	SSDs	Tapes	Optical
Overwriting	Effective	Unreliable	No	No

Degaussing	Effective	Useless	Effective	Useless
Physical Destruction	Effective	Effective	Effective	Effective

Certificate of Destruction Requirements:

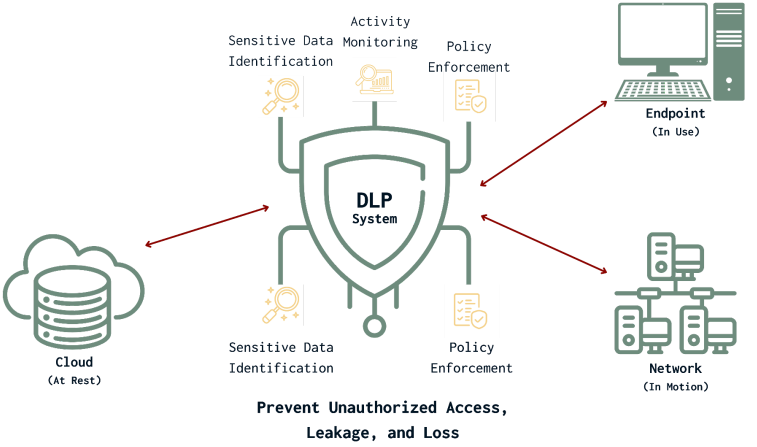
- Date and time of destruction
- Description of media (serial numbers, asset tags)
- Method used (Clear/Purge/Destroy per NIST)
- Verification method and personnel involved
- Third-party vendor certification

Indian Context:

- IT Act Section 43: Reasonable security for data disposal
- CERT-In: Secure disposal of digital media
- RBI: Banks maintain destruction certificates
- DPDP Act 2023: Data principals can request deletion with proof

Exam Tip: SSDs must be physically destroyed. Degaussing only works on MAGNETIC media. Always get a certificate of destruction for an audit trail.

Data Loss Prevention (DLP)



Network DLP (Perimeter Defence)

Key Points:

- Monitors data leaving organisational network boundaries
- Deep packet inspection (DPI) for content scanning
- Pattern recognition: regex, machine learning, statistical analysis
- Challenge: Cannot inspect encrypted traffic without decryption

Detection Techniques:

- Structured data: Credit cards, SSNs, bank account formats
- Unstructured data: Document fingerprinting, keyword density
- Contextual analysis: Sender-recipient relationships
- File type analysis: Document properties, metadata

Exam Tip: Network DLP = first line of defence, but limited by encryption. Cannot inspect HTTPS without SSL/TLS decryption.

Cloud DLP (Sky Police)

Key Points:

- API-based monitoring of cloud services (Office 365, Google Workspace, Salesforce)
- Proxy-based or API-based, or agent-based deployment
- Multi-tenant considerations and geographic distribution
- Shared responsibility model: delineate cloud provider vs customer duties

Endpoint DLP (Last Guardian)

Key Points:

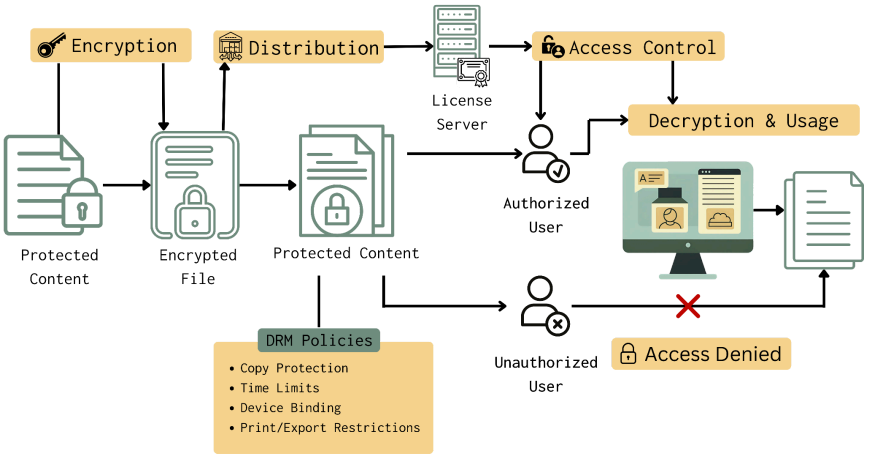
- An agent on devices monitors file operations, USB ports, screen captures, and printing
- Works offline when the device is disconnected
- Kernel-level integration for comprehensive monitoring
- BYOD considerations for personal device privacy

DLP Career Applications:

- Security Analyst: Configure and tune DLP rules
- Network Security: Integrate DLP with infrastructure
- Compliance Officer: Ensure DLP meets regulatory requirements
- CISO: Balance business enablement with data protection

Exam Tip: Layered DLP = defence in depth. Network → Storage → Endpoint. DLP effectiveness depends on proper data classification first.

Digital Rights Management (DRM)



Key Points:

- Controls how content is used after distribution
- Licensing agreements define a legal framework
- Encryption ensures only valid keys can decrypt
- Digital watermarking embeds user/device IDs
- Copy/view restrictions limit downloads, screenshots, and device transfers

DRM vs Encryption:

- DRM = persistent control over content usage
- Encryption = prevents unauthorised access
- DRM typically includes encryption + usage policy enforcement

Legal Framework:

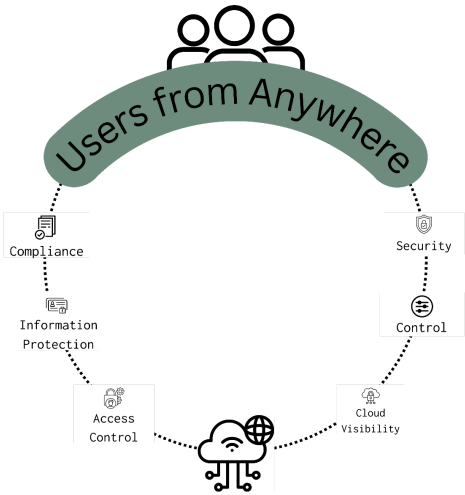
- DMCA (US): Breaking DRM is a criminal offence
- Copyright Act 1957 (India): Digital copyright protection
- IT Act 2000: Added digital provisions
- Breaking DRM = jail time in India

Examples:

- Streaming platforms prevent screenshots via DRM
- E-books can't be copied between devices
- MS Office disables features if the license expires

Exam Tip: DRM = content control AFTER delivery. Encryption = access prevention BEFORE delivery. DRM needs online authentication.

Cloud Access Security Broker (CASB)



Four Pillars of CASB

1. Visibility (Shadow IT Discovery):

- Discovers ALL cloud apps in use (80% without IT approval)
- Network traffic analysis, DNS monitoring
- Cloud app risk assessment
- Example: Infosys discovered 400+ cloud services across operations

2. Data Security (DLP Extension):

- Extends on-premises DLP to the cloud
- Real-time blocking of uploads/downloads/sharing
- API integration with major cloud platforms
- Example: TCS blocks customer data upload to personal cloud storage

3. Threat Protection (Behavioural Analytics):

- User behaviour analytics (UBA) for anomaly detection
- Impossible travel detection (login from India and the USA simultaneously)
- Credential compromise identification
- Insider threat detection
- Example: Wipro CASB caught an employee downloading client data before resignation

4. Compliance (Regulatory Framework):

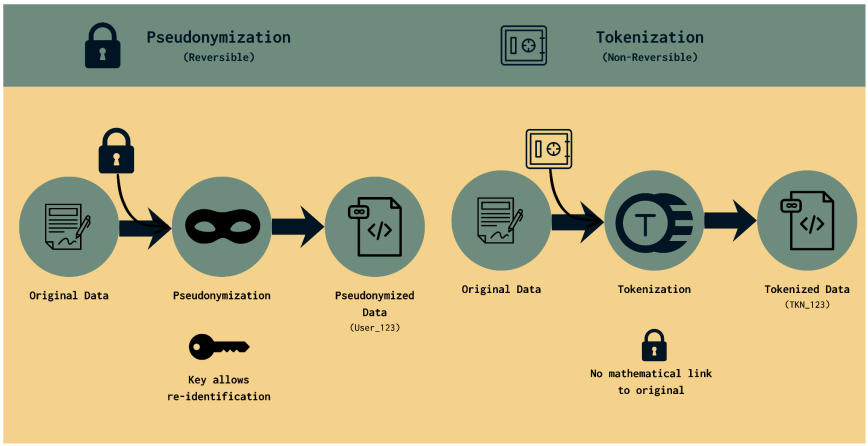
- Data sovereignty enforcement (data residency in India)
- Cross-border transfer monitoring
- RBI cybersecurity guidelines compliance
- Audit trail generation
- Example: TCS Bank ensures customer data never leaves India

CASB Deployment Models:

- Proxy-based: Routes cloud traffic through inspection points
- API-based: Monitors via native cloud service APIs
- Agent-based: Software on cloud workloads
- Hybrid: Combination for comprehensive coverage

Exam Tip: CASB = cloud DLP + visibility + threat detection + compliance. Addresses the shadow IT problem. Key for multi-cloud security.

Pseudonymization vs Tokenisation



Pseudonymization:

- Replaces real identity with a consistent fake ID
- Maintains secure mapping for reversal
- Designed to be REVERSIBLE with the right key

- Example: Health insurance uses "P12345" instead of "Raj Kumar"

Tokenization:

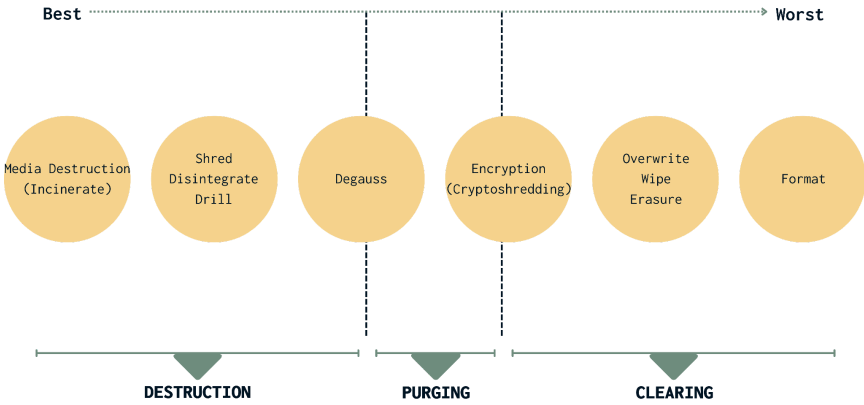
- Replaces data with completely random tokens
- Original stored in ultra-secure vault
- NO mathematical relationship - cannot reverse without the vault
- Example: UPI replaces the card number with a random token

Key Difference for Exam:

- Pseudonym = fake name but same person (like film star stage names - might guess relationship)
- Token = random replacement with no connection (impossible to guess)
- A pseudonym can be analysed, token cannot

Exam Tip: Tokenisation requires a secure vault for mapping. Pseudonymization allows data analysis while protecting identity. Both are reversible, but tokenisation is stronger.

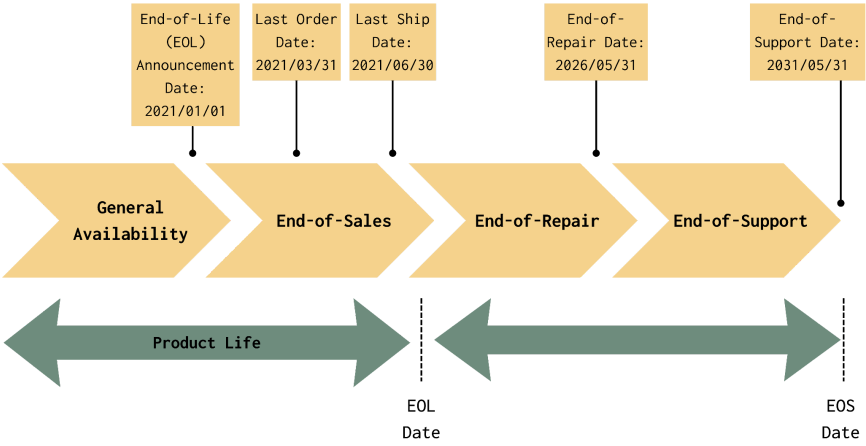
Data Remanence and Destruction



Data Remanence:

- Data residue after deletion
- Standard deletion = hiding data, not removing
- Formatting = cleaning the room, but not under the bed
- SSDs: Wear levelling spreads data everywhere
- RAM: Retains data briefly after power off (cold boot attack)

End-of-Life Stages:



- GA (General Availability): Product is being actively sold and fully supported.
- End-of-Sales: No new sales/orders; existing customers can still get support, repairs, and updates.
- EOL (End-of-Life announcement): Vendor announces phase-out and sets last-order / last-ship dates, but support continues for a defined period.
- End-of-Repair: Vendor stops hardware repair/service; software support and updates may continue.
- EOS (End-of-Support): No more support, patches, or updates; using it is now a security/operational risk.
- Post-EOS / Retirement: System should be decommissioned, data sanitised, and hardware disposed of or recycled securely.

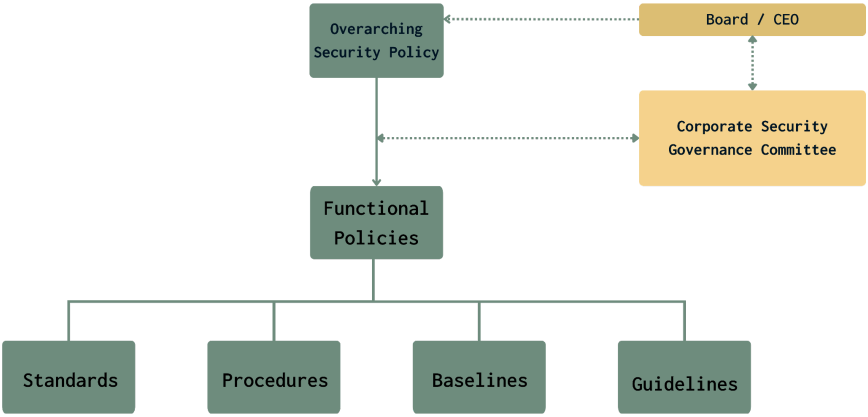
Compensating Controls for Legacy:

- Network isolation (air-gapping)
- Enhanced monitoring
- Virtual patching through IPS
- Accelerated replacement planning

Example: PSU banks running Windows XP ATMs in 2024 - can't patch, so isolate networks

Exam Tip: Deletion ≠ Destruction. Remanence = data traces remain after deletion. Legacy systems need compensating controls.

Policies, Standards, Procedures



Policy (What must be done):

- Strategic level, mandatory
- Sets organisational commitment
- Example: "All customer PAN data must be encrypted"

Standard (Specific requirements):

- Mandatory technical/procedural requirements
- Example: "Use AES-256 encryption for all data transfers"

Baseline (Minimum configuration):

- Default security settings
- Example: "Windows hardening checklist for all workstations"

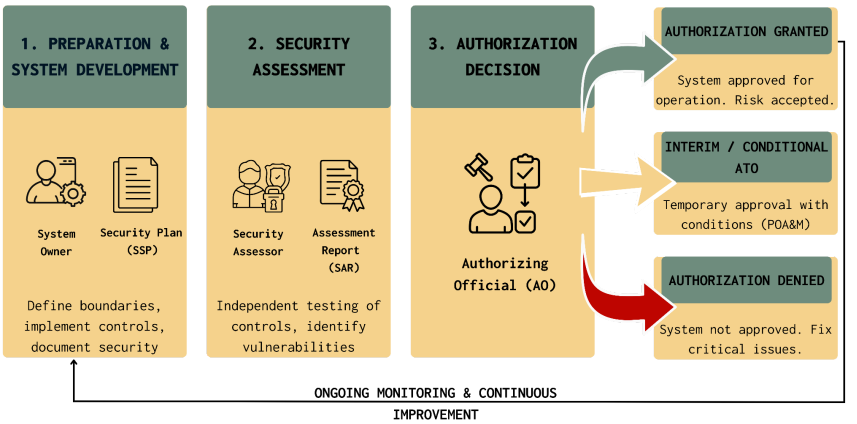
Guideline (Recommendations):

- Optional best practices
- Example: "Suggested patch deployment windows"

Procedure (Step-by-step):

- Detailed implementation instructions
- Example: "How to configure BitLocker for full-disk encryption"

Authorisation to Operate (ATO):



- Formal risk acceptance by designated authorities
- Critical for government/defence contractors

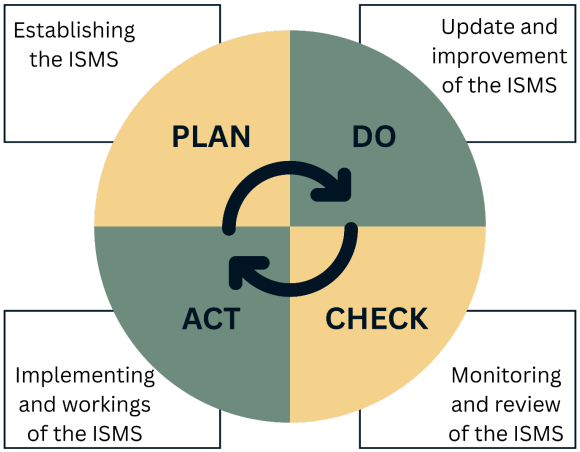
- Four outcomes: ATO, Common Control Authorisation, Authorisation to Use, Denial

Indian Context:

- RBI guidelines require SOPs for failed ATM transactions
- CERT-In directives mandate incident reporting procedures
- The DPDP Act requires data breach notification procedures
- Exam Tip:
- Policies = mandatory strategies.
- Standards = mandatory technical.
- Guidelines = optional recommendations.
- Procedures = implementation steps.

Framework Selection and Application

ISO 27001 - ISMS Foundation



Key Points:

- Requirements standard (mandatory for certification)
- PDCA cycle: Plan → Do → Check → Act
- Risk-based control selection
- Statement of Applicability (SoA) documents control choices

Theme	Count	Key Areas
Organizational	37	Policies, access management, threat intelligence, supplier relationships
People	8	Training, screening, remote working, NDAs
Physical	14	Secure areas, clear desk, equipment maintenance
Technological	34	Encryption, logging, network security, secure coding

ISO 27001 vs 27002:

- 27001 = "What" must be done (requirements, certifiable)
- 27002 = "How" to implement (guidance, not certifiable)

Indian Context:

- Major IT services companies (TCS, Infosys, Wipro) are ISO 27001 certified
- Client contracts often require certification
- RBI references ISO 27001 for banks

Exam Tip: ISO 27001 = certifiable requirements. ISO 27002 = implementation guidance. PDCA cycle = continuous improvement.

NIST Cybersecurity Framework

Key Points:

- Five functions: Identify, Protect, Detect, Respond, Recover
    - Note: Nist CSF 2.0 - includes 'govern'
- Risk-based approach to cybersecurity
- NIST SP 800-53: Comprehensive control catalogue
- Excellent for data Labeling and marking guidance

Indian Adoption:

- Public sector units reference NIST for cloud security
- MeitY empanelment requirements align with NIST
- Increasingly adopted for supply chain security

PCI DSS - Payment Card Security

Key Points:

- 12 requirements under 6 control objectives
- Mandatory for organisations handling payment card data
- Audit log retention: Minimum 1 year, 3 months immediately available
- Four compliance levels based on transaction volume

Indian Context:

- All payment processors must maintain PCI DSS compliance
- RBI mandates PCI compliance for banks
- Often extended to other sensitive data types

COBIT - IT Governance

Key Points:

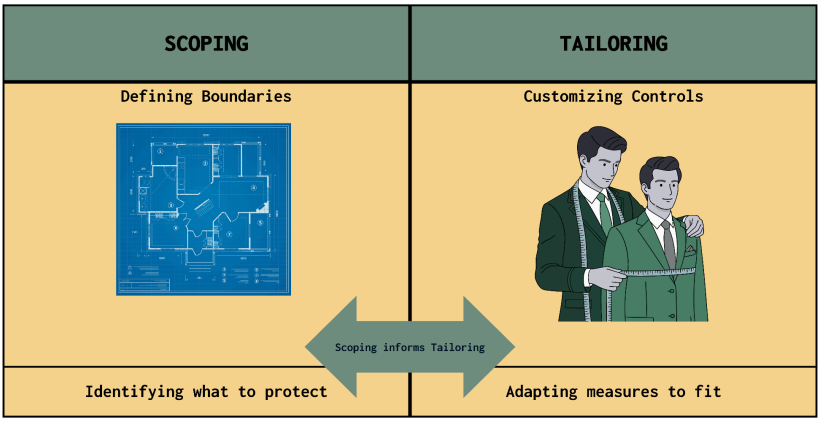
- 5 principles: Meet stakeholder needs, Cover enterprise end-to-end, Apply single integrated framework, Enable holistic approach, Separate governance from management
- Used by RBI and SEBI for IT audits
- Maturity model for capability assessment

Multi-Framework Strategy:

- Control alignment: Map common controls across frameworks
- Gap analysis: Identify unique requirements
- Unified reporting: Single dashboard for compliance
- Cost reduction: 40% savings through shared implementations

Exam Tip: Large organisations implement MULTIPLE frameworks. Focus on risk-based selection, business alignment, and control mapping efficiency.

Scoping and Tailoring



Scoping (What applies):

- Determines which controls apply to the organisation
- Based on technologies, data types, and boundaries
- Document exclusions with justification
- Example: Fintech without wireless can exclude wireless controls from the PCI scope

Tailoring (How to implement):

- Modifies HOW controls are implemented
- Adjusts to risk tolerance, resources, and local regulations
- Defines organisation-specific baselines
- Example: Bangalore startup simplifies NIST logging due to resource constraints

Documentation Requirements:

- Controls deemed out of scope with rationale

    - That includes justification, along with being reviewed and approved by the concerned authority

- Tailoring decisions and risk acceptance
- Compensating controls for gaps
- Essential for audit and regulatory examination

Common Scenarios in India:

- Exclude cloud controls for purely on-premises deployments
- Adjust password complexity for legacy systems
- Implement alternative controls when specified tech is unavailable
- Extend frameworks for local data protection requirements (DPDP Act)

Exam Tip: Scoping = "Does this apply to us?" Tailoring = "How do we implement this?" Both need clear documentation and risk acceptance along with management approval.

Digital Watermarking vs Encryption

Aspect	Digital Watermarking	Encryption
Primary Purpose	Attribution and tracking	Access prevention
Data Readability	Content remains readable	Content becomes unreadable
Protection Method	Invisible identification	Mathematical transformation
Key Management	Not required for basic operation	Critical for all operations
Performance Impact	Minimal processing overhead	Moderate to significant overhead
Removal Resistance	Designed to survive attacks	Complete protection or failure
Legal Evidence	Strong proof of ownership	Limited evidentiary value
Compliance Role	Attribution and audit trails	Data confidentiality requirements

Digital Watermarking (Attribution)

When to Use:

- Content tracking and leak investigation
- Copyright protection and proof of ownership
- Forensic evidence for legal proceedings
- Regulatory compliance for content provenance

Implementation Types:

- Robust: Survives intentional attacks and format conversions
- Fragile: Detects ANY modification (integrity verification)
- Semi-fragile: Survives acceptable modifications, detects malicious changes

Example: Bollywood films watermarked at production, distribution, and theatre levels to trace piracy sources

Encryption (Confidentiality)

When to Use:

- Data privacy and access prevention
- Regulatory compliance, frameworks, standard (GDPR, HIPAA, DPDP , ISO, PCI)
- Secure communications and storage
- Protection from breaches and device theft

Key Management Challenges:

- Secure key generation, distribution, storage
- Key rotation/replacement
- Recovery planning for lost keys

- Performance impact of encryption/decryption

Combined Strategy (Defence in Depth)

Use Both When:

- Multiple threat vectors (confidentiality AND attribution)
- High-value intellectual property
- Complex regulatory requirements
- Supply chain with third-party handling
- Need both evidence collection and content protection

Implementation:

- Apply watermarks during creation
- Encrypt for storage/transmission
- Decrypt for authorised users (preserving watermarks)
- Monitor watermarked content usage
- Investigate incidents using watermarks

Example: Digital news platforms watermark articles to track redistribution, then encrypt for transmission to subscribers

Indian Examples:

- Film Industry: 60% piracy reduction through production-stage watermarking + encryption
- Publishing: 75% reduction in textbook piracy via student-specific watermarks
- Government: 90% reduction in document forgery using citizen-specific watermarks

Exam Tip: Watermarking = "Who leaked this?" Encryption = "Who can access this?" Different purposes, often complementary.

Segregation of Duties (SoD)

Key Points:

- Divides critical functions among multiple people
- Prevents fraud and errors
- No single individual controls the entire critical process

- Split control / split knowledge: A secret/key is split so no one person has the whole thing.
- Dual control: Two or more people must act together to perform one critical operation.
- Least privilege: Each subject gets only the minimum access needed to do their job.
- Database admin ≠ backup operator
- Code development ≠ , production deployment

Examples:

- Financial systems: Separate approval and payment processing roles
- IT operations: Different teams for development and deployment
- Access management: Different admins for creation and approval

Exam Tip: SoD = fraud prevention through division of responsibilities. Critical for financial systems and privileged access.

Emerging Challenges

Cloud and Hybrid Environments

Key Points:

- Data across multiple geographic locations and jurisdictions
- Shared responsibility model: clear delineation is needed along with documentation and adherence. Most compliances require evidence for everything
- Data localisation requirements (India-specific)

- Unified visibility and control across distributed infrastructure
- Classification must extend consistently across environments

Privacy Regulations and Cross-Border Flows

Key Points:

- DPDP Act 2023: Indian data protection requirements
- GDPR, CCPA: International compliance for global operations
- Data localisation prohibits storing certain data outside India
- Cross-border transfers need standard contractual clauses
- Track data lineage for compliance throughout operations

Indian Context:

- RBI data localisation: Payment data must be stored in India
- CERT-In: 6-hour incident reporting, 180-day log retention
- DPDP Act: Consent management, right to erasure, data breach notification

AI and Machine Learning

Key Points:

- Training data requires protection while maintaining utility
- Model parameters = valuable intellectual property
- Privacy-preserving techniques: Federated learning, differential privacy
- Address bias, ensure explainability, protect against adversarial attacks

- Asset security programs must evolve for AI/ML

Exam Tip: Emerging challenges = apply fundamental principles to new technologies. Classification, lifecycle, and controls still apply.

Key Exam Takeaways - Domain 2

Classification:

- Classification = system of categories (blueprint)
- Categorisation = sorting data into categories (filing)
- Government: Top Secret → Secret → Confidential → Unclassified
- Private: Confidential → Private → Sensitive → Public

Data States:

- At Rest: Encrypted storage (AES-256-GCM recommended)
- In Transit: TLS/HTTPS, VPNs, IPsec
- In Use: Most vulnerable - homomorphic encryption, secure enclaves

Data Roles:

- Owner = Legal accountability
- Custodian = Technical implementation
- Processor = No ownership, works on behalf of the owner

Destruction:

- NIST SP 800-88: Clear → Purge → Destroy

- SSDs must be physically destroyed (wear levelling prevents effective overwriting)
- Certificate of destruction required for audit trail
- Deletion ≠ Destruction (critical distinction!)

DLP:

- Three layers: Network → Storage → Endpoint
- Effectiveness depends on proper classification first
- Cannot inspect encrypted traffic without decryption

Frameworks:

- ISO 27001 = certifiable ISMS requirements
- NIST CSF = risk-based cybersecurity approach
- PCI DSS = Payment Card Industry Data Security Standards mandatory
- A multi-framework strategy is common in large organisations

Labeling vs Marking:

- Labeling = machine-readable metadata (automated controls)
- Marking = human-visible indicators (awareness)

AES Encryption:

- AES-256 = 256-bit KEY size (block size always 128 bits)
- ECB mode = INSECURE (never use)
- GCM mode = RECOMMENDED

Exam Strategy:

- Focus on strategic understanding over technical implementation
- Know distinctions: deletion vs destruction, Labeling vs marking, classification vs categorisation
- Remember Indian context examples, but apply globally
- Risk-based decision-making is core to the CISSP philosophy

Memory Aids

Data Lifecycle: "C-U-S-S-A-D" = Create, Use, Store, Share, Archive, Destroy

NIST Sanitization: "Clear-Purge-Destroy" = increasing security levels

CASB Pillars: "V-D-T-C" = Visibility, Data Security, Threat Protection, Compliance

AES Modes: "GCM Good, CBC Careful, ECB Evil"

Data States: "RAT" = Rest, Active (in use), Transit

Policy Hierarchy: "P-S-B-G-P" = Policies, Standards, Baselines, Guidelines, Procedures

ISO Standards: "27001 = Requirements (What), 27002 = Guidance (How)"

Common Exam Mistakes to Avoid

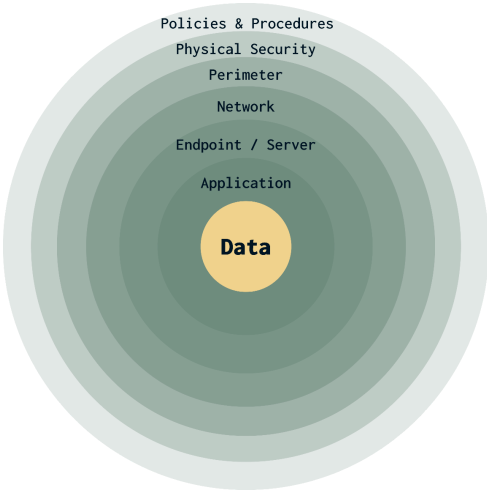
- Confusing deletion with destruction - Deletion only removes pointers; data remains recoverable
- Thinking ECB mode is acceptable - ECB is cryptographically broken, always the wrong answer.

- Forgetting SSDs need physical destruction - Overwriting doesn't work due to wear leveling.
- Mixing up Labeling and marking - Labels for machines, marks for humans
- Assuming DLP works on all encrypted traffic - Cannot inspect without decryption
- Confusing owner and custodian roles - Owner = accountability, Custodian = implementation
- Forgetting certificate of destruction - Required for defensible destruction
- Not knowing NIST SP 800-88 superseded DoD 5220.22-M - Use current standards
- Thinking one framework fits all - Large organisations use multiple frameworks
- Ignoring risk-based approach - CISSP is about strategic risk management, not checklist compliance

Domain 3: Security Architecture and Engineering

Secure System Design Fundamentals

Defense-in-Depth & Layering

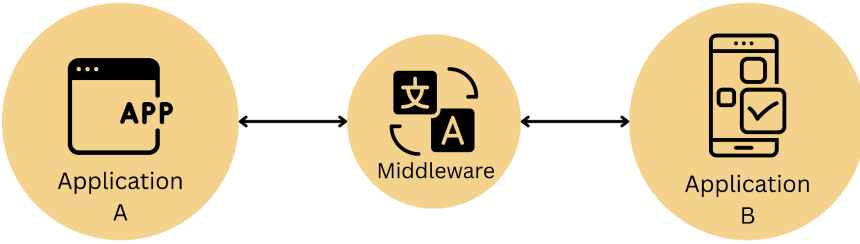


Key Points:

- Multiple overlapping controls at different layers (technical, administrative, physical)
- Each layer only communicates with adjacent layers
- No single point of failure - if one layer fails, others still protect
- Hardware → Drivers → Kernel → OS → Applications
- Example: Email security with cloud filter → gateway → server → endpoint → SOC

Exam Tip: Defence-in-depth ≠ redundancy. It's about the diversity of controls across layers, not duplicating the same control.Think from a perspective of Secure Design Principles, Least Privilege, Fail-Safe Defaults.

Abstraction in Security



Key Points:

- Hides complexity from users, provides simple interfaces
- Protects implementation details
- Common layers: APIs, virtualisation, middleware
- Reduces attack surface by limiting direct access
- Example: Payment app → API gateway → auth → fraud detection → encryption → banking system

Exam Tip: Abstraction enables security by limiting what users/processes can directly access.

Security Domains & Trust Boundaries

Government Classification Domains:

- Confidential - Regular staff area
- Secret - Officer's section
- Top Secret - Minister's cabin

- Strict rules for information flow between levels

Key Points:

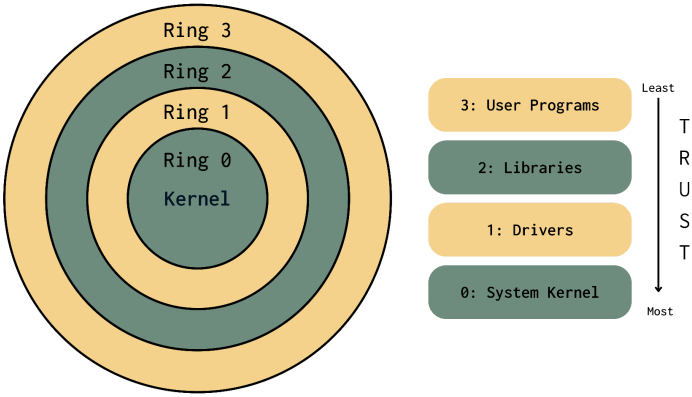
- Security domains define different trust/access levels
- Trust boundaries = transitions between domains (require validation)
- User Mode (Ring 3): Limited access, where applications run
- Kernel Mode (Ring 0): Full system access, where the OS core runs
- Strict information flow rules between levels

Indian Context:

- Defence/government use classified domains for data segregation
- DPDP Act requires clear data boundaries

Exam Tip: User mode can't directly access hardware - must request from kernel mode. This prevents malicious apps from directly controlling hardware.

The Ring Model



Key Points:

- Ring 1: Hypervisor (controls VMs, highest privilege)
- Ring 0: Kernel (OS core, most trusted)
- Most modern operating systems use only ring 0 for the kernel and drivers and ring 3 for applications, while rings 1 and 2 are rarely used intermediate privilege levels.
- Ring 3: Applications (least privilege)
- Lower ring number = more privilege = more dangerous if compromised
- Modern extensions: Intel SGX, AMD SEV, ARM TrustZone

Modern Hardware Security Extensions:

- Intel VT-x/AMD-V: Hardware virtualisation for Ring-1
- Intel SGX: Secure enclaves in Ring 3, protected from Ring 0
- AMD SEV: Encrypts VM memory from the hypervisor
- ARM TrustZone: Secure World vs Normal World separation

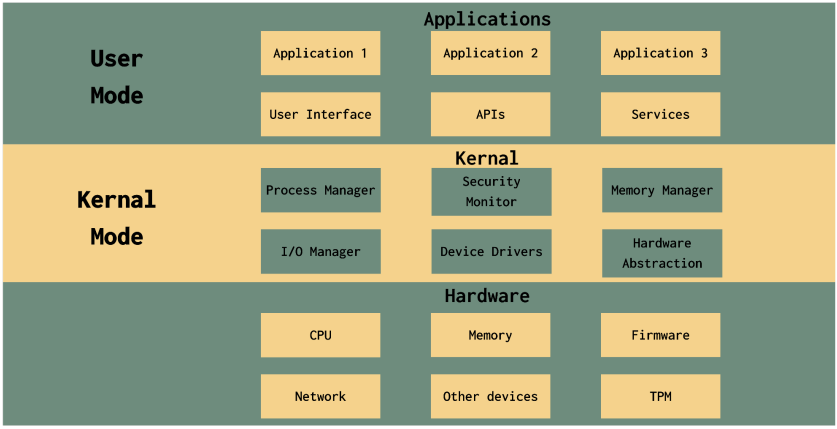
- SMEP/SMAP: Prevent kernel from executing/accessing user memory

Indian Context:

- UPI payments use TrustZone for PIN protection (50+ crore users)
- Payment processors use SGX for sensitive data processing

Exam Tip: Ring 0 compromise (rootkit) >> Ring 3 compromise (app malware). Memorise: Lower ring = higher privilege = higher risk.

Process Isolation & Memory Protection



Key Points:

- Each process gets an isolated memory space
- Memory Management Unit (MMU) enforces access controls

- Virtual memory makes each process think it owns the entire system
- Prevents accidental data mixing and deliberate snooping
- Critical for cloud/multi-tenant environments

Exam Tip: Process isolation is THE foundation of modern OS security. Without it, any app could read/modify any other app's data.

Reference Monitor & Security Kernel

Three Unbreakable Rules:

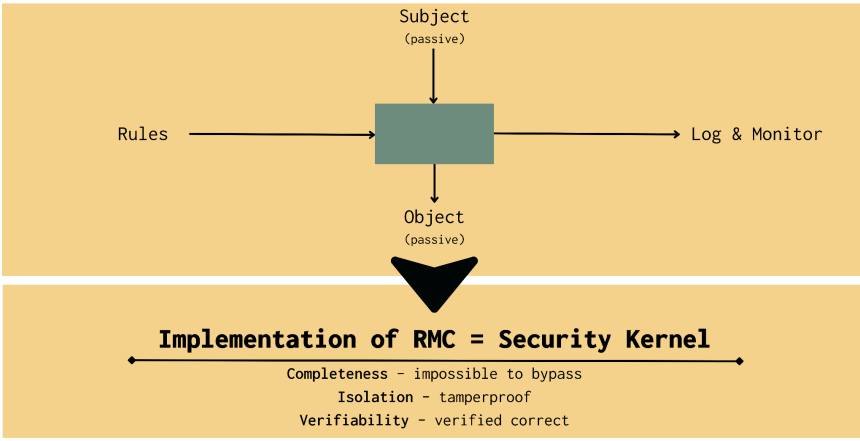
- Completeness: Mediates ALL access (no bypasses)
- Isolation: Tamper-proof (can't be modified/disabled)
- Verifiability: Simple enough to test thoroughly

Key Points:

- Security kernel = implementation of the reference monitor concept
- Implements Mandatory Access Control (MAC)
- Prevents information leakage between classification levels
- Example: Military systems enforcing Secret vs Top Secret separation

Exam Tip: Reference monitor is a concept; security kernel is the implementation. Think airport security - EVERYONE must pass through (completeness), can't break the scanner (isolation), we can verify it works (verifiability).

Trusted Computing Base (TCB)



Key Points:

- TCB = all hardware/software critical for security enforcement
- Includes: hardware, security kernel, critical utilities, security drivers
- Smaller TCB = Better security (less code to verify, fewer vulnerabilities)
- If ANY TCB component fails, security is compromised
- Example: Chrome OS has a minimal TCB with most functions in the user space

Exam Tip: TCB is like a building foundation - if it fails, everything collapses. Always minimise TCB size.

Security Models

Layer / Lattice-based Models	Rule-based Models
• Bell-LaPadula • Biba	• Information Flow • Clark-Wilson • Brewer-Nash (Chinese Wall) • Graham-Denning • Harrison-Ruzzo-Ullman

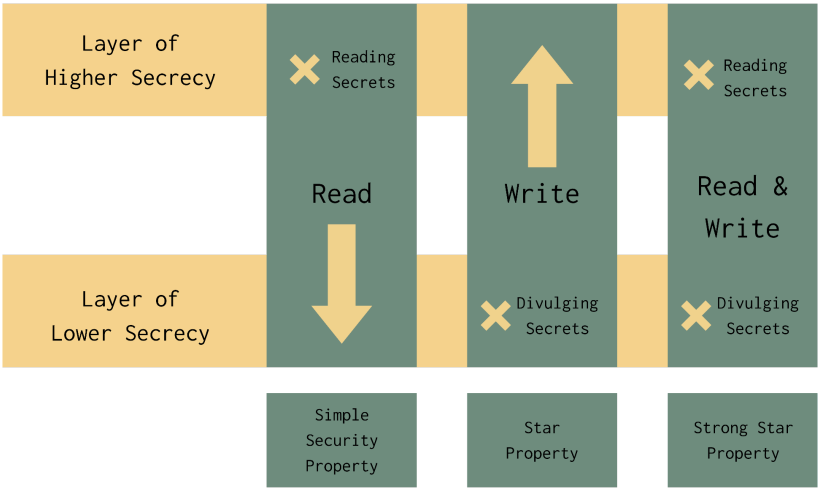
Lattice-Based Access Control (LBAC)

Key Points:

- Hierarchical access based on security labels
- Information flows follow dominance rules
- Read down hierarchy (see subordinates' work)
- Write up or same level (no leaking down)
- Example: Engineers with Confidential clearance can read Public/Restricted/Confidential but not Secret/Top Secret

Exam Tip: Lattice = hierarchy. Think corporate org chart - you see below, not above.

Bell-LaPadula Model (Confidentiality)



Key Points:

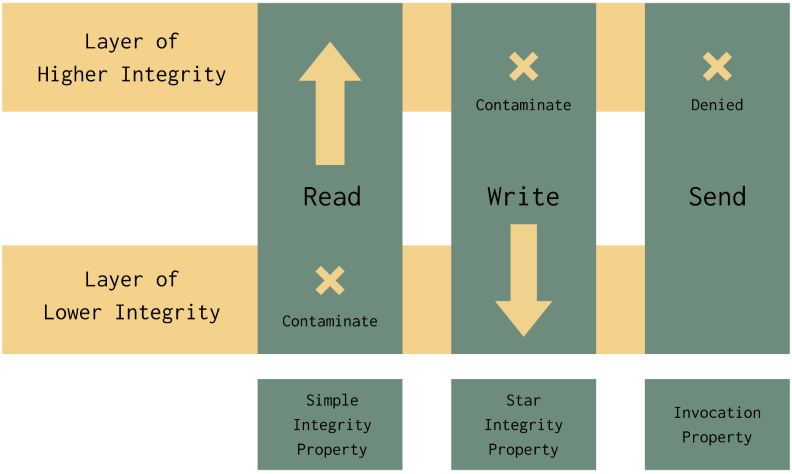
- Focus: CONFIDENTIALITY (prevents information leakage)
- Simple Security (ss-property): "No Read Up" - can't read higher classification
- Star Property (*-property): "No Write Down" - can't write to lower classification
- Strong Star: Read AND write only at the same level
- Tranquillity: Security labels don't change (Strong) or only change if policy allows (Weak)
- Example: Secret clearance can't read Top Secret or write to Unclassified

Memory Trick:

- Bell-LaPadula = Confidentiality (both have NO 'i')
- Read UP? NO! Write DOWN? NO!
- Prevents secrets from flowing down

Exam Tip: Military/government use this for classified data. If the question mentions "classified," "military," "prevent leaks" → Bell-LaPadula.

Biba Model (Integrity)



Key Points:

- Focus: INTEGRITY (prevents data contamination)
- Simple Integrity: "No Read Down" - can't read lower integrity (prevents contamination)
- Star Integrity: "No Write Up" - can't write to higher integrity (prevents corruption)
- Invocation Property: Can't execute higher integrity subjects
- OPPOSITE of Bell-LaPadula!
- Example: Bank clerks can't modify central reports (no write-up) or use unverified data (no read-down)

Memory Trick:

- Biba = Integrity (both have 'i')

- OPPOSITE of Bell-LaPadula
- Keeps quality data clean

Exam Tip: Banking/financial systems use Biba. If the question mentions "data quality," "accuracy," "prevent corruption" → Biba.

Clark-Wilson Model (Commercial Integrity)

Well-Formed Transactions	Separation of Duties	Access Triple
• Good, consistent, validated data • Only perform operations in a manner that won't compromise the integrity of objects	• One person shouldn't be allowed to perform all tasks related to a critical function	• Subject | Program | Object • A subject cannot directly access an object • Access must go through a program that enforces access rules (e.g., in a database)

Key Points:

- Focus: Commercial transaction integrity
- CDIs (Constrained Data Items): Protected data (account balances)
- UDIs (Unconstrained Data Items): Unprotected data (customer inquiries)
- TPs (Transformation Procedures): Authorised programs only
- IVPs (Integrity Verification Procedures): Validation processes
- No direct data manipulation - all changes through validated programs

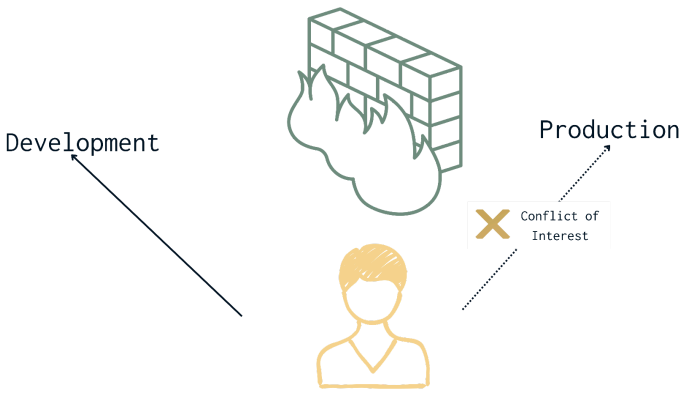
- Enforces separation of duties with audit trails

Key Guarantees:

- Well-formed transactions only
- Separation of duties
- Audit trail for all changes

Exam Tip: Banking transactions = Clark-Wilson. If the question mentions "transactions," "banking," "separation of duties," "audit trails", → Clark-Wilson.

Brewer-Nash Model (Chinese Wall)



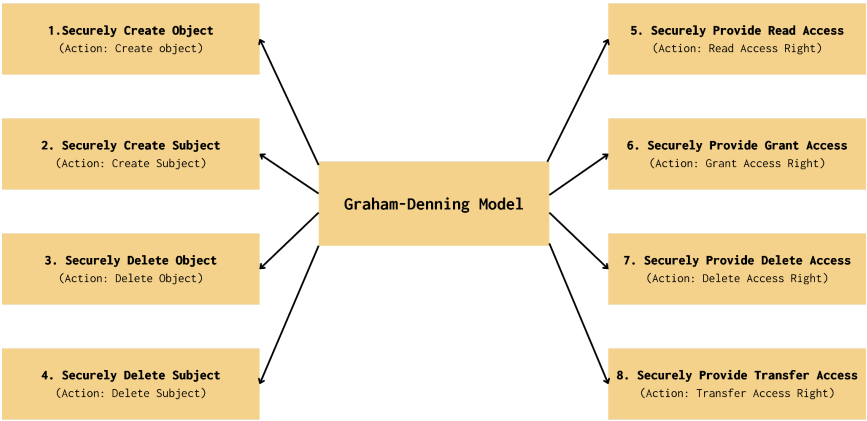
Key Points:

- Focus: Conflict of interest prevention
- Access rules change dynamically based on what you've already accessed
- Once you access Company A, you're blocked from competitor Company B

- Used in: investment banking, consulting, law firms
- Example: A Consultant working on the Bank A merger is automatically blocked from Bank B data

Exam Tip: "Conflict of interest" in question → Chinese Wall. Hypothetically, a lawyer can't represent both sides in a divorce.

Graham-Denning Model

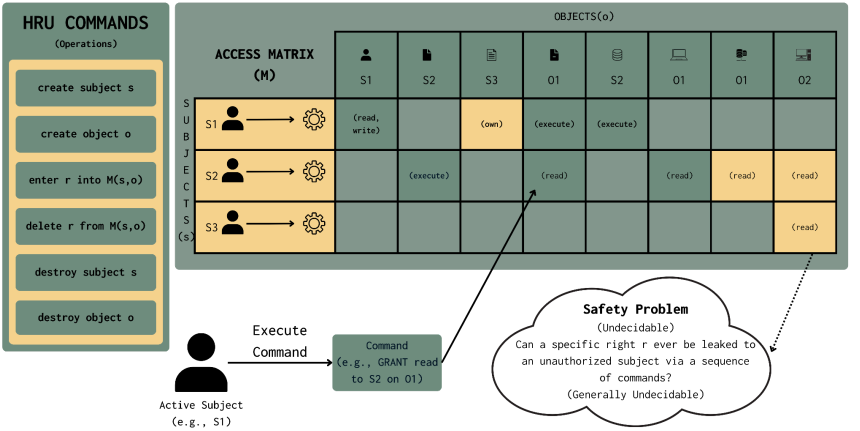


Eight Primitive Rights:

1. Create object
2. Create subject
3. Delete object
4. Delete subject
5. Read access right
6. Grant access rights
7. Delete access right
8. Transfer access rights

Exam Tip: Foundational model for OS access control. Defines WHO can do WHAT to objects/subjects.

Harrison-Ruzzo-Ullman (HRU) Model

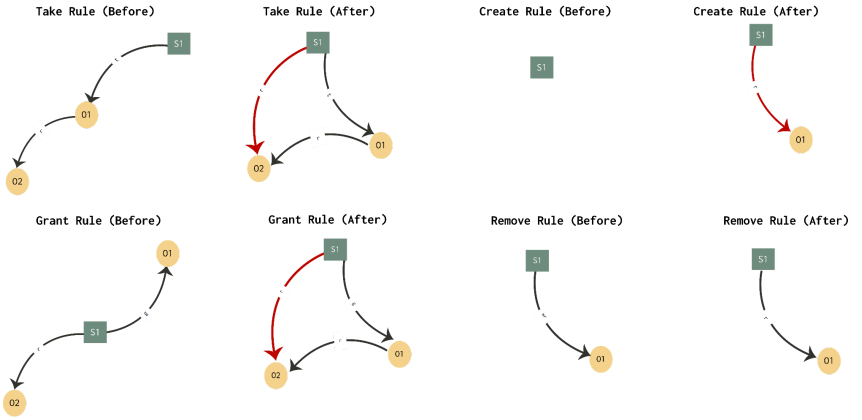


Key Points:

- Formalises Access Control Matrix and state changes
- Safety Problem: Can a specific right ever leak through the operations chain?
- Undecidability: For complex systems, safety is mathematically unprovable
- Proves that DAC (Discretionary Access Control) is inherently "unsafe"
- High-security environments use MAC (Mandatory Access Control) for decidable safety

Exam Tip: HRU proves why the military/government uses MAC instead of DAC - DAC safety can't be guaranteed.

Take-Grant Model



Four Operations:

- Take: Subject takes rights from another subject
- Grant: Subject grants rights to another subject
- Create: Subject creates a new object/subject
- Remove: Subject removes own rights

Exam Tip: Graph-based model. Think cloud IAM with assume-role (take) and delegate (grant).

Model Selection Quick Reference

Exam Scenario Matching:

- Military classification → Bell-LaPadula
- Banking transactions → Clark-Wilson
- Data quality/accuracy → Biba
- Conflict of interest → Chinese Wall (Brewer-Nash)
- OS access control → Graham-Denning

- Proving safety limits → HRU

Security Evaluation & Certification

Certification vs Accreditation

Characteristics	Certification	Accreditation
Definition	Refers to a written assurance by a third party on the conformity of a service, product, or process, based on certain specified requirements provided by some form of education, audit, assessment, or external review.	Refers to formal recognition of competency towards specified standards by an authoritative body.
Base activities	Relates to all company activities in a given industry.	Is based on specific activities and is not based on all activities in an organization.
Endorsements	Involves the endorsement of a product, service, or process by a third party.	Involves the endorsement of a product, service, or process by an independent third party.

Key Points:

- Certification: Technical evaluation - "Does it work as claimed?"
- Accreditation: Management decision - "Is it safe to use here?"
- Certification = technical validation, Accreditation = risk acceptance
- Example: RBI certifies the payment system technically, then accredits it for production use

Exam Tip: Certification is TECHNICAL, Accreditation is a MANAGEMENT decision. Don't get confused!

Common Criteria (ISO/IEC 15408)

Assurance Level	Description
E6	Formal end-to-end security tests + source code reviews
E5	Semi-formal system + unit tests and source code review
E4	Semi-formal system + unit tests
E3	Informal system + unit tests
E2	Informal system tests
E1	System in development
E0	Inadequate assurance

Key Components:

- TOE (Target of Evaluation): Product being evaluated
- PP (Protection Profile): Standard security requirements for the product category
- ST (Security Target): Vendor's specific implementation claims
- EAL (Evaluation Assurance Level): Depth of evaluation (1-7)

EAL Levels:

- EAL1: Functionally tested (basic)
- EAL2: Structurally tested
- EAL3: Methodically tested
- EAL4: Methodically designed/tested (highest commercially feasible)
- EAL5-7: Semi-formal to formal verification (government/military)

Indian Context:

- Defence procurement often requires Common Criteria certification
- Critical infrastructure may mandate specific EAL levels

Exam Tip: EAL4 = sweet spot for commercial products. Higher levels are too expensive except for the government/military.

Legacy Standards (Know for Exam)

Orange Book (TCSEC):

- D (failed) → C1/C2 (discretionary) → B1/B2/B3 (mandatory) → A1 (verified)
- Confidentiality ONLY (no integrity/availability)
- Military-focused, now superseded

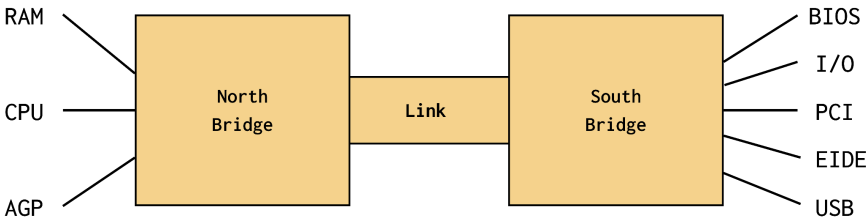
ITSEC (European):

- Separated functionality from assurance
- Addressed confidentiality, integrity, AND availability
- Led to Common Criteria

Exam Tip: Orange Book = old, confidentiality-only, military. Common Criteria = current, comprehensive, international.

Secure Hardware & System Architecture

System Architecture Fundamentals



Traditional Architecture:

- Northbridge: High-speed (CPU, RAM, graphics)
- Southbridge: Slower peripherals (USB, storage, network, BIOS)
- Modern CPUs integrate the Northbridge for better security

Exam Tip: Compromising Northbridge (memory access) >> Southbridge (peripherals) in impact.

CPU Security Features

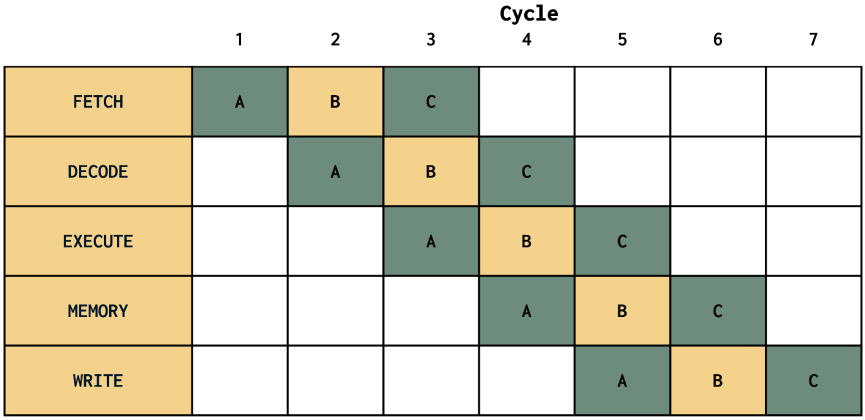
Key Features:

- DEP (Data Execution Prevention (DEP): Data Execution Prevention (DEP) is an OS security feature that marks certain memory regions as non-executable to help prevent

malicious code execution from data pages such as the stack and heap
- ASLR (Address Space Layout Randomisation): Randomises memory locations
- Hardware RNG: True random numbers for crypto
- Intel TXT/AMD SVM: Trusted execution, hardware attestation

Exam Tip: DEP + ASLR together make exploitation much harder. DEP prevents execution, ASLR prevents prediction.

Instruction Pipeline & Vulnerabilities



Pipeline Stages:

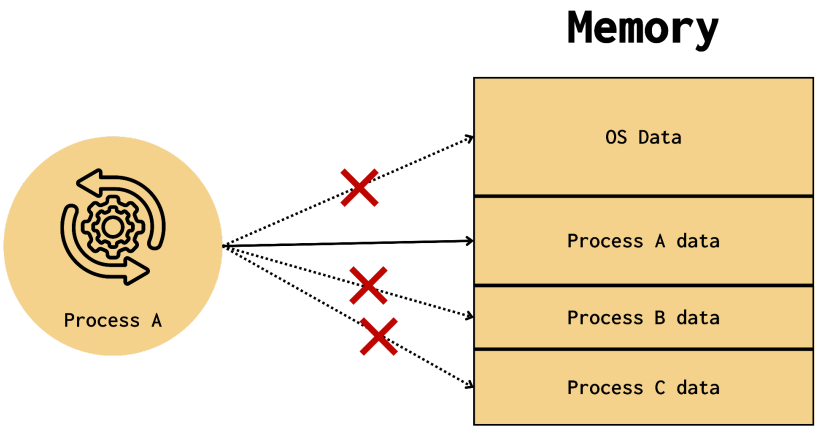
1. Fetch instruction
2. Decode instruction
3. Execute operation
4. Store results

Security Implications:

- Speculative execution can leak info (Spectre/Meltdown)
- Cache timing attacks reveal sensitive data
- Pipeline stalls can indicate security operations

Exam Tip: Modern CPUs sacrifice some security for performance (speculative execution). Know the tradeoff.

Memory Protection



Key Mechanisms:

- Virtual Memory: Each process sees an isolated address space
- MMU (Memory Management Unit): Translates virtual→physical, enforces access
- Segmentation: Different protection for code/data segments
- Paging: Fixed-size pages with granular permissions
- ASLR: Randomises base addresses

Exam Tip: Virtual memory + MMU = foundation of process isolation. Critical for multi-tenant cloud.

Trusted Platform Module (TPM)

Key Functions:

- Secure Key Storage: Keys never leave TPM in plaintext
- Platform Attestation: Proves legitimate boot (secure boot)
- Sealed Storage: Data encrypted, only decryptable on the same platform
- Protection even if the OS/system is compromised

Indian Context:

- Banking devices use TPM for transaction signing

Exam Tip: TPM = hardware root of trust. Keys in TPM >> keys in software.

Hardware Security Modules (HSMs)

Key Features:

- Physical Security: Tamper-evident/responsive cases destroy keys if breached
- Crypto Acceleration: Thousands of operations/second
- Compliance: FIPS 140-2 Level 3/4 certification
- Dedicated cryptographic processor

Uses:

- ATM PIN verification
- Core banking transaction signing

- Payment card key management
- OTP generation

Indian Context:

- Major banks use HSMs for all crypto operations
- RBI mandates HSMs for critical financial systems

Exam Tip: HSMs for high-value keys (banking), TPM for platform security. HSMs >> general-purpose systems for crypto.

Watchdog Timers

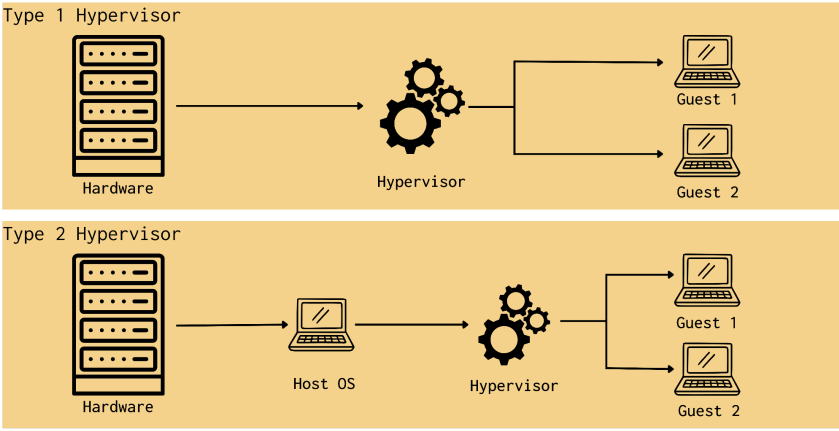
Key Points:

- The system must periodically reset the timer ("kick the dog")
- If the system hangs/crashes, the timer triggers corrective action
- Actions: reset, safe shutdown, fail-safe state
- Critical for: embedded systems, industrial controls, network equipment

Exam Tip: Watchdog = availability control. Ensures automatic recovery from failures.

Virtualisation & Cloud Security

Hypervisor Types



Type 1 (Bare Metal):

- Runs directly on hardware
- Examples: VMware ESXi, Hyper-V, Xen
- Better security (smaller attack surface)
- Production environments

Type 2 (Hosted):

- Runs on host OS
- Examples: VMware Workstation, VirtualBox, Parallels
- Larger attack surface (OS vulnerability)
- Development/testing

Exam Tip: Type 1 >> Type 2 for production security.

Virtual Machine Security

Key Threats:

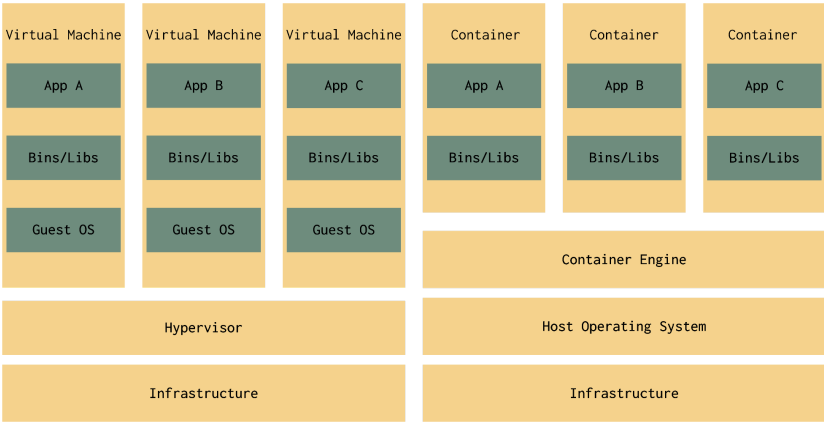
- VM Escape: Breaking out to hypervisor/other VMs (catastrophic)
- VM Sprawl: Uncontrolled VM proliferation (forgotten, unpatched systems)
- Resource Contention: Side-channel attacks via shared resources
- Snapshot Management: Old snapshots contain vulnerabilities

Countermeasures:

- VM lifecycle management
- Regular patching
- Isolation of sensitive workloads
- Encrypted VM memory (AMD SEV)

Exam Tip: VM escape = worst-case scenario. Proper hypervisor patching is critical.

Container Security



Benefits:

- Lighter than VMs (share kernel)
- Faster deployment
- Consistent environments
- Efficient resources

Security Considerations:

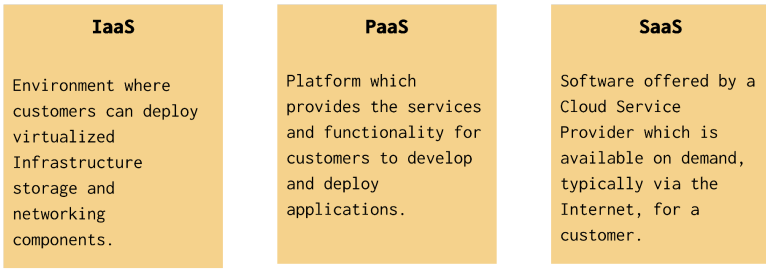
- Kernel vulnerabilities affect ALL containers
- Weaker isolation than VMs
- Image security (supply chain)
- Runtime monitoring challenges

Indian Context:

- Fintech/startups use containers (Docker/Kubernetes) extensively
- Require a careful security architecture for isolation

Exam Tip: Containers share kernels = weaker isolation than VMs. Good for microservices, but consider security tradeoffs.

Cloud Shared Responsibility Model



Provider Responsibilities:

- Physical security
- Hypervisor security
- Network infrastructure
- Hardware maintenance

Customer Responsibilities:

- Data encryption
- IAM (Identity & Access Management)
- Application security
- Configuration management

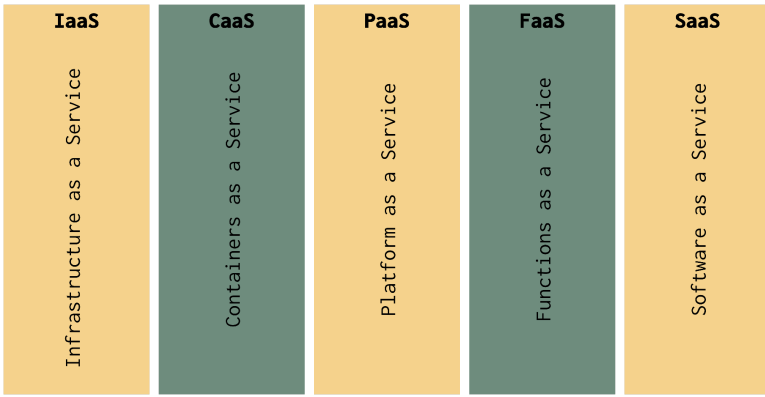
Service Model Differences:

- IaaS: Customer manages OS upward
- PaaS: Customer manages apps and data
- SaaS: Customer manages data and has access only

- FaaS (Serverless): Customer manages code and data
- CaaS (Containers): Customer manages images, code, data

Exam Tip: Most cloud breaches = customer misconfiguration, NOT provider failure. Know YOUR responsibilities!

Serverless Security



Advantages:

- No server management
- Auto-scaling prevents resource DoS
- Minimal attack surface (brief execution)
- Cost-effective for variable workloads

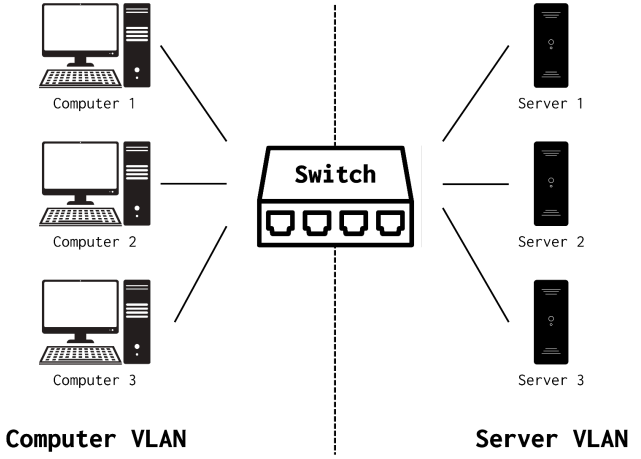
Challenges:

- Limited runtime visibility
- Dependency on provider security
- Complex access control across functions

- Potential bill shock from abuse

Exam Tip: Serverless = less operational burden but less control. Good for specific use cases, not everything.

IoT & Mobile Device Isolation



IoT Security Challenges:

- Weak/default credentials
- Limited processing power (weak crypto)
- Infrequent updates
- Physical access vulnerability
- Heterogeneous protocols

VLAN Isolation Strategy:

- Device Type Segregation:
    - VLAN 100: IP cameras, physical security
    - VLAN 200: HVAC, building automation

    - VLAN 300: Industrial sensors
    - VLAN 400: Guest/employee mobile
- Risk-Based Isolation:
    - High-Risk: Legacy, unknown, personal IoT
    - Medium-Risk: Managed corporate IoT
    - Low-Risk: Updated devices with strong auth

Mobile Security:

- Treat smartphones as untrusted endpoints
- MDM (Mobile Device Management) integration
- Certificate-based authentication
- Traffic inspection through security gateways

Indian Context:

- Smart meters in the power grid (thousands of IoT devices)
- BYOD culture requires strong mobile security

Exam Tip: IoT = high risk due to weak security. Network segmentation is critical. Isolate by device type and risk level.

Cryptographic Systems

Core Cryptographic Principles

Kerckhoffs's Principle:

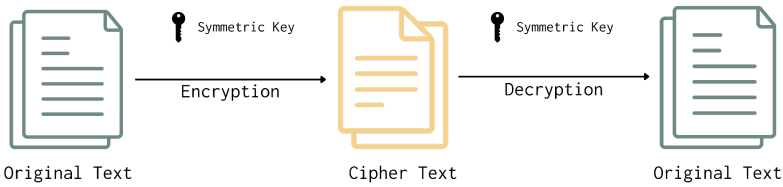
- Security depends ONLY on key secrecy, NOT algorithm secrecy
- Use open, peer-reviewed algorithms (AES, RSA)
- Avoid proprietary "security through obscurity"

Indian Context:

- Aadhaar biometrics, UPI payments use open algorithms (AES, RSA)
- Security = key management, not secret algorithms

Exam Tip: "Security through obscurity" = BAD. Open algorithms + strong key management = GOOD.

Symmetric Cryptography



Key Points:

- Same key for encryption AND decryption
- Fast, efficient for bulk data
- Key Distribution Problem: How to securely share a key?

Block Ciphers:

- AES: Global standard (128/192/256-bit keys)
- 3DES: Legacy, still in banking

- Fixed-size blocks (AES = 128-bit blocks)

Stream Ciphers:

- Bit-by-bit or byte-by-byte
- Faster for real-time (wireless, streaming)
- More vulnerable if improperly implemented

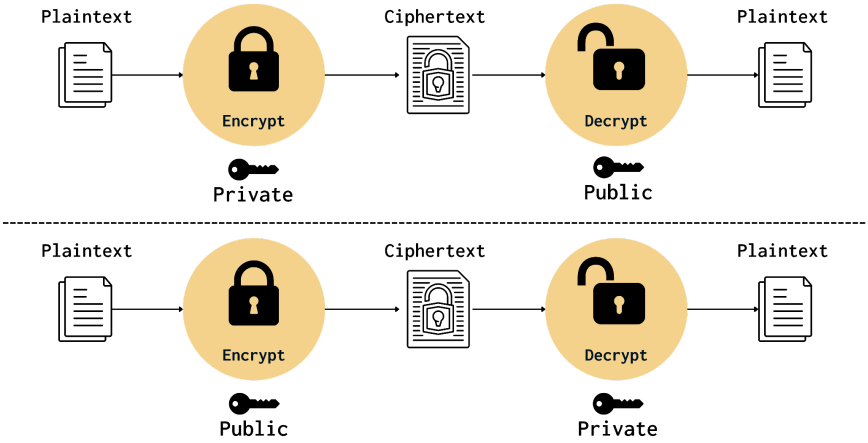
Modes of Operation:

- ECB (Electronic Codebook): INSECURE, reveals patterns
- CBC (Cypher Block Chaining): Common, needs IV (Initialisation Vector)
- CTR (Counter): Parallelizable, turns block into stream
- GCM (Galois/Counter Mode): Encryption + authentication

Exam Tip:

- AES = current standard
- Avoid ECB (reveals patterns)
- GCM provides encryption + integrity

Asymmetric Cryptography



Key Points:

- Key pair: public key (shareable) + private key (secret)
- Solves the key distribution problem
- SLOW compared to symmetric (computational overhead)

Common Algorithms:

- RSA: Most widely deployed (2048-bit minimum, 4096-bit for long-term)
- ECC (Elliptic Curve): Smaller keys, same security (256-bit ECC ≈ 3072-bit RSA)
- Diffie-Hellman: Key exchange over an insecure channel

Uses:

- Digital signatures
- Key exchange
- Initial authentication (then switch to symmetric for speed)

Indian Context:

- Digital signatures for IT Act compliance
- UPI uses ECC for mobile efficiency

Exam Tip:

- Asymmetric = key distribution solution, but SLOW
- Hybrid: asymmetric to exchange symmetric key, then symmetric for bulk data
- RSA minimum 2048-bit, ECC 256-bit for equivalent security

Cryptographic Hash Functions

Properties:

- One-way: Can't recover input from hash
- Avalanche Effect: Small input change → large output change
- Collision Resistance: Infeasible to find two inputs with the same hash

Common Algorithms:

- MD5: 128-bit, BROKEN, checksums only
- SHA-1: 160-bit, DEPRECATED, legacy only
- SHA-2: 224/256/384/512-bit, CURRENT STANDARD
- SHA-3: Latest, different construction

Uses:

- Password storage (with salting!)
- Digital signatures (hash then sign)
- Integrity verification

- Blockchain

Indian Context:

- Government mandates SHA-256 minimum for new systems
- Legacy systems still use older algorithms (migration needed)

Exam Tip:

- SHA-256+ for new systems
- ALWAYS salt passwords before hashing
- Birthday attacks target collision resistance

Digital Signatures

Process:

1. Hash the message
2. Encrypt hash with sender's private key = signature
3. The recipient verifies the signature using the public key
4. Compare with independently computed hash

Provides:

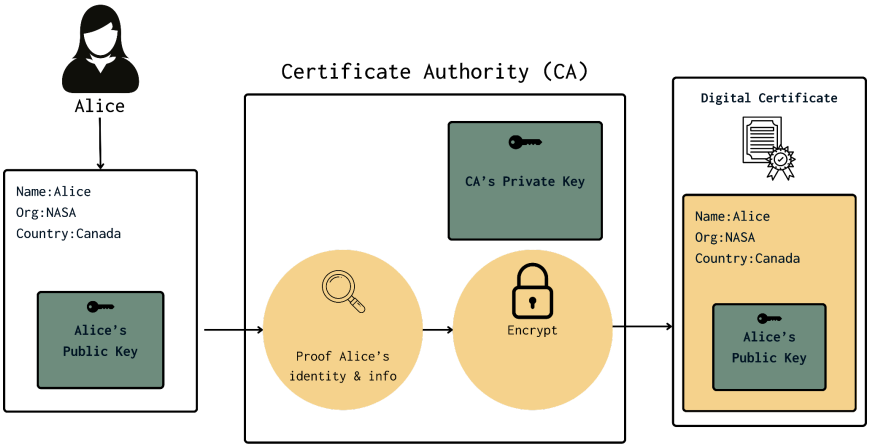
- Authentication: Only the private key holder could create a signature
- Integrity: Any modification invalidates the signature
- Non-repudiation: Sender can't deny signing

Indian Context:

- IT Act recognises digital signatures = handwritten signatures
- e-filing, company registration, and government services use digital signatures

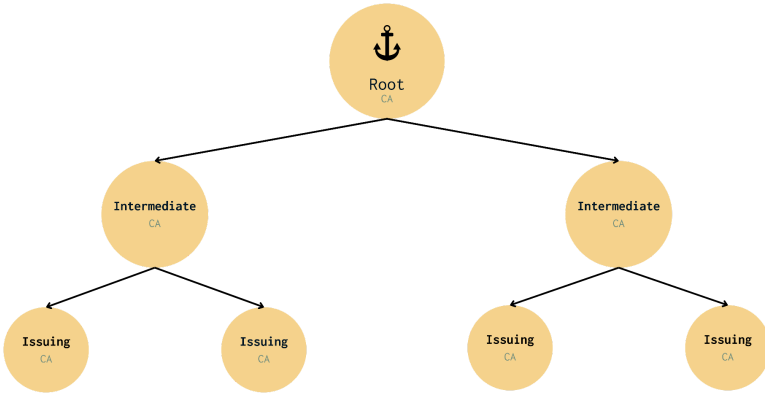
Exam Tip: Digital signature = hash + private key encryption. Provides authentication + integrity, + non-repudiation.

Public Key Infrastructure (PKI)



Components:

- CA (Certificate Authority): Issues and revokes certificates
- RA (Registration Authority): Verifies identity before issuance
- Certificate Repository: Stores issued certificates
- CRL (Certificate Revocation List): Lists revoked certificates
- OCSP (Online Certificate Status Protocol): Real-time validation



X.509 Certificates Contain:

- Subject's public key
- Subject's identity
- Issuer's identity and signature
- Validity period
- Usage restrictions

Indian Context:

- National CAs for digital signatures (e-governance)
- Tax filing and company registration use PKI

Exam Tip: PKI = trust infrastructure. CA is a trusted third party. Certificate = binding of identity to a public key.

Key Management Lifecycle

Key Stages:

1. Generation: Use hardware RNG, secure environment

2. Distribution: Out-of-band for symmetric, PKI for asymmetric
3. Storage: HSMs for high-value, encrypted key stores, access controls
4. Rotation: Regular replacement (limits compromise exposure)
5. Destruction: Cryptographic erasure, physical destruction, audit trail

Exam Tip: Key management is often harder than crypto itself. Most crypto failures = key management, not algorithm breaks.

Cryptographic Attacks

Attack Types:

- Brute Force: Try all keys (defeated by key length - 128-bit symmetric secure)
- Cryptanalysis: Mathematical attacks (linear, differential, birthday)
- Implementation Attacks: Timing, power analysis, fault injection
- Social Engineering: Phishing for passwords/keys

Birthday Attack:

- Exploits collision probability in hash functions
- With 23 people, 50% chance that two share a birthday
- For n-bit hash, collision in ~2^(n/2) attempts vs 2^n brute force
- We need larger hashes than keys

Exam Tip: Most attacks target implementation/humans, not algorithms. Strong crypto ≠ secure system if poorly implemented.

Quantum Computing Impact

Quantum Threat:

- Shor's Algorithm: Breaks RSA, ECC, Diffie-Hellman
- Grover's Algorithm: Weakens symmetric (double key size needed)
- "Harvest now, decrypt later" - attackers storing encrypted data for future quantum decryption

Post-Quantum Cryptography (PQC):

- NIST PQC Standards: Kyber (KEM), Dilithium/FALCON (signatures), SPHINCS+ (conservative)
- Requires crypto-agility (ability to update algorithms)
- Hybrid approach: classical + PQC during transition

Timeline:

- Quantum threat imminent, not distant
- Start planning migration NOW for long-term sensitive data

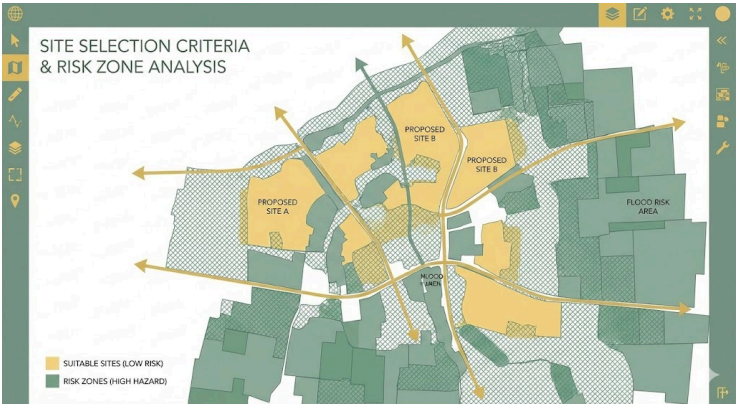
Exam Tip:

- Quantum breaks asymmetric, weakens symmetric
- Long-term sensitive data at risk NOW (harvest now, decrypt later)
- Crypto-agility is essential for algorithm updates

Physical Security

Control Type	Description
Deter / Prevent	This type of control serves to deter or prevent an intruder from taking a certain action. A sign in front of a property is an example.
Delay	Delay controls function to hinder activity being pursued by an intruder. Locks are a great example.
Detect	Detective controls help detect or alert to an intrusion. A barking dog is a good example of a detective control.
Assess	Assessment can lead to a proper response to a given situation. Assessment functions in the same manner as detective controls.
Respond	Aligned with “assess” is “respond,” which functions in the same manner as a corrective control.

Site Selection & Design



Geographic Considerations:

- Natural disaster risks (floods, earthquakes, cyclones)
- Distance from hazards (chemical plants, airports)
- Crime rates
- Proximity to emergency services
- Utility reliability (power, internet, water)

CPTED (Crime Prevention Through Environmental Design):

- Natural Surveillance: Maximise visibility (clear sight lines, transparent materials)
- Natural Access Control: Guide movement (limited entry points, landscaping)
- Territorial Reinforcement: Clear ownership (branding, maintenance, public/private transitions)

Indian Context:

- Data centres avoid flood zones (Mumbai monsoons), seismic zones
- Consider region-specific risks (cyclones in coastal areas)

Exam Tip: Life safety first, asset protection second. Site selection = proactive physical security.

Perimeter Defenses

Landscaping:

- Avoid large trees/bushes near buildings (concealment)
- Slope away from critical assets (flood prevention)
- Direct foot traffic

Fencing:

- 3-4 feet: Casual deterrent
- 6-7 feet: Serious barrier
- 8+ feet with anti-climb: High security
- PIDAS: Multiple fences with detection

Lighting:

- Continuous for high-security areas
- Motion-activated for detection
- Emergency backup (battery/generator)
- Eliminate shadows

Gates & Bollards:

- Control authorised entry
- Bollards prevent vehicle ramming
- Rated for vehicle size/speed

Indian Context:

- Major facilities use bollards after security incidents
- Critical infrastructure has multiple fence layers

Exam Tip: Defence-in-depth applies to physical security too. Multiple perimeter layers.

Building Security

Entry Controls:

- Mantraps: Two interlocking doors prevent tailgating
- Turnstiles: One person per authentication
- Metal Detectors/X-ray: Contraband detection
- Security Guards: Human judgment

Internal Security Zones:

- Public (lobbies, meeting rooms)
- General work areas
- Restricted areas (server rooms, executive offices)
- High-security areas (data centre vaults)
- Progressive controls for each zone

Lock Types:

- Mechanical: Vulnerable to picking, bumping, and key duplication
- Electronic: Card cloning, replay attacks, power failures

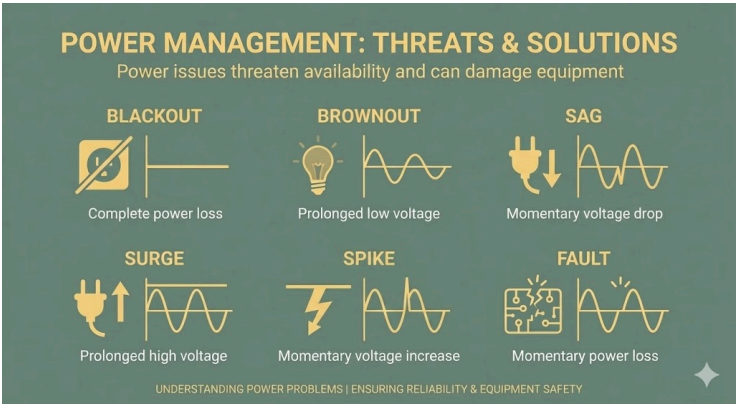
- Biometric: False accept/reject, spoofing
- Multi-factor: Best - combine multiple methods

Indian Context:

- Smart cards dominate corporate environments
- Sensitive areas: smart card + PIN or biometric

Exam Tip: Mantraps prevent tailgating (one person at a time). Multi-factor locks are best for high-security areas.

Environmental Controls



Power Issues & Protection:

- Blackout: Complete loss → UPS + Generator
- Brownout: Prolonged low voltage → Voltage regulator
- Sag: Momentary drop → UPS
- Surge: Prolonged high voltage → Surge protector
- Spike: Momentary high → Surge protector
- Fault: Momentary loss → UPS

Power Protection:

- UPS: Minutes for graceful shutdown
- Generator: Hours/days with fuel
- Power Conditioners: Clean/regulate power
- Dual Feeds: Redundant grid connections
- Automatic Transfer Switch: Seamless failover

HVAC Requirements:

- Temperature: 60-75°F (15-23°C)
- Humidity: 40-60% RH
    - Too low → static electricity
    - Too high → condensation
- Hot aisle/cold aisle configuration
- Filtration for dust/contaminants

Exam Tip: UPS for short-term (minutes), generator for long-term (hours/days). Proper humidity is critical - too low or too high, both damage equipment.

Fire Detection & Suppression

US Class	Europe Class	Material	Suppression Agent
A	A	Ordinary combustibles such as wood and paper	Water or soda acid
B	B	Liquid	Halon / Halon substitute, CO_2, or soda acid
B	C	Flammable gases	Halon / Halon substitute, CO_2, or soda acid
C	E	Electrical equipment	Halon / Halon substitute, CO_2
D	D	Combustible metals	Dry powder
K	F	Kitchen (oil or fat) fires	Wet chemicals

Detection Systems:

- Heat Detectors: Temperature changes
- Smoke Detectors: Photoelectric or ionisation
- Flame Detectors: UV/IR radiation
- VESDA (Very Early Smoke Detection): Earliest warning

Fire Stages:

1. Incipient: Air ionisation, no smoke
2. Smoke: Visible smoke
3. Flame: Visible flame
4. Heat: Intense heat, everything burns

Suppression Systems:

Water-based (damages electronics):

- Wet Pipe: Always charged with water
- Dry Pipe: Filled with air until activation
- Pre-action: Two-stage activation (prevents false discharge)

- Deluge: All sprinklers activate simultaneously

Gas-based (safe for electronics):

- FM-200: Common Halon replacement
- Inergen: Breathable inert gas
- CO2: Effective but dangerous to humans

Fire Classes:

- Class A (Ordinary combustibles): Water OK
- Class C (Electrical): Non-conductive agents only

Indian Context:

- Data centers use FM-200/Inergen (protect equipment + humans)
- Factory acts mandate fire safety based on size

Exam Tip:

- Data centres: gas-based suppression (FM-200/Inergen)
- Pre-action best for data centres (prevents false discharge)
- Life safety first - evacuate before suppression

Fire Type		Powder	Foam	CO_2	Water	Wet Chemical
Class A	**Solids** (e.g., wood, plastic, paper)	✓	✓	✗	✓	✗
Class B	**Flammable liquids** (e.g., solvents, paint, fuels)	✓	✓	✓	✗	✗
Class C	**Gases** (e.g., butane, propane, LPG)	✓	✗	✗	✗	✗
Class D	**Metals** (e.g., lithium, magnesium)	✓	✗	✗	✗	✗
Electrical	**Equipment** (e.g., computers, servers, TVs)	✓	✗	✓	✗	✗
Class F	**Cooking oils** (e.g., cooking fat, olive oil)	✗	✗	✗	✗	✓
Typical Use Locations		Outdoor locations, garages, welding workshops, forecourts	Schools, offices, hotels, shops, hospitals, apartments	Offices, server rooms	Schools, hospitals, shops, apartment blocks	Kitchens, canteens, restaurants

Personnel Safety

Key Points:

- Life safety ALWAYS > asset protection
- Multiple marked exits
- Regular drills
- Accounting for all personnel
- Special assistance for the disabled
- Emergency response teams
- Crisis management

Indian Context:

- Factory acts require safety measures based on occupancy
- Fire safety codes mandate exits, drills

Exam Tip: LIFE SAFETY FIRST. If a question asks about the conflict between protecting people vs assets → people win EVERY time.

Administrative Controls

Physical Security Order of Operations:

1. Deter
2. Deny
3. Detect
4. Delay
5. Determine
6. Decide

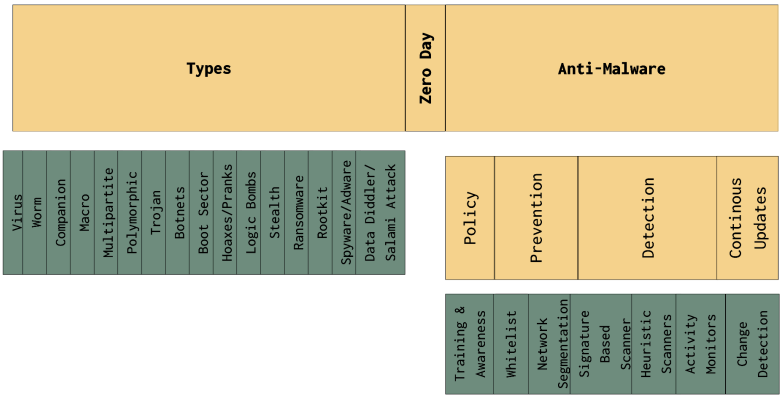
Key Controls:

- Visitor Management: Registration, badges, escorts, time-limited
- Asset Management: Inventory, property passes, cable locks, RFID
- Clean Desk Policy: Lock documents, clear whiteboards, and secure disposal
- Security Awareness: Tailgating prevention, social engineering, and incident reporting

Exam Tip: Physical security = technical + administrative controls. Both are needed for defence-in-depth.

System Vulnerabilities & Countermeasures

Malware Categories



Viruses (Require human action):

- Boot Sector: Infects startup areas
- File Infector: Attaches to executables
- Macro: Embedded in documents
- Polymorphic: Changes code to evade signatures
- Metamorphic: Completely rewrites itself
- Stealth: Hides from detection

Worms (Self-propagate):

- Automatic network spreading
- Exploit vulnerabilities
- Cause network congestion
- Example: WannaCry ransomware worm

Trojans (Masquerade as legitimate):

- No self-replication

- Backdoor access
- Social engineering distribution

Rootkits (Hide presence):

- Kernel-level (Ring 0): Most dangerous, hardest to detect
- User-level (Ring 3): Easier to detect/remove
- Firmware/BIOS: Survive OS reinstall
- Modify system functions to hide

Logic Bombs:

- Trigger on conditions (time/event-based)
- Often, an insider planted
- Difficult to detect before activation

Data Diddler / Salami Attack:

- Very small changes over time
- Evades detection through incremental modifications
- Financial systems (small amounts from many accounts)

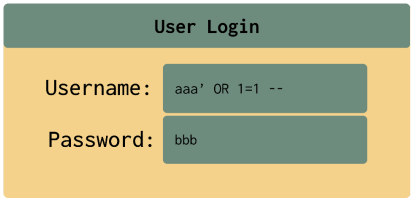
Exam Tip:

- A virus needs human action, a worm self-propagates
- Rootkit at Ring 0 >> Ring 3 (harder to detect/remove)
- Logic bomb = time/event trigger

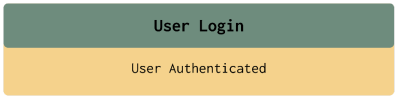
Web Application Vulnerabilities

Injection Attacks:

- SQL Injection: Malicious database queries through input




```
SELECT * FROM users WHERE username = 'aaa' OR 1=1 --' AND password = 'bbb'
SELECT * FROM users WHERE FALSE OR TRUE --' AND password = 'bbb'
SELECT * FROM users WHERE TRUE
```



- Command Injection: OS commands through the application
- LDAP Injection: Directory service manipulation
- XXE Injection: XML parser exploitation

Cross-Site Scripting (XSS):

XSS Type	Description
Persistent / Stored	Injected code is stored on the server and embedded in the HTML page sent to all subsequent users.
Reflected	Injected code is passed to a vulnerable server via a URL and reflected back to the victim.
DOM-based	Client-side Document Object Model (DOM) environment is modified, and malicious code is executed in the browser.

- Stored XSS: Malicious script saved on the server
- Reflected XSS: Script reflected from user input

- DOM-based XSS: Client-side script manipulation
- Exploits the user's trust in the website

Cross-Site Request Forgery (CSRF):

- Forces authenticated users to perform unwanted actions
- Exploits the website's trust in the user's browser
- Prevented by anti-CSRF tokens

Key Distinction:

- XSS: Website trusts user → user attacked
- CSRF: Website trusts browser → website attacked

Security Misconfiguration:

- Default passwords
- Unnecessary services enabled
- Verbose error messages
- Directory listing
- Outdated software

Indian Context:

- E-commerce sites targeted with SQL injection
- Government websites vulnerable to XSS (defacement)

Exam Tip:

- Injection = #1 web vulnerability
- XSS vs CSRF: XSS attacks the user, CSRF attacks the website
- Input validation is critical for all web apps

Covert Channels

Storage Covert Channels:

- Hidden data in file attributes
- Steganography (images, audio)
- DNS tunneling
- Cloud storage sync

Timing Covert Channels:

- Information encoded in timing
- Network packet delays
- CPU usage patterns
- Cache timing attacks

Exam Tip: Covert channels bypass normal security. Difficult to detect. High-security environments (military) are most concerned.

Inference & Aggregation Attacks

Inference Attacks:

- Deduce sensitive info from non-sensitive data
- Database queries revealing patterns
- Metadata analysis
- Traffic analysis

Aggregation Attacks:

- Combine multiple non-sensitive pieces → sensitive information
- Public records building complete profiles
- Social media intelligence

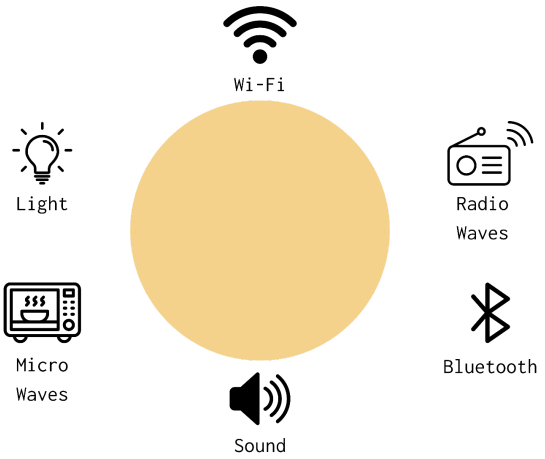
- Data broker compilation

Indian Context:

- National ID databases prevent aggregation attacks
- DPDP Act restricts data combination

Exam Tip: Inference = deduce, Aggregation = combine. Both reveal sensitive data without direct access.

Side-Channel Attacks



Attack Types:

- Power Analysis: Simple (SPA) or Differential (DPA) - reveals crypto keys from smart cards
- Timing Attacks: Execution time reveals secrets
- Electromagnetic Emanations: TEMPEST standard for emission security

- Acoustic Cryptanalysis: Key extraction from keyboard/CPU/printer sounds

Emanations:

- Radio (Bluetooth, Wi-Fi)
- Magnetic (hard drives)
- Light
- Sound

Exam Tip: Side-channel attack implementation, not algorithm. Physical proximity is often required. TEMPEST = classified emission security standard.

Mobile Device Vulnerabilities

ID	Risk
M1	Improper Platform Usage
M2	Insecure Data Storage
M3	Insecure Communication
M4	Insecure Authentication
M5	Insufficient Cryptography
M6	Insecure Authorization
M7	Poor Code Quality
M8	Code Tampering
M9	Reverse Engineering
M10	Extraneous Functionality

Key Threats:

- Platform Fragmentation: Android version fragmentation delays patches

- App Store Risks: Malicious apps, sideloading
- Network Vulnerabilities: Rogue APs, IMSI catchers, Bluetooth/NFC
- Data Leakage: Cached credentials, unencrypted storage, cloud sync

Indian Context:

- Budget devices with delayed/missing updates
- Sideloading common (cost sensitivity)
- Public WiFi is extensive (cafes, malls, transport)

Exam Tip: Mobile devices = untrusted endpoints. MDM is critical for enterprise security.

Industrial Control System (ICS) Vulnerabilities

SCADA (Supervisory Control and Data Acquisition)	DCS (Distributed Control System)	PLC (Programmable Logic Controller)
System architecture that comprises computers, networking, and proprietary devices, as well as graphical interfaces for management of the entire system	Process control system that monitors, controls, and gathers data from components like controllers, sensors, and other devices typically found in large processing facilities	Industrial computer specifically used for the control of manufacturing processes
Used to manage small- and large-scale industrial, infrastructure, and facility processes	Unlike SCADA, which includes local and remote management capabilities, DCS is typically controlled locally	Key features include high reliability, ease of programming, and diagnosis of process problems Often networked with other PLC devices and SCADA systems

Challenges:

- Legacy Systems: 20+ year lifespan, can't patch easily
- No Security by Design: Designed for isolated environments
- Availability Requirements: Can't tolerate downtime for patching
- Proprietary Protocols: No encryption

Air Gap Myths:

- Stuxnet proved that air gaps can be breached
- Maintenance laptops bridge gaps
- Supply chain compromises
- Insider threats

Indian Context:

- Power, water, and manufacturing are critical sectors
- Finally prioritising ICS security after global incidents

Exam Tip: ICS = availability first (unlike IT = confidentiality/integrity first). Air gaps are not foolproof.

Countermeasure Strategies

Defense-in-Depth:

- Perimeter (firewalls, IPS)
- Network segmentation
- Endpoint protection
- Application security
- Data protection
- User awareness

Patch Management:

- Vulnerability assessment/prioritisation
- Test environment validation
- Staged deployment
- Rollback procedures
- Emergency patching

Security Monitoring:

- Log aggregation/analysis
- SIEM
- Network traffic analysis
- User behaviour analytics
- Threat intelligence

Incident Response:

- IR plans
- Trained teams
- Forensic capabilities
- Communication procedures
- Lessons learned

Exam Tip: Defence-in-depth = multiple overlapping controls. Single control failure doesn't compromise security.

Exam Preparation - Quick Reference

Security Models - When to Use

Scenario	Model

Military classified data	Bell-LaPadula
Banking transactions	Clark-Wilson
Data quality/accuracy	Biba
Conflict of interest	Chinese Wall
OS access control	Graham-Denning

Memory Tricks:

- Bell-LaPadula = Confidentiality (no 'i' in both)
- Biba = Integrity (both have 'i')
- Clark-Wilson = Commercial integrity (transactions)
- Chinese Wall = Conflicts (lawyer/consultant)

Cryptography Selection

Need	Solution

Bulk data encryption	AES (symmetric)
Key exchange	Diffie-Hellman or RSA
Password storage	Salted SHA-256+ hash
Digital signatures	RSA or ECC private key
Integrity verification	SHA-256+ hash
Non-repudiation	Digital signature

Key Sizes:

- AES: 128-bit minimum (256-bit for sensitive)
- RSA: 2048-bit minimum (4096-bit for long-term)
- ECC: 256-bit (≈ 3072-bit RSA)
- SHA: SHA-256 minimum

Physical Security Priorities

ALWAYS in this order:

1. Life safety (evacuate people)

2. Asset protection (protect systems)
3. Evidence preservation (forensics)

Exam Tip: If a question presents conflict → life safety wins EVERY time.

Think Like a CISSP

Question Approach:

1. Identify primary concern: Confidentiality, Integrity, or Availability?
2. Consider context: Military, commercial, healthcare, government?
3. Apply appropriate framework: Which model/standard fits?
4. Choose the MOST correct answer: Often, multiple seem right
5. Think like a manager: Risk-based, cost-effective, business-aligned

CISSP Answer Patterns:

- Safety first: Life > assets
- Policy emphasis: Policy answers are often correct
- Comprehensive: Broader solutions are usually right
- Strategic: Long-term implications matter
- Business enablement: Security facilitates business

Common Exam Traps

Avoid These Mistakes:

- Confusing certification (technical) with accreditation (management)
- Mixing up Bell-LaPadula (confidentiality) with Biba (integrity)
- Thinking air gaps are foolproof
- Forgetting shared responsibility in the cloud
- Choosing a technical fix when a policy/process answer exists
- Prioritising assets over life safety

Indian Context - Quick Reference

Regulators:

- RBI: Banking cybersecurity frameworks
- CERT-In: Critical infrastructure directives
- DPDP Act: Data protection obligations

Common Applications:

- Aadhaar: Biometric identity (TPM/TrustZone)
- UPI: Payment security (ECC, TrustZone)
- Digital Signatures: IT Act compliance (PKI)

Unique Challenges:

- Legacy system proliferation
- Cost sensitivity
- Talent shortages
- Regulatory complexity
- BYOD culture
- Public WiFi dependency

Final Exam Tips

Domain 3 = 13% of Exam (Most Technical)

Must Know Cold:

- Ring Model (Ring -1 to Ring 3)
- Bell-LaPadula vs Biba (opposite models)
- Certification vs Accreditation
- Symmetric vs Asymmetric crypto
- TPM vs HSM
- Type 1 vs Type 2 hypervisors
- Cloud shared responsibility
- Fire suppression for data centres
- Life safety priority

Common Question Types:

- "Which model for [scenario]?" → Match the security model to the use case
- "Which crypto for [need]?" → Match algorithm to requirement
- "What's the priority?" → Usually life safety or policy
- "Cloud security responsibility?" → Know customer vs provider split
- "What's the risk?" → Ring 0 > Ring 3, Type 1 > Type 2, etc.

Time Management:

- Domain 3 questions are often scenario-based (longer)
- Don't overthink - first instinct is usually correct
- Flag and return to difficult questions
- Watch for keywords (classified → Bell-LaPadula, transaction → Clark-Wilson)

Conclusion

Domain 3 is the MOST TECHNICAL domain, but mastery here builds the foundation for understanding all other domains. Focus on:

1. Understanding WHY, not just memorising WHAT
2. Matching models to scenarios (practice this!)
3. Thinking strategically (manager mindset, not technician)
4. Knowing security priorities (life safety > assets > evidence)
5. Applying defence-in-depth across all layers

Remember: Good security architecture = right controls, right places, right times, based on sound principles and risk analysis. This is what separates a CISSP from a technician.

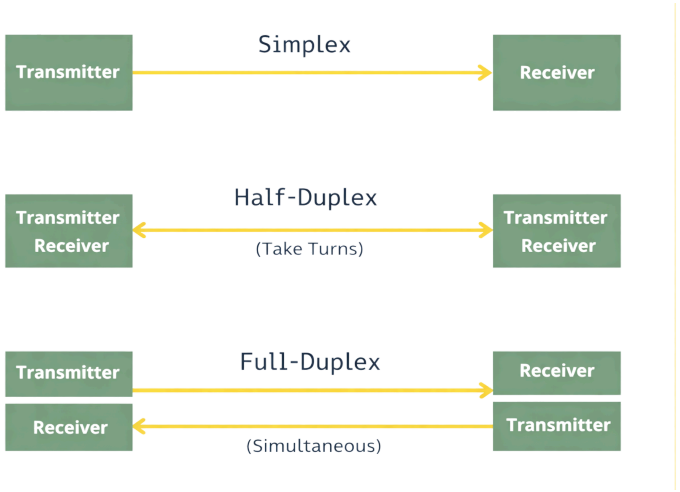
You're architecting security, not just implementing it.

Study Strategy:

1. Read this guide 3x
2. Practice scenario matching (models, crypto, controls)
3. Review Indian context examples
4. Take practice exams
5. Focus on weak areas
6. Rest well before the exam

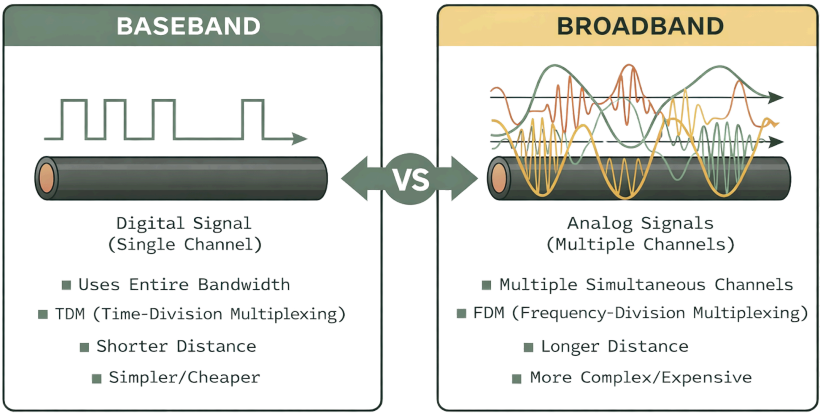
Domain 4: Communication and Network Security

Network Communication Fundamentals



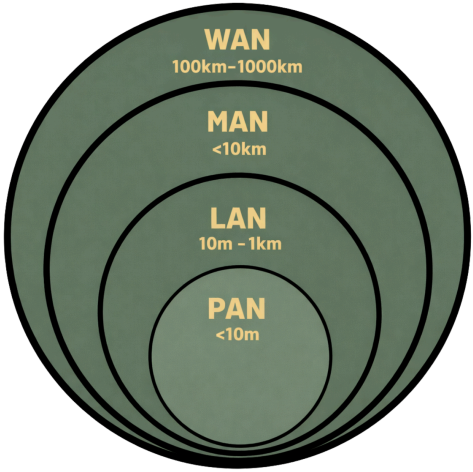
Key Points:

- Simplex: One-way communication only (FM radio broadcasts)
- Half-Duplex: Two-way but alternating (walkie-talkies, CSMA/CD)
- Full-Duplex: Simultaneous two-way (modern Ethernet, VoIP)
- Baseband: Single signal uses entire bandwidth (LANs, 1000base-T)
- Broadband: Multiple signals on different frequencies (WANs, cable internet)



Exam Tip: "Walkie-talkie style" = Half-duplex, "Radio broadcast" = Simplex, "Phone call" = Full-duplex

Network Types and Scope



Key Points:

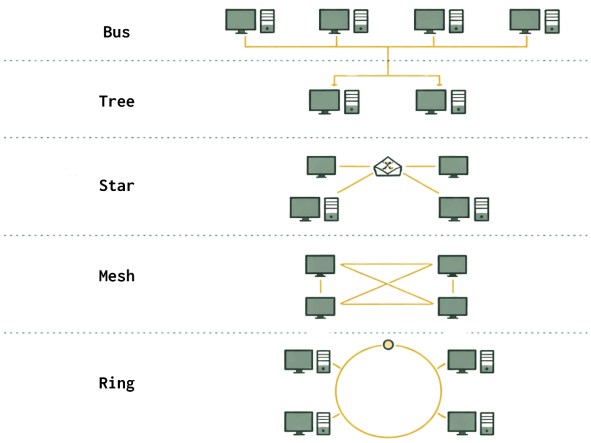
- PAN (Personal Area Network): <10m, Bluetooth/NFC, vulnerable to proximity attacks
- LAN (Local Area Network): Building/campus, high-speed, insider threat concerns
- MAN (Metropolitan Area Network): City-wide, fibre rings, shared medium risks
- WAN (Wide Area Network): Cross-country, carrier infrastructure, requires encryption
- GAN (Global Area Network): Continental, Internet, completely untrusted environment

Trust Boundaries:

- Intranet: Private, internal users only, higher trust, but insider threats exist
- Extranet: Semi-trusted, controlled partner access, strict monitoring needed
- Internet: Public, untrusted, assume hostile environment

Exam Tip: Higher trust ≠ security. Insider threats are significant on LANs and intranets.

Physical LAN Topologies



Key Points:

- Bus: Single cable, any break affects all downstream devices, collision domain issues
- Star: Central switch/hub, single point of failure, but good fault isolation
- Ring: Token passing, circular loop, single break disrupts entire ring
- Tree: Hierarchical, mainframe-based, root failure = total outage
- Mesh: Multiple interconnected paths, high redundancy, expensive, HA systems

Security Implications:

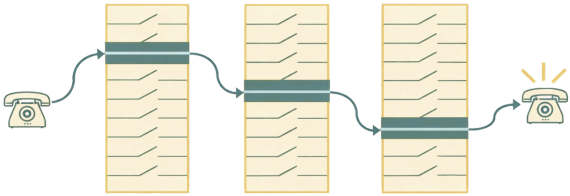
- Bus/Ring: All traffic visible to all devices (high sniffing risk)
- Star with switch: Segmentation possible, better security
- Mesh: Best for availability and redundancy

Exam Tip: Question mentions occurrence of a "collision domain" or "single cable" = Bus topology

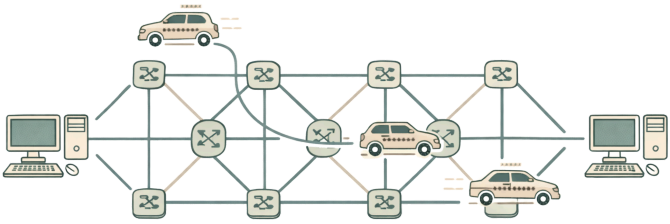
Circuit-Switched vs Packet-Switched Networks

Key Points:

- Circuit-Switched: Dedicated end-to-end path, guaranteed bandwidth, inefficient, legacy PSTN

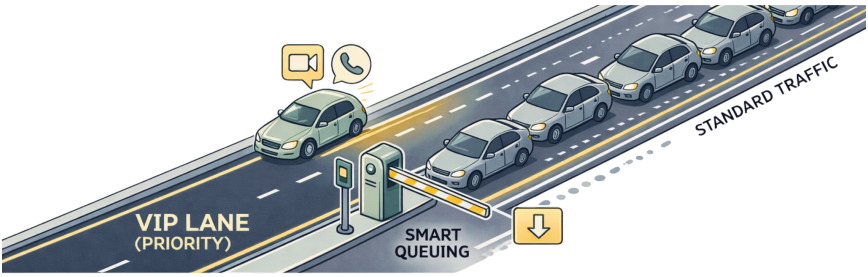


  -
- Packet-Switched: Shared resources, data broken into packets, efficient, best-effort delivery



  -
- QoS (Quality of Service): Configurable feature that allows you to prioritises time-sensitive traffic (VoIP, video) in packet networks

- Modern networks are packet-switched with QoS for real-time applications



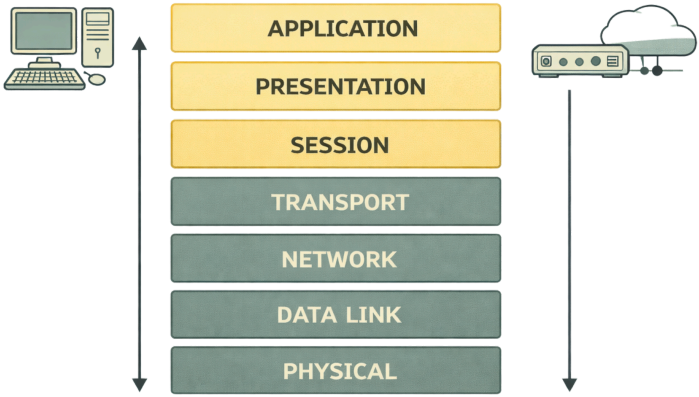
- **Priority Lane:** Quicker delivery for high-priority traffic
- **Smart Queuing:** Prioritizes important data
- **Standard Traffic:** Lower priority for non-real-time traffic

Indian Context:

- BSNL landlines (legacy circuit-switched) vs Reliance Jio 4G/5G (packet-switched)

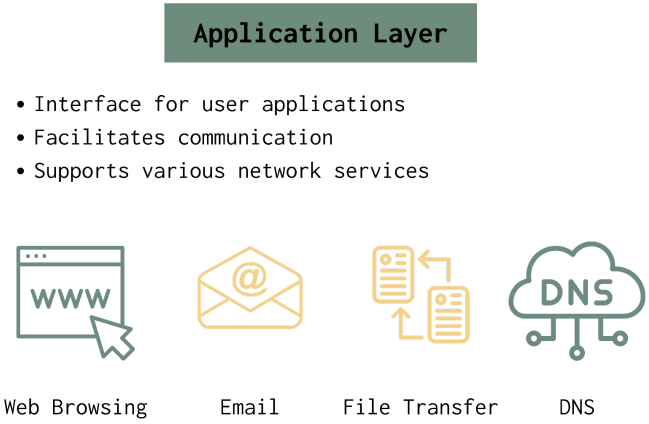
Exam Tip: Circuit = expensive but predictable, Packet = cheap & reliable but needs QoS for real-time

OSI Model (7 Layers)



Mnemonic: Please Do Not Throw Sausage Pizza Away

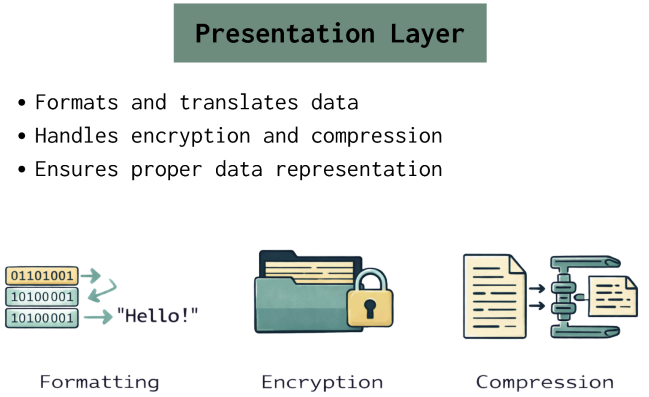
Layer 7 - Application:



- User-facing protocols: HTTP/HTTPS, FTP, SMTP, DNS

- Supports authentication and authorisation at the application level
- Most vulnerable to app-specific attacks

Layer 6 - Presentation:



- Data format conversion, encryption/decryption, compression
- Character encoding (ASCII, Unicode), file formats (JPEG, PNG)
- No dedicated protocols (functions integrated into apps)

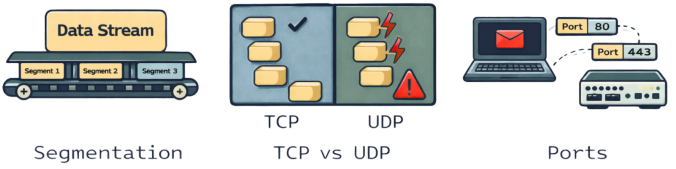
Layer 5 - Session:

- Establishes, manages, and terminates connections
- Handles session management
- Supports synchronization

- Establishes, maintains, and terminates sessions
- Simplex/half-duplex/full-duplex mode management
- Vulnerabilities: Session hijacking, replay attacks

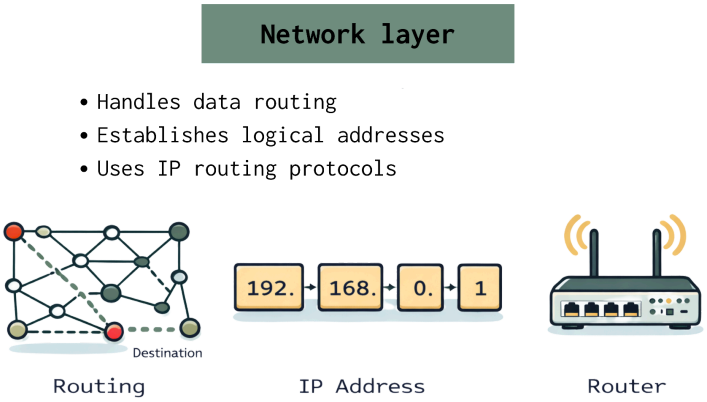
Layer 4 - Transport:

- Ensures reliable data transfer
- Handles end-to-end communication
- Utilizes protocols like TCP and UDP



- TCP: Reliable, connection-oriented, three-way handshake, flow control
- UDP: Fast, connectionless, no guarantees, real-time applications
- Port numbers identify applications (well-known 0-1023, registered 1024-49151, ephemeral 49152-65535)
- Attacks: SYN flood (TCP), Fraggle (UDP amplification)

Layer 3 - Network:



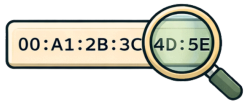
- Logical addressing (IP), routing between networks
- Protocols: IP, ICMP, IPsec, IGMP, routing protocols (OSPF, BGP)
- Routers operate here, making packet forwarding decisions
- Attacks: IP spoofing, routing attacks, DDoS

Layer 2 - Data Link:

Data-link layer

- Handles node-to-node data transfer
- Detects and corrects frame errors
- Manages MAC addressess

Ethernet Frame



MAC Address

Switch

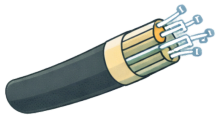
- MAC addresses for local device identification
- Framing, error detection, media access control
- Switches operate here, separate collision domains
- Sublayers: MAC (Media Access Control), LLC (Logical Link Control)
- Attacks: MAC spoofing, ARP poisoning, CAM table overflow

Layer 1 - Physical:

Physical layer

- Transmission media and hardware
- Transfers raw bitstream
- Defines electrical, optical, and radio signals

Twisted Pair



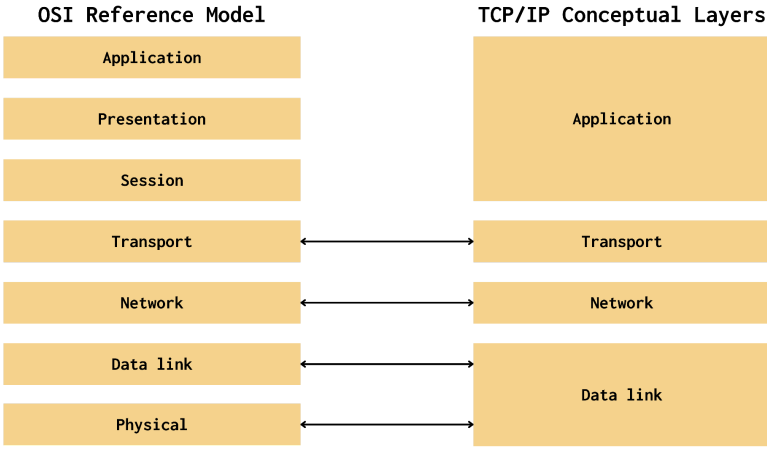
Fiber Optics

Wireless

- Raw bits as electrical/optical/radio signals
- Physical cables, connectors, hubs, repeaters
- Physical topology (bus, star, ring)
- Attacks: Wiretapping, signal jamming, physical access

Exam Tip: Lower layers = speed, upper layers = intelligence. Know which protocols operate at which layer.

TCP/IP Model (4 Layers)



Key Points:

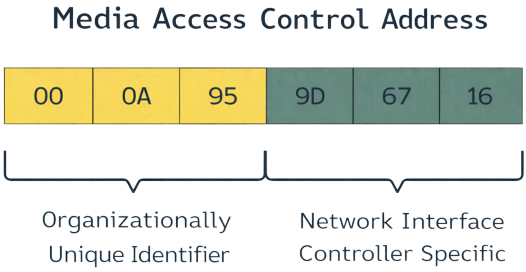
- Network Interface (OSI 1+2): Ethernet, Wi-Fi, ARP, MAC addressing
- Internet (OSI 3): IP, ICMP, routing between networks
- Transport (OSI 4): TCP (reliable) vs UDP (fast)
- Application (OSI 5+6+7): HTTP, DNS, SMTP, all user protocols

Encapsulation Process:

- Data → Segments (Transport) → Packets (Internet) → Frames (Network Interface) → Bits

Exam Tip: TCP/IP = practical reality of the internet, OSI = theoretical teaching model

MAC Addresses



Key Points:

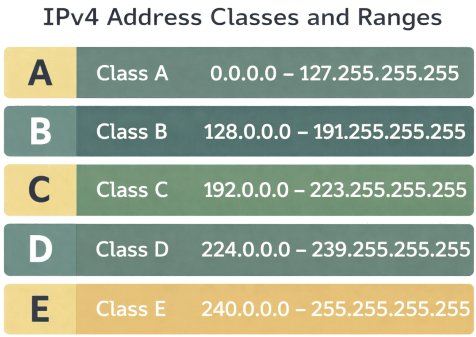
- 48-bit (EUI-48) hardware address: 00:1A:2B:3C:4D:5E
- First 24 bits = OUI (Organizationally Unique Identifier, manufacturer)
- Last 24 bits = device-specific serial number
- EUI-64: 64-bit extended format for IPv6 autoconfiguration
- Layer 2 addressing, local network only

Security Vulnerabilities:

- MAC spoofing trivially bypasses MAC filtering
- Wi-Fi probe requests enable tracking
- ARP poisoning exploits MAC-to-IP mapping trust

Exam Tip: MAC filtering = security through obscurity, weak control. Don't rely on it.

IPv4 Addressing



Key Points:

- 32-bit address (4.3 billion), nearly exhausted
- Dotted decimal notation: 192.168.1.1
- CIDR notation: /24 = 255.255.255.0 subnet mask
- RFC 1918 Private Ranges (memorise these):
    - 10.0.0.0/8 (Class A)
    - 172.16.0.0/12 (Class B)
    - 192.168.0.0/16 (Class C)

Private IP address space

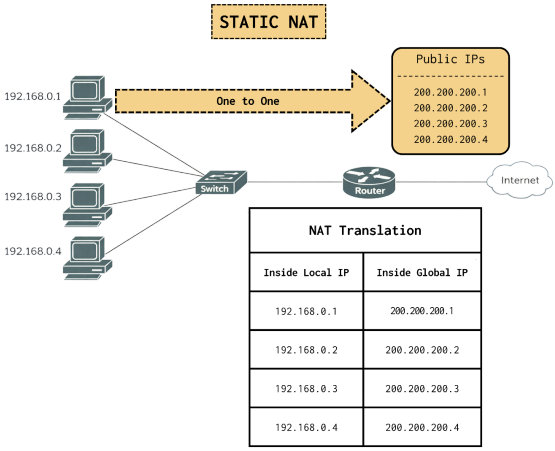
From	To
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255
192.168.0.0	240.0.00 -255.255

Special Addresses:

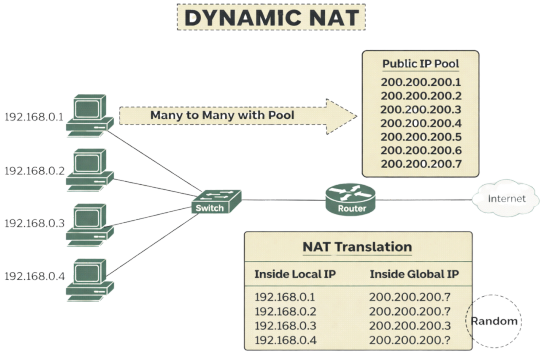
- 127.0.0.0/8: Loopback testing
- 169.254.0.0/16: Link-local (APIPA)
- 255.255.255.255: Limited broadcast

NAT Types:

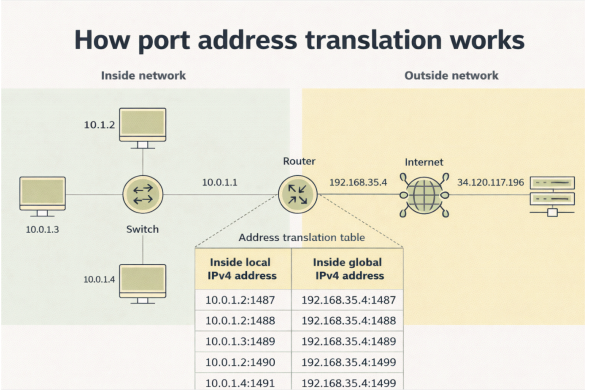
- Static NAT: 1-to-1 mapping (servers needing consistent public IPs)



- Dynamic NAT: Public IP pool for outbound connections



- PAT (Port Address Translation): Many private IPs share one public IP via port numbers



Transmission Methods:

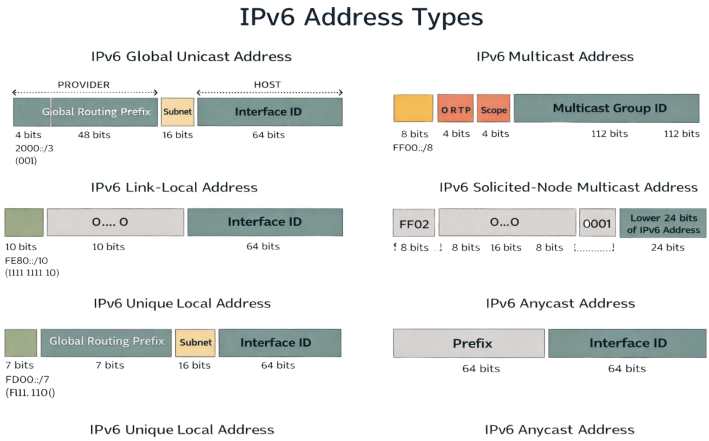
- Unicast: One-to-one communication
- Broadcast: One-to-all in subnet (.255 address)
- Multicast: One-to-many (224.0.0.0 to 239.255.255.255)

Indian Context:

- Banking data centres use private IP ranges with PAT for internet access

Exam Tip: Know RFC 1918 ranges cold. NAT extends IPv4 life but breaks end-to-end connectivity.

IPv6 Addressing



Key Points:

- 128-bit address (340 undecillion addresses)
- Hexadecimal notation: 2001:0db8:0000:0000:0001:0000:0000:0001
- Compression rules: Leading zeros omitted,:: replaces consecutive zero groups (once per address)
- Eliminates the need for NAT, built-in IPsec support

Address Types:

- Unicast: Point-to-point (global, link-local fe80::/10)
- Multicast: One-to-many (ff00::/8), replaces broadcast
- Anycast: Same address on multiple interfaces, routes to the nearest

SLAAC (Stateless Address Autoconfiguration):

- Hosts auto-configure without DHCP using Router Advertisements
- EUI-64 derives the interface ID from the MAC address

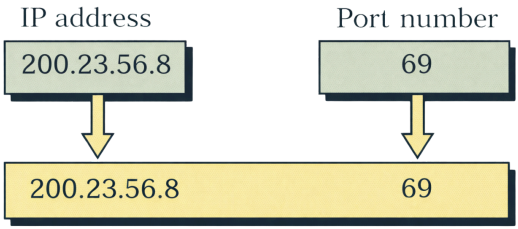
- Privacy extensions use random temporary addresses to prevent tracking

Security Advantages:

- Native IPsec integration (AH and ESP headers)
- End-to-end encryption without NAT complications
- Privacy extensions prevent MAC-based tracking

Exam Tip: IPv6 has NO broadcast, only multicast. SLAAC = plug-and-play addressing.

Ports and Socket Pairs



Socket Pair (Five-Tuple):

1. Source IP address
2. Source port number
3. Destination IP address
4. Destination port number

5. Protocol (TCP or UDP)

Port Categories:

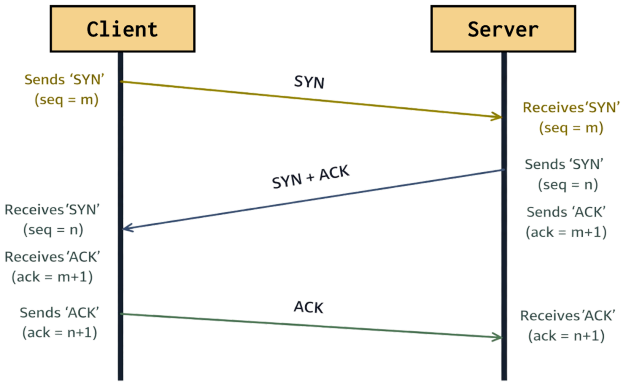
- Well-known (0-1023): HTTP (80), HTTPS (443), SSH (22), DNS (53), SMTP (25)
- Registered (1024-49151): Application-specific assignments
- Ephemeral (49152-65535): Dynamic client-side ports

Common Ports (Memorise):

- FTP: 20 (data), 21 (control)
- SSH: 22
- Telnet: 23
- SMTP: 25
- DNS: 53 (TCP and UDP)
- DHCP: 67 (server), 68 (client)
- HTTP: 80
- POP3: 110
- IMAP: 143
- HTTPS: 443
- RDP: 3389
- L2TP: 1701

Exam Tip: Port scanning reveals services. Firewalls filter by port numbers.

TCP Three-Way Handshake



3-Way Handshaking(for establishing connection)

Connection Establishment:

1. SYN: Client sends a synchronise packet with an initial sequence number
2. SYN-ACK: Server acknowledges and sends its own sequence number
3. ACK: Client acknowledges server's sequence number → ESTABLISHED state

Data Transfer Features:

- Sequence numbering ensures proper ordering
- Acknowledgements confirm receipt (reliability)
- Flow control prevents receiver overflow
- Congestion control adjusts to network conditions
- Retransmission on timeout or packet loss

Connection Termination (Four-Way):

1. FIN from initiator
2. ACK from receiver

3. FIN from receiver
4. ACK from initiator → TIME_WAIT → CLOSED

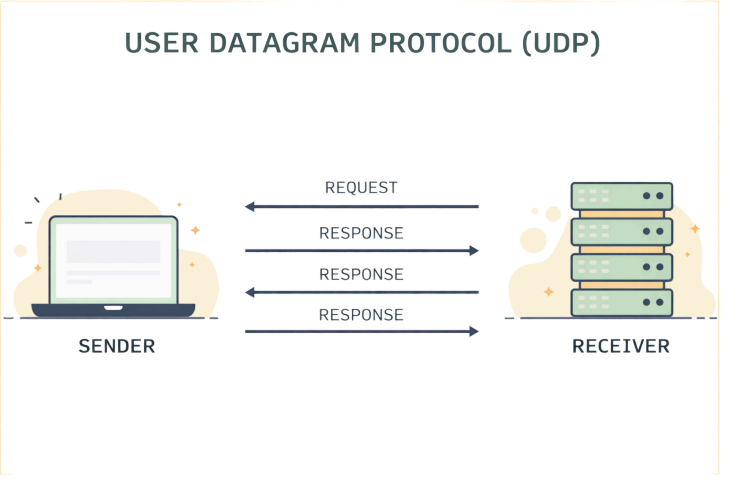
Attacks:

- SYN Flood: Exhaust server resources with incomplete handshakes
- Sequence Number Prediction: Hijack sessions by predicting the next sequence number

Exam Tip: TCP = reliable but slower. UDP = fast but no guarantees.

Key Network Protocols

UDP (User Datagram Protocol):



- Connectionless, no handshake, 8-byte header
- No reliability, ordering, or flow control
- Best for real-time apps: VoIP, streaming, gaming, DNS queries

- Attacks: Fraggle (amplification via spoofed source)

ICMP (Internet Control Message Protocol):

- Network layer error reporting and diagnostics
- Ping: Echo Request/Reply tests reachability
- Traceroute: Uses TTL expiration (ICMP Time Exceeded messages)
- Path MTU Discovery: Uses "Don't Fragment" + ICMP Fragmentation Needed
- Security risks: Reconnaissance, ICMP flooding, Smurf attacks (amplification)

DHCP (Dynamic Host Configuration Protocol):

- Automatic IP configuration: IP address, subnet mask, gateway, DNS servers
- DORA process: Discover, Offer, Request, Acknowledge
- Ports: 67 (server), 68 (client) over UDP
- Predecessor: BOOTP (static mappings, diskless boot)

DNS (Domain Name System):

- Translates domain names to IP addresses
- Port 53 (UDP for queries, TCP for zone transfers). We also have DNS over HTTPS, which uses port 443)
- Hierarchical: Root servers → TLDs → authoritative servers
- Attacks: DNS poisoning, DDoS on DNS infrastructure

Exam Tip: "I" protocols usually Layer 3 (IP, ICMP, IGMP). DHCP uses broadcast initially.

WAN Technologies

Legacy Carrier Lines:

- T1: 1.544 Mbps (US), 24 channels of 64 Kbps
- E1: 2.048 Mbps (Europe/India), 30 channels of 64 Kbps
- T3: 44.736 Mbps, E3: 34.368 Mbps
- Used for dedicated point-to-point circuits

Frame Relay:

- Layer 2 packet-switched, variable-length frames
- NO error correction (relies on reliable digital networks)
- Virtual circuits (PVCs and SVCs), DLCI addressing
- CIR (Committed Information Rate) guarantees

X.25:

- Grandfather of packet-switching (1970s)
- Extensive hop-by-hop error correction (reliable but slow)
- Used for financial transactions (ATMs, POS) due to reliability

ATM (Asynchronous Transfer Mode):

- Fixed 53-byte cells (5 header, 48 data)
- Low latency, predictable, designed for voice/video/data
- Expensive, used in telecom backbones

MPLS (Multiprotocol Label Switching):

- Layer 2.5, label-based forwarding (faster than IP routing)
- Label Switched Paths (LSPs) for traffic engineering
- MPLS VPNs provide secure site-to-site connectivity
- QoS capabilities, traffic engineering
- Used by enterprises and ISPs for the backbone

SD-WAN (Software-Defined WAN):

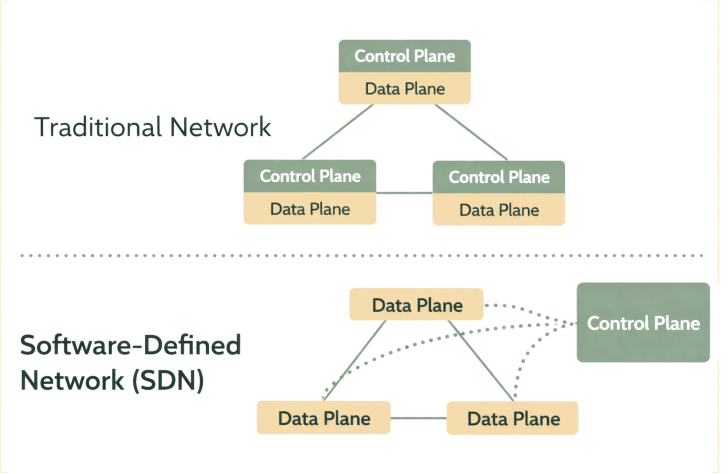
- Replaces expensive MPLS with commodity internet circuits
- Centralised policy management, application-aware routing
- Intelligent path selection, real-time failover
- Integrated security (IPsec, firewall, SWG)
- Cost reduction of 50-70% while increasing bandwidth

Indian Context:

- Indian banks migrated from X.25 → Frame Relay → MPLS → SD-WAN
- Cost savings and performance improvements drive SD-WAN adoption

Exam Tip: Frame Relay = fast, no error correction. X 25 = slow, reliable. MPLS = labels, not IPs.

Converged Protocols and Emerging Technologies



VoIP (Voice over IP):

- Packet-based voice over IP networks
- Uses UDP for real-time delivery (low-latency prioritised)
- Protocols: SIP (call setup), RTP (media), H.323 (legacy)
- Requires QoS to minimise jitter, latency, and packet loss
- Attacks: Eavesdropping, toll fraud, DoS

SDN (Software-Defined Networking):

- Separates the control plane from the data plane
- Centralised controller programs network behaviour
- OpenFlow protocol for switch communication
- Dynamic provisioning, vendor independence
- Essential for cloud and datacenter operations

Storage Protocols:

- iSCSI: Block storage over TCP/IP networks
- FCoE (Fibre Channel over Ethernet): High-speed without TCP/IP overhead

- FCIP: Tunnels Fibre Channel over IP for WAN

Industrial Protocols:

- DNP3: SCADA systems for utilities (power, water, gas)
- Security is critical for infrastructure protection

Exam Tip: SDN centralised control vs traditional distributed routing. VoIP needs QoS.

Wireless Standards (802.11)

IEEE Standard	WiFi Gen	Year	Frequency	Max PHY Data Rate	Max Range
802.11	–	1997	2.4 GHz	2 Mbps	20m (indoor) 100m (outdoor)
802.11a	–	1999	5 GHz	54 Mbps	35m (indoor) 120m (outdoor)
802.11 b	–	1999	2.4 GHz	11 Mbps	35m (indoor) 140m (outdoor)
802.11 g	–	2003	2.4 GHz	54 Mbps	38m (indoor) 140m (outdoor)
802.11 n	WiFi 4	2009	2.4/5 GHz	600 Mbps	70m (indoor) 250m (outdoor)
802.11 ac	–	2013	5 GHz	6.9 Gbps	35m (indoor)
802.11 ad	–	2012	2.4 GHz	8.1 Mbps	3.3m (indoor)
802.11 ah	WiFi 5	2009	2.4/5 GHz	347 Mbps	1km
802.11 ac	–	2013	5 GHz	9.9 Gbps	35m (indoor)
802.11 ad	–	2017	8.1 Gbps	347 Mbps	3.3m (indoor)
802.11 ah	WiFi 6	2019	2.4/5/6 GHz	9.6 Gbps	33m (indoor)
802.11 ax	–	2021	60 Gbps	603 Gbps	30m (indoor) 120m (outdoor)
802.11 ay	–	2024	46.1 Gbps	46.1 Gbps	30m (indoor) 120m (outdoor)

Standards Evolution:

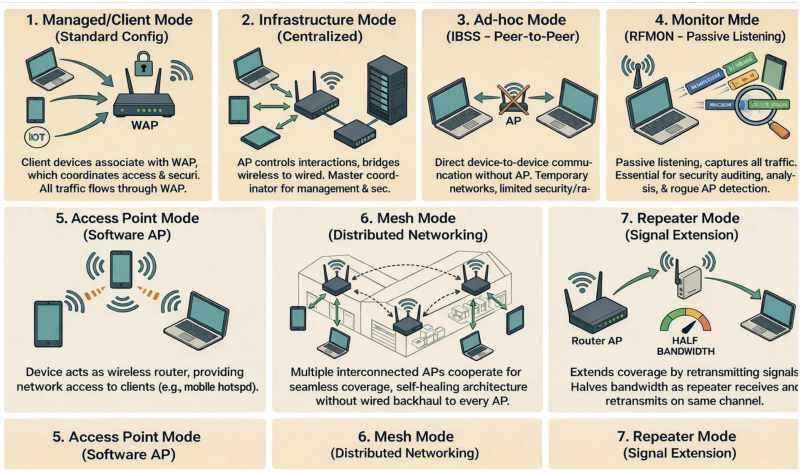
- 802.11b (1999): 11 Mbps, 2.4 GHz, widespread adoption
- 802.11a (1999): 54 Mbps, 5 GHz, shorter range
- 802.11g (2003): 54 Mbps, 2.4 GHz, backwards compatible with b
- 802.11n (2009): 200+ Mbps, dual-band, MIMO technology

- 802.11ac (2013): 1+ Gbps, 5 GHz only, MU-MIMO (Wi-Fi 5)
- 802.11ax (2019): 9.5 Gbps, OFDMA, dual-band/6 GHz (Wi-Fi 6/6E)

Frequency Trade-offs:

- 2.4 GHz: Better range, more interference, lower speeds
- 5 GHz: Higher speeds, shorter range, less congestion
- 6 GHz: Wi-Fi 6E, highest speeds, limited penetration

NIC Operating Modes:



- Managed/Client: Standard mode connecting to access points
- Infrastructure: AP coordinates all communication
- Ad-hoc (IBSS): Peer-to-peer without AP (limited security)
- Monitor (RFMON): Passive packet capture for security auditing
- Mesh: Distributed, self-healing networks

SSID and Network Identification:

- SSID: Network name (up to 32 characters), broadcast in beacons
- BSSID: MAC address of specific AP
- ESSID: Name spanning multiple APs for roaming
- Hidden SSID = security through obscurity (ineffective)
- MAC filtering = easily bypassed via spoofing

Exam Tip: 2.4 GHz = range, 5 GHz = speed. MIMO = multiple antennas for throughput.

Wireless Security Evolution

WEP (Wired Equivalent Privacy):

- Original 802.11 security, RC4 encryption
- 24-bit IV reuse vulnerability
- Cracked in minutes with tools (Aircrack-ng)

- NEVER use WEP - completely broken

WPA (Wi-Fi Protected Access):

- Interim fix for WEP, still uses RC4
- TKIP (Temporal Key Integrity Protocol) for dynamic keys
- Dictionary attacks against weak PSK passphrases
- Superseded by WPA2, not recommended

WPA2 (Wi-Fi Protected Access 2):

- AES-CCMP encryption (robust, no known breaks)
- PSK/Personal: Pre-shared key for home/SOHO
- Enterprise (802.1X): RADIUS authentication for business
- Vulnerabilities: KRACK attack against handshake (mitigated by patches)
- Still widely deployed and considered secure with patches

WPA3 (Wi-Fi Protected Access 3):

- SAE (Simultaneous Authentication of Equals) replaces PSK
- Dragonfly handshake prevents offline dictionary attacks.
- Forward secrecy: Past traffic is secure even if the key is compromised
- Individual data encryption prevents device-to-device eavesdropping
- Management Frame Protection (802.11w) mandatory
- 192-bit encryption for Enterprise mode

802.1X/EAP Enterprise Authentication:

- Port-based network access control (wired and wireless)
- Three components: Supplicant (client), Authenticator (AP/switch), Authentication Server (RADIUS)

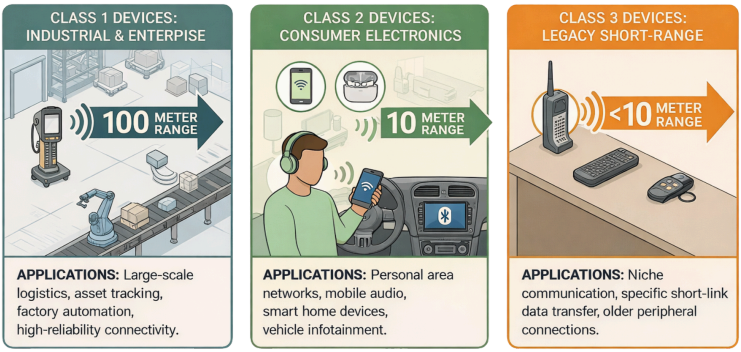
- EAP Methods:
    - EAP-TLS: Most secure, requires client and server certificates
    - PEAP: Encrypted tunnel, server certificate only
    - EAP-TTLS: Similar to PEAP
    - EAP-MD5: Weak, not recommended
    - LEAP: Cisco's proprietary, known vulnerabilities

Indian Context:

- Corporate offices use WPA2/WPA3-Enterprise with RADIUS
- Homes use WPA2/WPA3-Personal with strong passphrases

Exam Tip: WEP < WPA < WPA2 < WPA3. Enterprise = 802.1X. Hidden SSID and MAC filtering = weak.

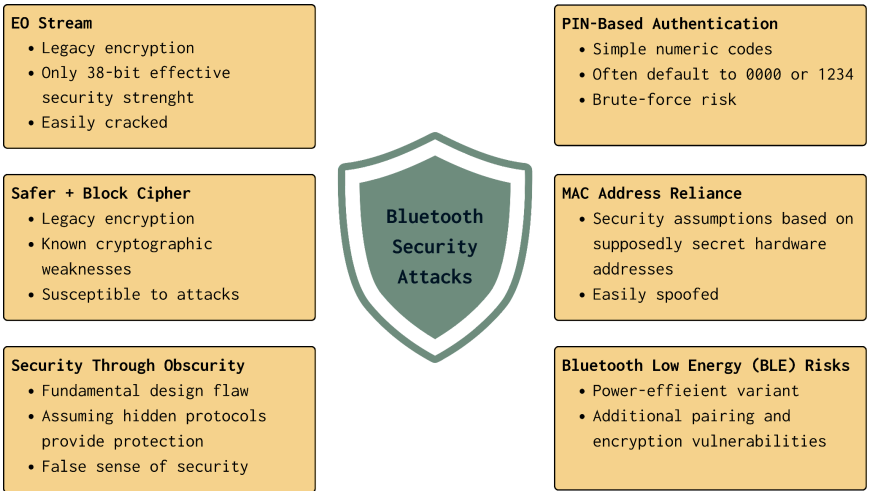
Bluetooth and Short-Range Wireless



Bluetooth (802.15.1):

- 2.4 GHz frequency, short-range Personal Area Network
- Classes: Class 3 (<10m), Class 2 (10m), Class 1 (100m)
- BLE (Bluetooth Low Energy): Low power for IoT, wearables
- Often uses weak default PINs (0000, 1234)
- Plaintext transmission is by default unless encrypted

Bluetooth Attacks:



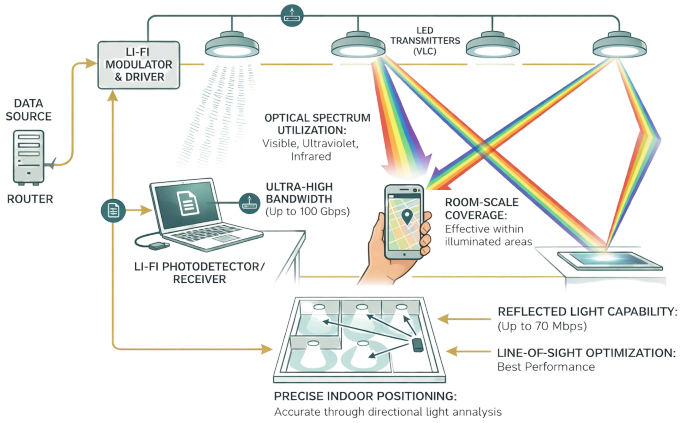
- Bluesniffing: Passive interception of data
- Bluesmacking: DoS attack flooding the device
- Bluejacking: Unsolicited spam messages
- Bluesnarfing: Unauthorised data access (contacts, messages)
- Bluebugging: Complete device takeover, eavesdropping

ZigBee (802.15.4):

- Ultra-low power mesh networking for IoT
- 20-250 Kbps data rates, 10-100m range

- AES-128 encryption (when properly configured)
- Battery life in months/years
- Self-organising, self-healing mesh networks
- Vulnerabilities often come from default keys and poor commissioning

Li-Fi (Light Fidelity):



- Data transmission via LED light modulation
- Speeds up to 100 Gbps (laboratory)
- Inherent security: Light doesn't penetrate walls
- Line-of-sight limitations
- Safe for hospitals, aircraft (no RF interference)
- Higher deployment costs than Wi-Fi

RFID and NFC:

- RFID: Passive (no battery) or Active (battery-powered) tags
- Privacy concerns: Tracking, profiling without consent
- NFC: Very short range (<4cm), used for payments (Google Pay, contactless cards)

- Attacks: NFC relay attacks extending range

Exam Tip: Bluetooth Class 1 = longest range = highest security risk. Disable when not needed.

Cellular Networks

Key Points:

- 3G: 2 Mbps, 100-500ms latency, basic mobile internet
- 4G (LTE): 200 Mbps, 20-30ms latency, enabled streaming and video calls
- 5G: 5-20 Gbps, <10ms latency, IoT and real-time apps
- Cell-based coverage, frequency reuse patterns
- Seamless handoffs between cells during movement
- Higher frequencies (5G mmWave) = higher speeds but shorter range, requires denser deployment

Security Evolution:

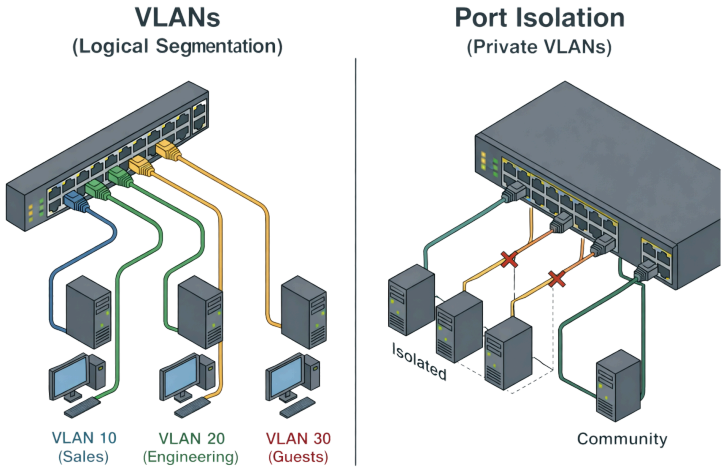
- 3G: Stronger SIM authentication
- 4G: LTE encryption
- 5G: Improved mutual authentication, network slicing security

Indian Context:

- Reliance Jio and Bharti Airtel 5G deployments in metros
- Coverage vs speed trade-offs in rural areas

Exam Tip: Lower latency is needed for real-time apps. 5G = ultra-fast but short range.

Network Devices



Layer 1 Devices (Physical):

- Repeater: Amplifies signal, extends distance, no intelligence
- Hub: Multi-port repeater, broadcasts to all ports, half-duplex
- Security issue: All traffic visible to all devices (easy sniffing)

Layer 2 Devices (Data Link):

- Bridge: Connects two network segments, filters by MAC address
- Switch: Multi-port bridge, each port = separate collision domain
- Uses the MAC address table to forward frames intelligently
- Full-duplex reduces collisions
- VLANs: Virtual LANs for logical segmentation (max 4094 VLANs)

- VXLAN: Cloud-scale VLAN for tenant isolation (millions of networks)
- Port Security: MAC address filtering per port (sticky MAC)
- SPAN Port: Switch Port Analyser mirrors traffic for monitoring/IDS

Layer 3 Devices (Network):

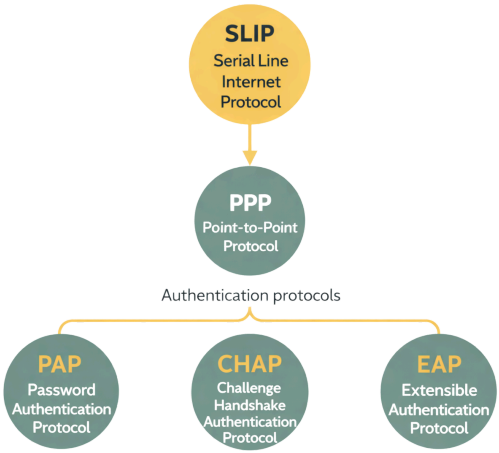
- Router: Forwards packets based on IP addresses
- Connects different networks (LAN to WAN)
- Separates broadcast domains
- Control Plane: Builds routing tables (RIB → FIB)
- Forwarding Plane: Moves packets based on FIB

Routing Types:

- Static: Manual configuration, fixed paths
- Dynamic: Auto-learn routes (RIP, OSPF, BGP)
- Default Gateway: Routes unknown destinations to the ISP

Exam Tip: Hub broadcasts = security risk. Switch = MAC-based forwarding. Router = IP-based routing.

Authentication Protocols



PAP (Password Authentication Protocol):

- Sends username/password in cleartext
- Extremely insecure, vulnerable to eavesdropping
- Legacy protocol should never be used

CHAP (Challenge-Handshake Authentication Protocol):

- Challenge-response mechanism using hash (MD5)
- The password is transmitted over the network
- Server sends random challenge → Client hashes challenge+password → Server verifies
- Prevents replay attacks (challenge changes each time)
- Limitation: Server stores plaintext passwords

EAP (Extensible Authentication Protocol):

- Framework supporting multiple authentication methods
- Used with 802.1X for network access control
- EAP-MD5: Weak, not recommended

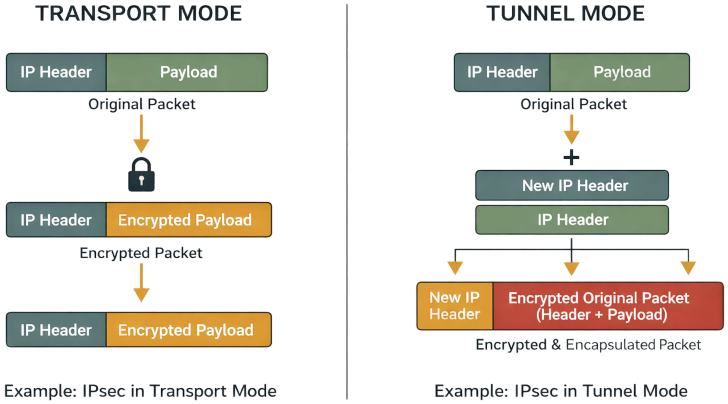
- EAP-TLS: Most secure, mutual authentication with certificates
- PEAP: Encrypted TLS tunnel, server certificate only
- EAP-TTLS: Similar to PEAP
- LEAP: Cisco's proprietary, known vulnerabilities

802.1X Port-Based Access Control:

- Three components:
    1. Supplicant: Client device requesting access
    2. Authenticator: Network device (switch/AP) controlling access
    3. Authentication Server: RADIUS server validating credentials
- Blocks network access until authentication succeeds
- Integrates with existing AAA infrastructure

Exam Tip: PAP = plaintext and pathetic. CHAP = challenge-based hashing. EAP-TLS = strongest.

VPN Protocols and Technologies



VPN Fundamentals:

- Creates a secure tunnel through untrusted networks
- Encapsulation: One protocol wrapped inside another
- Transport Mode: Encrypts payload only, original IP header intact
- Tunnel Mode: Encrypts the entire packet, including the header; a new IP header is added

VPN Configurations:

- Always-On VPN: Auto-reconnects every 2 minutes (mobile devices)
- Split Tunnel: Only corporate traffic via VPN, personal traffic direct
- Full Tunnel: All traffic routed through VPN (geo-restriction bypass)

PPTP (Point-to-Point Tunnelling Protocol):

- Based on PPP, Layer 2, TCP port 1723
- Initial negotiation unencrypted (exposes credentials)
- Considered obsolete and insecure
- Do not use PPTP

L2TP (Layer 2 Tunnelling Protocol):

- Combines PPTP and Cisco L2F

- Layer 2, UDP port 1701
- No native encryption - requires IPsec pairing (L2TP/IPsec)
- Supports multiple Layer 3 protocols

IPsec (Internet Protocol Security):

- Suite of protocols for Layer 3 security
- Native to IPv6, add-on for IPv4
- AH (Authentication Header): Integrity, authentication, no confidentiality
- ESP (Encapsulating Security Payload): Confidentiality, integrity, authentication
- IKE (Internet Key Exchange): Negotiates crypto parameters (AES, 3DES, SHA)
- Security Associations (SAs): Simplex (one-way), identified by SPI
- NAT issues: NAT-T (NAT Traversal) enables IPsec through NAT

SSL/TLS:

- Secures web traffic (HTTPS), email (SMTPS), and VoIP
- SSL v3.0 is obsolete; use TLS 1.2 or TLS 1.3
- Certificate-based authentication (X.509, PKI)
- Operates at multiple layers (4-7)

Indian Context:

- IT companies use split-tunnel VPNs for work-from-home
- Banking apps use TLS for secure transactions

Exam Tip: IPsec = gold standard VPN. Transport mode = host-to-host. Tunnel mode = site-to-site.

Remote Access Technologies

Legacy Remote Access:

- ISDN: Digital over POTS lines, superseded by broadband
- DSL: Last-mile over copper, still used in rural India
- Cable Modems: Shared bandwidth via coax

Modern Remote Access:

- RDP (Remote Desktop Protocol): Microsoft's proprietary, TCP/UDP port 3389
- VNC (Virtual Network Computing): Cross-platform screen sharing
- SSH (Secure Shell): Encrypted terminal access, port 22

VDI (Virtual Desktop Infrastructure):

- Thin Clients: Diskless workstations, apps run on servers
- Access via HTTP (80) or HTTPS (443)
- Centralised management, reduced hardware costs
- Used by Indian government offices and large corporations

Security Best Practices:

- Always use secure conduits: VPN, SSH, TLS
- Implement MFA for remote access
- Monitor and log all remote sessions

Exam Tip: RDP = 3389. Thin clients reduce endpoint security risks.

Network Security Technologies

Firewalls:

- Packet Filtering: Layer 3/4, inspects headers (IP, ports)
- Stateful Inspection: Tracks connection state (TCP handshake)
- Application Layer: Layer 7, deep packet inspection

- Next-Gen Firewall (NGFW): IPS, DPI, application awareness, threat intelligence
- Placed at network perimeters, DMZ boundaries

IDS/IPS (Intrusion Detection/Prevention System):

- IDS: Detects and alerts on suspicious traffic (passive)
- IPS: Detects and blocks attacks (inline, active)
- NIDS/NIPS: Network-based monitoring
- HIDS/HIPS: Host-based monitoring
- Signature-based vs anomaly-based detection

Proxies:

- Forward Proxy: Client-side, caches content, filters requests
- Reverse Proxy: Server-side, load balancing, WAF functionality
- Transparent Proxy: No client configuration needed

Content Distribution Networks (CDN):

- Geographically distributed caching servers
- Reduces latency, improves performance
- DDoS protection, load balancing
- Examples: Cloudflare, Akamai

NAC (Network Access Control):

- Automated policy enforcement before granting access
- Checks device posture: AV updates, patches, firewall status
- Quarantines non-compliant devices

Indian Context:

- NCIIPC guidelines for financial institutions require multi-layered defences
- Banks implement firewalls, IPS, and NAC for compliance

Exam Tip: Stateful firewall = tracks connections. IDS = alerts, IPS = blocks.

Third-Party Connectivity

Key Points:

- Medium enterprises: 20+ third parties
- Large orgs: 200+ third-party connections
- Many never interact with IT security directly

Required Documentation:

- MOU (Memorandum of Understanding): General agreement
- MOA (Memorandum of Agreement): Formal terms
- ISA (Interconnection Security Agreement): Security requirements

Connection Methods:

- VPN tunnels for secure communication
- Leased lines for dedicated connectivity
- Extranet for controlled partner access

Risk Management:

- Conduct thorough risk assessments
- Verify third-party security posture

- Continuous monitoring and auditing
- Ensure compliance with organisational policies

Exam Tip: Third-party risk is significant. Formal agreements and monitoring are essential.

Communication Technologies

Instant Messaging (IM):

- Real-time text communication
- Protocols: IRC, XMPP, proprietary (WhatsApp, Telegram)
- Security concerns: Plaintext transmission, limited encryption, privacy issues
- Only 2/18 major IM apps rated "nothing of concern" for privacy

Web Conferencing:

- Platforms: Zoom, Teams, WebEx, Google Meet
- TCP/IP-based, real-time multicast
- Security: Can bypass controls using SSL/TLS tunnels
- Requires proper hardening and policy alignment

VoIP (Voice over IP):

- Packet-based voice uses UDP for real-time delivery
- Protocols: SIP (call setup), RTP (media), H.323 (legacy)
- Codecs: G.711, G.729 (compression vs quality)
- Security: Eavesdropping, toll fraud, DoS attacks
- Requires QoS for quality (minimise jitter, latency, packet loss)

Indian Context:

- WhatsApp dominates IM in India
- COVID-19 drove Zoom adoption for education and business

Exam Tip: VoIP needs QoS. Most IM apps lack strong security.

Common Network Attacks

TCP/UDP Attacks:

- SYN Flood: Exhausts server resources with incomplete handshakes
    - Mitigation: SYN cookies, rate limiting, proxy protection
- Fraggle: UDP amplification via spoofed source to DNS/NTP servers
- Smurf: ICMP broadcast amplification (largely mitigated)
- Sequence Number Prediction: Session hijacking via predictable TCP sequence

Layer 2 Attacks:

- MAC Spoofing: Impersonate legitimate devices
- ARP Poisoning: Manipulate MAC-to-IP mappings for MitM
- CAM Table Overflow: Flood switch MAC table to force broadcast mode
- VLAN Hopping: Escape VLAN segmentation

Layer 3 Attacks:

- IP Spoofing: Forge source IP addresses
- ICMP Attacks: Ping of Death, ICMP flooding, redirect attacks

- Routing Attacks: BGP hijacking, route injection

Application Layer Attacks:

- DDoS (Distributed Denial of Service): Overwhelm services
- DNS Attacks: Poisoning, amplification, tunnelling
- Man-in-the-Middle: Intercept/modify communications
- Session Hijacking: Take over authenticated sessions

Mitigation Strategies:

- Multi-layered defence (firewalls, IPS, NAC)
- Ingress/egress filtering (prevent spoofing)
- Rate limiting and traffic shaping
- DDoS protection services (cloud scrubbing)
- Network segmentation and least privilege
- Monitoring and anomaly detection

Indian Context:

- NCIIPC guidelines for critical infrastructure protection
- Banking institutions require resilience testing against attack types

Exam Tip: Know attack mechanisms and appropriate mitigations for each layer.

Key Protocols Summary

Critical Ports (Memorise):

- FTP: 20/21 (TCP)
- SSH: 22 (TCP)

- Telnet: 23 (TCP)
- SMTP: 25 (TCP)
- DNS: 53 (TCP/UDP)
- DHCP: 67/68 (UDP)
- TFTP: 69 (UDP)
- HTTP: 80 (TCP)
- POP3: 110 (TCP)
- NTP: 123 (UDP)
- IMAP: 143 (TCP)
- SNMP: 161/162 (UDP)
- HTTPS: 443 (TCP)
- SMTPS: 465 (TCP)
- Syslog: 514 (UDP)
- LDAP: 389 (TCP)
- LDAPS: 636 (TCP)
- L2TP: 1701 (UDP)
- PPTP: 1723 (TCP)
- RDP: 3389 (TCP/UDP)

Protocol Characteristics:

- TCP: Reliable, connection-oriented, overhead
- UDP: Fast, connectionless, no guarantees
- ICMP: Network diagnostics, no ports
- ARP: MAC-to-IP resolution, Layer 2
- DHCP: Dynamic IP assignment
- DNS: Name resolution, hierarchical

Exam Tip: Know well-known ports. TCP vs UDP usage drives protocol selection.

Indian Regulatory and Compliance Context

Key Points:

- IT Act 2000: Legal framework for electronic transactions and cybercrime
- CERT-In: National incident response, mandatory reporting
- RBI Cyber Security Framework: Banking sector requirements
- NCIIPC: Critical infrastructure protection
- TRAI: Telecom regulations and security
- Data Protection Bill: Privacy and data localisation (upcoming)
- SEBI: Securities market cybersecurity guidelines

Compliance Requirements:

- Data localisation for payment systems (RBI)
- Incident reporting to CERT-In within 6 hours
- Regular security audits and penetration testing
- Network segregation and monitoring

Exam Tip: Understand that regional regulations (like RBI, SEBI) add layers to global frameworks.

CISSP Exam Strategy for Domain 4

High-Yield Topics:

1. OSI model layer functions and protocols
2. TCP/IP model vs the OSI model
3. TCP three-way handshake and attacks (SYN flood)
4. IPv4 vs IPv6 addressing and security
5. Wireless security evolution (WEP → WPA → WPA2 → WPA3)
6. VPN protocols (IPsec modes, PPTP vs L2TP)
7. Authentication protocols (PAP, CHAP, EAP methods)
8. Network devices and OSI layers

9. Common ports and protocols
10. Network attacks and mitigations

Common Exam Traps:

- SSL vs TLS (always think TLS)
- Hidden SSID and MAC filtering (security through obscurity = weak)
- PPTP (obsolete, don't recommend)
- NAT as security control (incidental protection, not primary)
- WEP (never use, completely broken)

Quick Decision Trees:

- Speed critical? → UDP, not TCP
- Reliability critical? → TCP, not UDP
- Wireless security? → WPA3 > WPA2 > WPA (never WEP)
- VPN protocol? → IPsec > L2TP/IPsec (never PPTP)
- Enterprise wireless? → 802.1X/EAP-TLS
- Preventing eavesdropping? → Encryption (WPA3, IPsec, TLS)
- Network segmentation? → VLANs, firewalls, subnets

Memory Aids:

- OSI Layers: Please Do Not Throw Sausage Pizza Away
- PAP: Plaintext And Pathetic
- CHAP: Challenge-based Hashing Authentication Protocol
- TCP: Transmission Control (reliable), UDP: Uncontrolled Delivery (fast)

Exam Mindset:

- Know WHY each technology exists and what problem it solves

- Understand security implications at each OSI layer
- Focus on modern best practices (TLS, not SSL, WPA3, not WEP)
- Think defence-in-depth: Multiple layers of security
- Balance security with usability and business requirements

CISSP Domain 5: Identity and Access Management (IAM)

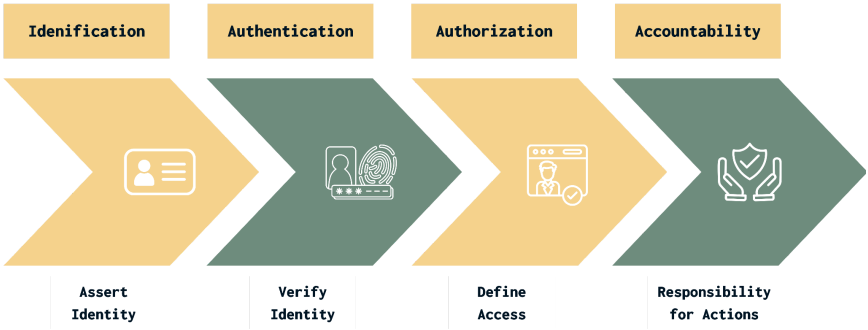
Chapter Overview

Key Points:

- IAM determines who gets access to what resources and when
- IAAA framework: Identification, Authentication, Authorisation, Accountability
- Critical for both external threat protection and insider risk management
- Evolved from simple passwords to sophisticated multi-factor authentication
- Essential for compliance, audit trails, and forensic investigation
- Represents 13% of the CISSP exam

Exam Tip: Remember IAM = "I Am Allowed Access" - all four components must work together. Without any one pillar, the entire system fails.

IAAA Framework: The Four Pillars



Identification

Key Points:

- Claiming an identity (username, employee ID, national ID)
- First step in the access control process
- Provides the system with the claimed identity to verify
- Examples: username entry, biometric ID scanning

Authentication

Key Points:

- Proving you are who you claim to be
- Uses passwords (something you know), tokens (something you have), biometrics (something you are)
- Single-factor = basic security, multi-factor = stronger protection
- Validates the claimed identity

Authorization

Key Points:

- Determines what actions/resources verified identity can access
- Checks permissions, roles, and access policies
- Can be static (role-based) or dynamic (context-based)
- The principle of least privilege guides decisions

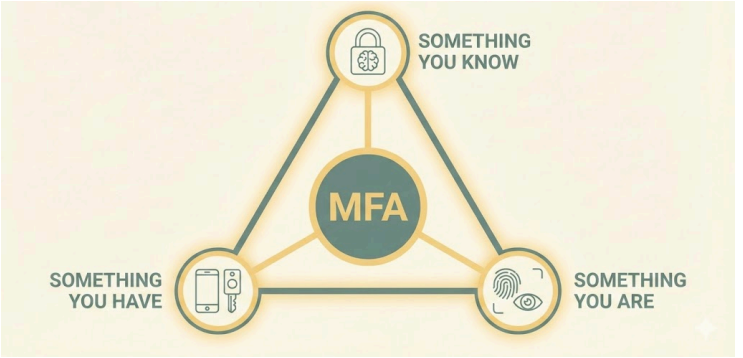
Accountability

Key Points:

- Tracks what users did with authorised access
- Detailed logs and audit trails
- Essential for forensics, compliance, and detecting unauthorised activities
- Requires non-repudiation mechanisms

Exam Tip: Shared credentials destroy accountability. Multiple users sharing an "admin" account = impossible to attribute actions = compliance violation.

Authentication Factors



Type 1: Something You Know

Password Types:

- Static passwords: Unchanging until manually updated, vulnerable to attacks, and require complexity policies
- Passphrases: Longer phrases with multiple words, more memorable, resistant to brute force
- Dynamic passwords (OTP): Change with each use, eliminate replay attacks, require infrastructure
- TOTP: Time-based codes valid 30-60 seconds, requires time synchronisation
- HOTP: Counter-based codes, valid until used, suitable for offline scenarios

Common Password Attacks:

- Dictionary attacks: Pre-computed word lists against password hashes
- Brute force: Try every possible combination, defeated by key stretching (bcrypt, PBKDF2)
- Rainbow tables: Pre-computed hash tables, defeated by salting passwords

- Password guessing: Online attempts against live systems, defeated by account lockout

Salt in Cryptography:

- Random string added to passwords before hashing
- Ensures that identical passwords create different hashes for different users
- Defeats rainbow table attacks
- Each user receives a unique salt stored with the password hash

Exam Tip: Salt is like a unique spice blend - same password, different users = different hash values. Rainbow tables require separate tables for each salt = impractical.

Type 2: Something You Have

Key Points:

- Banking tokens: Hardware devices with cryptographic processors, independent of mobile networks
- Smart cards: Contact/contactless cards with embedded chips, store cryptographic keys
- Mobile devices: Smartphones receiving OTPs via SMS or apps
- Soft tokens: Apps like Google/Microsoft Authenticator generate TOTP codes

OTP Generation Methods:

- HOTP: Counter-based, remains valid until used, offline capable
- TOTP: Time-based (30-60 sec validity), requires time sync

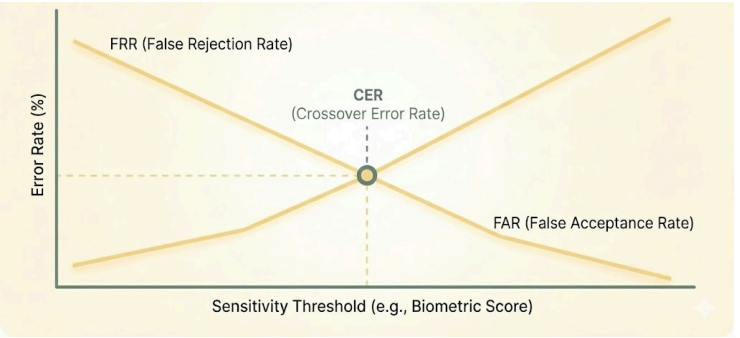
- Challenge-Response: Server sends challenge, device responds with calculated value

Indian Context:

- RBI mandates two-factor authentication for transactions above ₹1000
- National ID systems use mobile OTP combined with biometrics

Exam Tip: Transaction Authorisation Numbers (TANs) are counter-based OTPs used sequentially - each transaction requires the next number in sequence.

Type 3: Something You Are (Biometrics)



Biometric Accuracy Metrics:

- False Rejection Rate (FRR) - Type I Error: Authorised user incorrectly rejected, causing frustration
- False Acceptance Rate (FAR) - Type II Error: Unauthorised user incorrectly accepted, SERIOUS SECURITY BREACH
- Crossover Error Rate (CER): Point where FRR = FAR, lower CER = better accuracy, industry benchmark

Biometric Types:

- Physiological: Fingerprints (most common, cost-effective), iris (highly accurate), retina (reveals health conditions), facial recognition (passive, privacy concerns), hand geometry (harsh environments)
- Behavioural: Keyboard dynamics, dynamic signature, voice recognition, gait recognition

Critical Considerations:

- Privacy concerns: Retina scans reveal medical conditions
- Permanence problem: Biometrics cannot be changed if compromised (unlike passwords)
- Cultural sensitivity: Some communities object to certain scanning methods
- Throughput: Balance between security and convenience at high-traffic locations

Exam Tip: Type II error (FAR) is MORE SERIOUS than Type I error (FRR) from a security perspective. Better to frustrate a legitimate user than allow an attacker access.

Type 4: Someplace You Are (Location-Based)

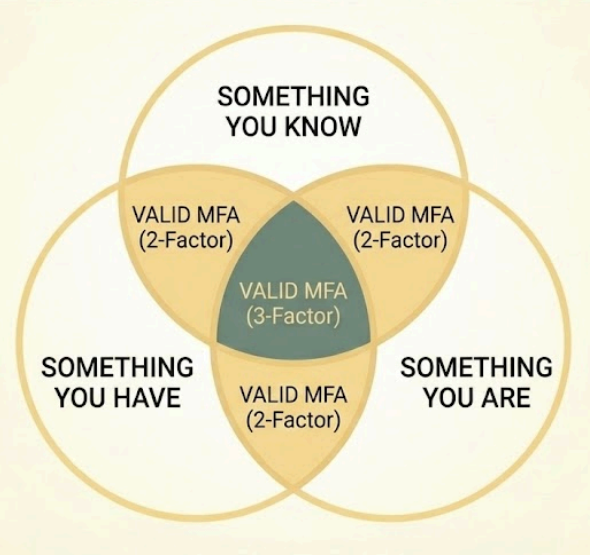
Key Points:

- IP geolocation: Block access from foreign/suspicious locations, which can be circumvented by VPN
- GPS coordinates: Precise location verification, can be spoofed
- Network-based: Restrict to corporate networks or approved locations

Indian Context:

- Payment systems flag transactions when a card is used in an unexpected location
- State-specific compliance may require location-based access restrictions.

Multifactor Authentication (MFA)



Key Points:

- True MFA requires elements from DIFFERENT factor categories
- Significantly raises the bar for attackers by requiring multiple independent compromises
- Essential as single-factor authentication is increasingly inadequate

Valid MFA Combinations:

- ATM card (have) + PIN (know)
- Fingerprint (are) + Password (know)
- Smart card (have) + Iris scan (are)
- Mobile OTP (have) + Location (are)

Invalid MFA (Same Factor):

- Password + Security question (both knowledge)
- Two different passwords (both knowledge)
- Two biometric types (both biometric)

Indian Context:

- National ID systems: ID number + fingerprint/iris + OTP to mobile
- Enables rapid digitisation while maintaining security

Exam Tip: Password + security question is NOT MFA - both are knowledge factors. Must be from different categories!

SMS OTP Vulnerabilities and Better Alternatives

Method	Phishing Resistant	No SS7 Risk	No SIM Swap Risk	User Convenience	Cost
SMS OTP	No	No	No	High	Low
TOTP	No	Yes	Yes	Medium	Low
FIDO2 / WebAuthn	Yes	Yes	Yes	High	Medium
Push (with number match)	Partial	Yes	Yes	High	Low
Hardware OTP Token	No	Yes	Yes	Medium	High

Critical SMS OTP Vulnerabilities:

SS7 Protocol:

- Legacy telecom protocol with no authentication/encryption
- Malicious actors with SS7 access can intercept SMS in transit
- SS7 access purchasable on the black market ($1000-$15,000)
- Requires telecom infrastructure changes to fix

SIM Swapping:

- Social engineering telecom provider to transfer number to attacker's SIM
- Can be completed in hours, often during the victim's sleep
- Enables complete account takeover
- Defence: Port freeze requests, carrier PINs (effectiveness varies)

Other Vulnerabilities:

- Phishing/Vishing: Attacker calls pretending to be a bank, requests OTP
- Malware: Banking trojans with SMS permissions intercept OTPs

- IMSI catchers: Fake cell towers intercept SMS within physical proximity

NIST SP 800-63B Guidance:

- SMS is classified as a "restricted authenticator"
- "Implementers of new systems SHOULD carefully consider alternative authenticators"
- Not prohibited, but strongly discouraged for new systems
- If using SMS: limit validity (5-10 min), pre-registered numbers only, rate limiting

Better MFA Alternatives:

TOTP (RECOMMENDED):

- RFC 6238 standard (Google/Microsoft Authenticator, Authy)
- Cryptographic secret shared during enrollment, no network transmission
- Prevents SS7 interception and SIM swapping
- Remaining risk: Phishing (user manually enters code), device theft

FIDO2/WebAuthn (BEST PRACTICE):

- W3C standard, phishing-resistant (origin-bound credentials)
- Public-key cryptography
- Hardware: YubiKey, Titan Security Key, biometric sensors
- Can eliminate passwords (passwordless)
- Prevents phishing, replay, and MITM attacks

Push Notification:

- Out-of-band verification (Duo, Microsoft Authenticator)
- User approves on a trusted device
- Risk: "Push fatigue" - users approve without reading
- Mitigation: Number matching (display number on login screen, user enters on phone)

Comparison Matrix:

Method	Phishing Resistant	No SS7 Risk	No SIM Swap	User Convenience	Cost

SMS OTP	No	No	No	High	Low
TOTP	No	Yes	Yes	Medium	Low
FIDO2 / WebAuth	Yes	Yes	Yes	High	Medium
Push (number match)	Partial	Yes	Yes	High	Low

Indian Context:

- RBI mandates two-factor authentication, but doesn't specify the method
- Most Indian banks use SMS OTP due to smartphone penetration
- UPI apps increasingly support biometric + device binding
- Expect a regulatory push toward phishing-resistant MFA (FIDO2)

Exam Tip: NIST doesn't ban SMS OTP but strongly discourages it. For example, know vulnerabilities (SS7, SIM swap) and recommend FIDO2 for phishing resistance or TOTP for broad compatibility.

Access Control Principles

Least Privilege

Key Points:

- Users receive the minimum access necessary for job functions
- Start with no access, add only what's required

- Reduces attack surface and limits damage from compromised accounts
- Requires detailed job understanding and regular review

Example: Bank teller: transactions up to ₹50,000; Assistant manager: up to ₹2 lakhs; Branch manager: unlimited branch authority.

Need to Know

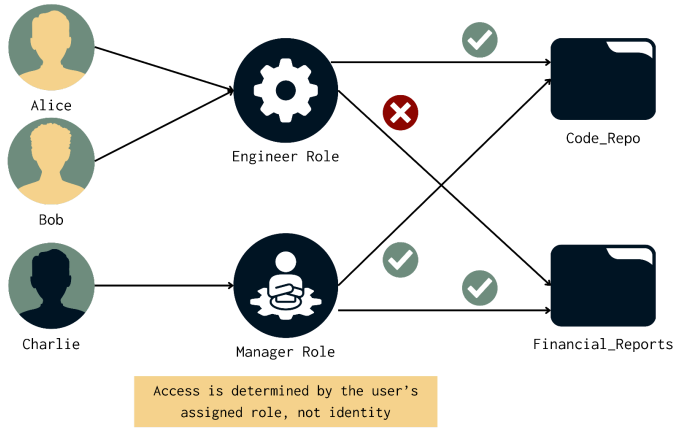
Key Points:

- Access granted ONLY with a legitimate business requirement
- Independent of security clearance or position level
- Requires formal justification for access requests
- Minimises insider threat and accidental disclosure

Example: A Defence scientist with "Secret" clearance cannot access submarine blueprints despite the same classification - requires project involvement (need-to-know).

Exam Tip: Classification hierarchy: Restricted < Confidential < Secret < Top Secret. Users can READ at/below clearance level, can only CREATE at clearance level or higher (prevents accidental downgrade).

Separation of Duties (SoD)



Key Points:

- Prevents fraud/errors by requiring multiple people for critical functions
- Divide critical processes among different individuals/roles
- Types: Preventive (stops fraud before) and detective (identifies after)
- Can slow processes, but is essential for high-risk operations

Examples:

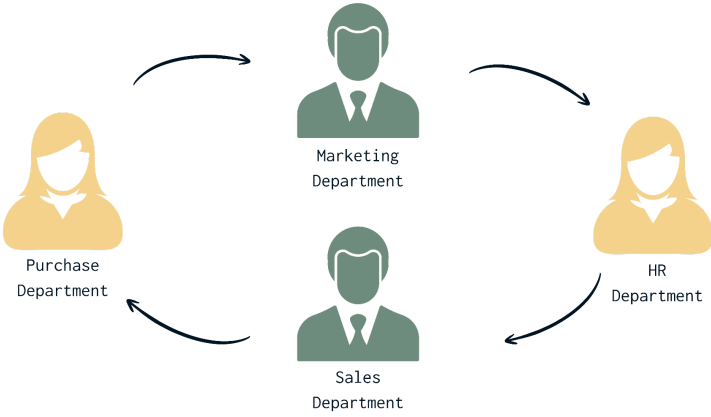
- Loan approval and disbursement by different departments
- Developers cannot deploy to production
- Internal auditors cannot audit their own departments

Indian Context:

- Government procurement: Technical and financial bids opened by separate committees

- Public sector banks: Loan applications evaluated by credit, legal, and disbursement teams

Rotation of Duties



Key Points:

- Cross-training, fraud prevention, process improvement
- Ensures business continuity, reduces fraud opportunities
- Systematic rotation schedules for sensitive positions
- Training costs and temporary productivity reduction

Indian Context:

- Public sector banks rotate branch managers every 2-3 years to prevent inappropriate relationships and collusion in loan approvals

Exam Tip: Separation of Duties prevents fraud by requiring collusion. Rotation of Duties prevents long-term fraud schemes by forcing different people into roles periodically.

Access Control Components

Subjects and Objects

Subject	Object
Active entities	Passive entities
A subject is a person, process, program, or anything similar that actively tries to access an object	An object is anything that is being passively accessed by a subject, like a file, server, process, or hardware component.

Subjects (Active):

- Users, processes, programs, services
- Initiate actions and make access requests
- Can assume different roles in different contexts

Objects (Passive):

- Files, databases, printers, and network resources
- Acted upon by subjects

- Cannot initiate actions independently

Critical Dual Nature:

- Chrome.exe running = subject (accesses websites)
- Chrome.exe stored on disk = object (being backed up)

Access Control Matrix

- Two-dimensional table: subjects × objects
- Centralised permission management
- Clear visualisation of access rights
- It can become complex in large enterprises

Capability Tables

- Subject-centric view: lists all permissions for each subject
- Easy to determine which specific user can access
- Difficult to see all users with access to a specific object

Constrained Interface

- Different views/options based on user privileges
- The same banking app shows different menus for customers vs. employees, vs. managers.
- Reduces confusion and prevents accidental or unauthorised actions
- Must maintain security even if the interface is bypassed

Content-Dependent Control

- Authorisation based on actual data content
- Databases with field-level security
- Example: Junior HR sees name/department; Senior HR adds salary; Payroll adds bank details
- May impact performance due to content analysis

Context-Dependent Control

Types:

- Time-based: Restrict during specific hours; night shift workers are blocked during the day
- Location-based: Access only from corporate premises, geographic restrictions
- Sequence-based: Cannot download product until payment is complete
- Transaction-based: ATM withdrawals require a sufficient balance

Exam Tip: Context-dependent uses environmental factors (time, location, sequence). Content-dependent examines the actual data being accessed.

Access Control Models

Discretionary Access Control (DAC)

Key Points:

- Resource owners have full discretion over access permissions
- Flexible, easy-to-share resources
- Prioritises AVAILABILITY and usability
- Common in Windows/Linux file systems
- Risk: Access creep over time, difficult to enforce consistent policies

Example: Google Drive - document creator has complete discretion over who can view/edit/comment.

Exam Tip: DAC = Owner decides. Focuses on AVAILABILITY. Best for collaboration environments.

Mandatory Access Control (MAC)

Key Points:

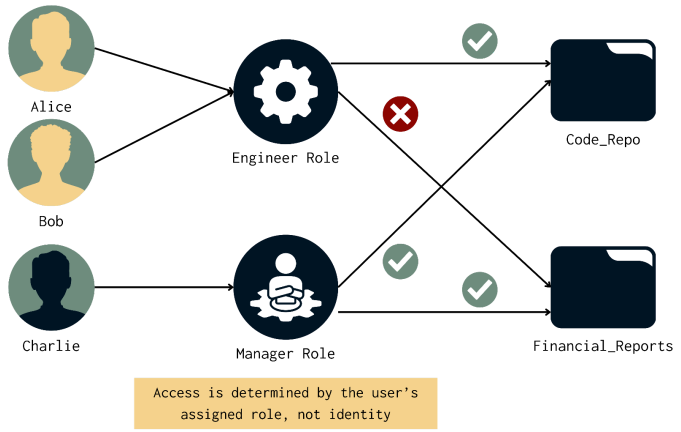
- System-enforced based on labels and clearances
- No user discretion - users cannot override system decisions
- Prioritises CONFIDENTIALITY above all
- Label-based: resources and users assigned security labels
- Common in military, government, and high-security environments

Security Label Rules:

- Read Down: Users can read at or below their clearance level
- Write Up: Users can only write to the exact clearance level or higher (prevents accidental downgrade)

Exam Tip: MAC = Military-style. Focuses on CONFIDENTIALITY. System decides, not users. Remember: Read down, write up.

Role-Based Access Control (RBAC)



Key Points:

- Permissions grouped into job functions (roles)
- Users assigned to appropriate roles
- Users and permissions are connected ONLY through roles
- Roles can inherit permissions from other roles
- Prioritises INTEGRITY through controlled access

Benefits:

- Administrative efficiency - manage through roles, not individual users
- Scalability for large organisations
- Naturally enforces least privilege
- Supports compliance and audit trails

Example: Developer role: code repos, dev servers, bug tracking. Tester role: test environments, testing tools. When roles change, permissions are automatically updated.

Exam Tip: RBAC = Job title decides. Focuses on INTEGRITY. Most common in modern enterprises. Prevents privilege accumulation through automated role changes.

Attribute-Based Access Control (ABAC)

Attribute Categories:

- Subject: User characteristics (clearance, department, seniority, certifications)
- Object: Resource properties (classification, owner, creation date, data type)
- Environmental: Contextual factors (time, location, threat level, network)
- Action: Operation characteristics (read, write, execute, delete)

Key Points:

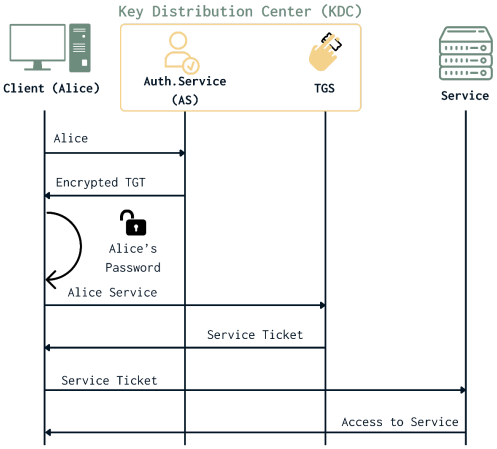
- Most sophisticated approach
- Complex policies combining multiple attributes
- Dynamic real-time evaluation based on current attribute values
- Very granular control is possible
- Can implement any other access control model
- Requires sophisticated policy management

Example: Hospital patient records - Doctor can access only their assigned patients' records, during working hours, on the hospital network, with emergency overrides for critical situations.

Exam Tip: ABAC = Most flexible, most complex. Uses multiple attributes for dynamic decisions. Can replace any other model.

Authentication Protocols

Kerberos



Core Components:

- KDC (Key Distribution Centre): Central trusted authority
- AS (Authentication Server): Verifies identity, issues TGT
- TGS (Ticket Granting Server): Issues service-specific tickets
- TGT (Ticket Granting Ticket): Initial authentication proof
- Service Tickets: Access credentials for specific services

Process:

1. User proves identity to AS, receives TGT
2. User presents TGT to TGS, requesting service access
3. TGS issues a Service Ticket for a specific service
4. User presents the Service Ticket to access the service

5. Mutual authentication between the user and the service

Advantages:

- Single Sign-On (SSO) capability
- Mutual authentication protects both client and server
- Strong cryptographic protection (symmetric keys)
- Replay attack protection via timestamps

Limitations:

- Single point of failure if KDC is unavailable
- Requires synchronised clocks (within 5 minutes typically)
- Complex troubleshooting

Exam Tip: Kerberos = Three-headed dog = three components (AS, TGS, Service). Requires TIME SYNCHRONIZATION. Named after the Greek mythology guard dog.

RADIUS (Remote Authentication Dial-In User Service)

Key Points:

- Centralised AAA services for network access
- Uses UDP (port 1812 authentication, 1813 accounting)
- Encrypts ONLY the password field, not the entire packet
- Supports multiple Network Access Servers (NAS)
- Detailed logging of sessions and usage

Applications:

- ISP broadband authentication

- Corporate WiFi authentication
- VPN access
- Network device management (routers/switches)

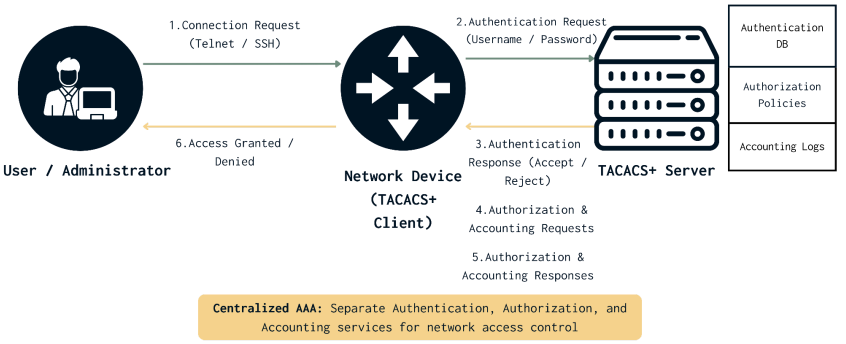
Process:

1. User attempts connection to NAS
2. NAS forwards the request to the RADIUS server
3. RADIUS verifies credentials
4. RADIUS sends Accept/Reject to NAS
5. NAS grants access, sends accounting data to RADIUS

Example: Fibre internet router authenticates against ISP's RADIUS servers, determines service level (speed, data caps), logs session for billing.

Exam Tip: RADIUS uses UDP, encrypts only the password. Primarily for network access control.

TACACS+ (Terminal Access Controller Access-Control System Plus)



Advantages over RADIUS:

- Encrypts ENTIRE packet content, not just passwords
- Separates Authentication, Authorisation, and Accounting as distinct functions
- Uses TCP (port 49) for reliable delivery
- Can authorise individual commands on network devices
- Detailed accounting of administrative actions

Use Cases:

- Router and switch administrative access
- Security appliances (firewalls, IPS)
- High-security environments requiring detailed audit trails
- Compliance requiring granular command-level authorisation

Example: Bank network operations - junior admins can VIEW router configs but cannot CHANGE, senior admins have full authority, all commands logged for compliance.

Exam Tip: TACACS+ = Cisco protocol, encrypts the full packet, uses TCP, and separates AAA functions. Better for device administration than RADIUS.

Active Directory

Organisational Structure:

- Domains: Administrative boundaries containing users/computers/resources
- Domain Controllers: Servers providing authentication and directory services
- Forests: Collections of domains sharing common schema and trust relationships
- Organisational Units (OUs): Containers for organising objects within domains

Trust Relationships:

- One-way Trust: Domain A trusts users from Domain B (not vice versa)
- Two-way Trust: Mutual trust, authentication in both directions
- Transitive Trust: Trust extends through intermediate domains
- External Trust: Trusts with domains outside the forest

Group Policies:

- GPOs (Group Policy Objects): Centralised configuration settings
- Security Groups: Collections of users with similar access rights

- Distribution Groups: Email lists without security implications
- Administrative Delegation: Granular assignment of admin privileges

Exam Tip: AD = Microsoft's enterprise identity management. Uses Kerberos for authentication. Forests contain domains; domains contain OUs.

SAML (Security Assertion Markup Language)

Architecture:

- Identity Provider (IdP): Authenticates users, issues SAML assertions
- Service Provider (SP): Applications accepting SAML assertions
- SAML Assertions: XML documents with authentication/authorisation info
- Metadata: Configuration exchanged between IdP and SP

Flow:

1. User attempts to access the SP application
2. SP redirects the user to the configured IdP
3. User authenticates with IdP
4. IdP creates a signed SAML assertion
5. User's browser posts assertion to SP
6. SP validates the assertion and grants access

Indian Context:

- Digital government services: Citizens authenticate once with national ID, access multiple services (tax filing, vehicle registration, certificates) without re-authentication

Exam Tip: SAML = SSO across organisations using XML assertions. As a passport-issuing authority (IdP) vouches for identity, foreign countries (SPs) accept it.

Identity Lifecycle Management

Onboarding Phase

Key Points:

- Identity creation: Username, initial password (forced change), profile info
- Initial access: Role-based groups, baseline system access
- Account activation: Email verification, initial login, policy acknowledgement

Example: New developer receives employee ID, temporary password, email access, and dev environment permissions. Production access is only available after security training.

Maintenance Phase

Key Points:

- Regular access reviews: Quarterly privilege assessments, annual recertification
- Privilege modifications: Project-based temporary access, training access, cross-functional permissions
- Password management: Regular expiration/renewal, reset support, MFA enrollment

Transfer Phase

Key Points:

- Role transition planning: Advance notification, new access analysis, timeline
- Access modification: Remove old role access, add new role permissions, temporary overlap for knowledge transfer
- Validation: Test new access, user training, and documentation updates

Example: Bank employee transfers from retail to corporate banking - individual customer access removed, corporate client access added, brief overlap for knowledge transfer.

Offboarding Phase

Key Points:

- Access revocation: Immediate deactivation, removal from groups/roles, termination of VPN/remote access

- Account deactivation: Suspend (not delete) for future reference, email forwarding, backup essential data
- Asset recovery: Return laptops/devices/access cards, collect documents, verify data deletion from personal devices

Exam Tip: Accounts should be SUSPENDED rather than immediately deleted - enables future reference for investigations or knowledge transfer. Immediate deletion destroys the audit trail.

Account Management Best Practices

Automated Monitoring

Key Points:

- Dormant account detection: Flag accounts inactive > 30 days, investigate unused new accounts > 10 days
- Privilege escalation monitoring: Alerts for significant privilege increases, review temporary access becoming permanent
- Access pattern analysis: Unusual login times/locations, access outside normal job functions, high-volume data access

Service Account Management

Key Points:

- Strong authentication: Complex passwords exceeding user requirements, 90-day rotation, enterprise password management integration

- Privilege minimisation: Least privilege application, regular permission review, documented justification
- Activity monitoring: Detailed audit trails, real-time unusual behaviour monitoring, SIEM integration
- Inventory : Maintain an inventory and classify all service accounts.
    - Identify → Classify → Control → Monitor

Example: Bank core banking service accounts can transfer funds, generate reports, and modify customer records. Use 20-character random passwords changed every 60 days, all activities logged and monitored.

Exam Tip: Attackers often look for service accounts as they are high-value targets due to elevated privileges and automated nature. Require stronger controls than regular user accounts.

Federated Identity Management

Federation Benefits

Having a single, consistent set of policies, practices, and procedures to manage the identities of users and devices, and to establish trust across the organisation's IT systems.

User Experience:

- Single Sign-On (SSO): Authenticate once, access multiple services
- Reduced password fatigue: Fewer forgotten passwords
- Faster access: Seamless application switching
- Consistent experience: Uniform login procedures

Administrative:

- Centralised management: Single source of truth for identities
- Simplified provisioning/deprovisioning: One place to manage access
- Consistent policies: Uniform security policies across services
- Enhanced security: Centralised monitoring, consistent MFA enforcement

Compliance:

- Simplified audits: Single location for access reviews
- Consistent data formats: Easier compliance demonstration
- Policy enforcement: Uniform password policies, centralised incident response

Identity as a Service (IDaaS)

Popular Solutions:

- Okta: Enterprise SSO and identity management, cloud/on-premises integration
- Auth0: Developer-focused, APIs for custom integration, social media login support
- Microsoft Azure AD: Integrated with Office 365, Windows infrastructure, and comprehensive compliance
- AWS Cognito: Cloud-native applications, scalable user management for mobile/web

Benefits:

- Cost efficiency: Reduced infrastructure investment, predictable subscription pricing
- Scalability: Automatic scaling for varying loads, global presence
- Security: Regular updates, threat intelligence, compliance certifications

Indian Context:

- Startups use Auth0 for secure authentication in mobile payment apps
- Enterprises use Azure AD for Microsoft-based infrastructure
- Multinational corporations with Indian operations use Okta

Exam Tip: IDaaS = Cloud-based identity services. Reduces on-premises infrastructure burden but requires trusting the external provider with authentication.

Common Access Control Attacks

Password-Based Attacks

Social Engineering:

- Phishing: Fake login pages, urgent messages pressuring action. Mitigation: User training, email filtering
- Vishing: Phone calls impersonating banks/IT requiring a password. Mitigation: Verification procedures, callback protocols
- Pretexting: Fabricated scenarios (fake help desk). Mitigation: Strict identity verification

Technical Attacks:

- Keylogging: Hardware (USB) or software malware that captures keystrokes. Mitigation: Virtual keyboards, malware scanning
- Shoulder surfing: Direct observation of password entry. Mitigation: Privacy screens, awareness training
- Man-in-the-Middle: Fake WiFi, DNS hijacking. Mitigation: VPN, HTTPS enforcement, certificate validation

Indian Context:

- Bank fraud: Attackers call claiming to be from fraud prevention, request OTP while the victim provides it
- Increasing vishing attacks targeting banking customers

Exam Tip: Social engineering exploits HUMAN psychology, not technical vulnerabilities. User awareness training is a critical defence.

Biometric Attacks

Spoofing:

- Fingerprint: High-res images, silicone/gelatin moulds. Mitigation: Liveness detection (pulse, temperature)
- Facial recognition: Printed photos, video playback. Mitigation: 3D analysis, anti-spoofing algorithms
- Voice recognition: Recordings, AI-generated synthesis. Mitigation: Randomised challenge phrases, pattern analysis

Template Attacks:

- Template theft: Database breaches exposing biometric templates. Mitigation: Template encryption, distributed storage
- Reverse engineering: Mathematical attacks converting templates back to usable samples. Mitigation: Irreversible transformation, secure algorithms

Exam Tip: Biometric compromise is PERMANENT - cannot reissue fingerprints like passwords. Biometric databases require the highest security controls.

Advanced Persistent Threats (APT)

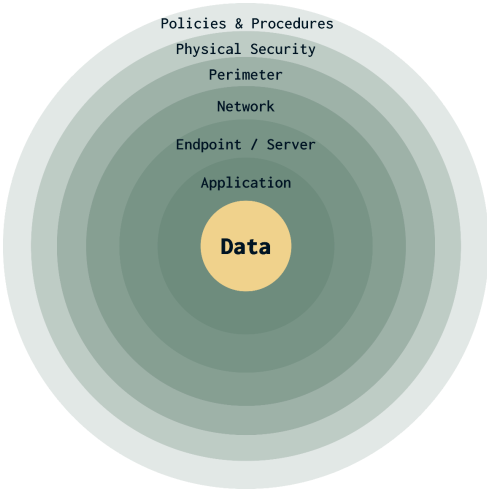
Credential Harvesting:

- Watering hole: Compromising frequently visited websites, injecting malicious code. Mitigation: Web application security, user education
- Supply chain: Malicious updates to authentication software, compromised hardware tokens. Mitigation: Vendor security assessments, secure update procedures

Privilege Escalation:

- Horizontal: Gaining access to resources at the same privilege level, exploiting shared accounts. Mitigation: Network segmentation, zero-trust architecture
- Vertical: Gaining higher-level access, exploiting vulnerabilities for admin rights. Mitigation: Regular patching, privilege monitoring, and access reviews

Comprehensive Defence Strategies



Multi-Layered Authentication:

- Defence in depth: Multiple independent controls
- Combining different authentication factors and technologies
- Controls at the network, system, and application levels
- Continuous monitoring and adaptive authentication

Risk-Based Authentication:

- Higher requirements for unusual access patterns
- Location-based and behavioural analysis
- Real-time adjustment based on threat intelligence
- Balance security with user experience

Organisational Measures:

- Security awareness training: Regular education, simulated phishing, role-specific training, continuous reinforcement
- Incident response: Rapid detection/containment, forensic analysis, recovery procedures, lessons learned integration

Exam Tip: Defence in depth = Multiple INDEPENDENT layers. If one fails, others still protect. Like a castle with a moat, walls, inner keep.

Key Exam Takeaways

Critical Distinctions:

- Biometric Errors: Type II (FAR) is more serious than Type I (FRR) from a security perspective
- Access Control Priorities: MAC = Confidentiality, DAC = Availability, RBAC = Integrity
- Authentication Protocols: Kerberos requires time sync, RADIUS encrypts only passwords, TACACS+ encrypts entire packets
- Security Principles: Separation of Duties prevents fraud, and Least Privilege prevents excessive access
- Password Security: Salts prevent rainbow tables, and account lockouts prevent guessing
- IAAA Framework: Identification + Authentication + Authorization + Accountability = complete access control

Memory Aids:

- IAAA: "I Am Allowed Access"
- Kerberos: Three-headed dog = AS + TGS + Service
- CER: Lower is better (sweet spot where FAR = FRR)
- MFA: Must be from DIFFERENT factor categories
- MAC: Military Access Control (confidentiality focus)
- RBAC: Role-Based (integrity focus, most common in enterprises)
- DAC: Discretionary (owner decides, availability focus)

Common Exam Mistakes:

- Confusing Type I and Type II errors (remember: Type II FAR is worse)
- Thinking password + security question is MFA (both knowledge factors)
- Forgetting the Kerberos time synchronisation requirement
- Confusing RADIUS (UDP, partial encryption) with TACACS+ (TCP, full encryption)
- Not recognising need-to-know is INDEPENDENT of clearance level
- Thinking accounts should be immediately deleted vs. suspended during offboarding

Quick Review Formulas:

- Something You Know = Passwords, PINs, passphrases
- Something You Have = Tokens, smart cards, mobile devices
- Something You Are = Biometrics (fingerprint, iris, facial, voice)
- Someplace You Are = Location (IP geolocation, GPS, network)

Indian Regulatory Context:

- RBI: Mandates two-factor authentication for transactions > ₹1000
- DPDP Act: Consent management requirements for identity data
- National ID Systems: Largest biometric authentication deployment globally
- UPI: Increasingly uses biometric + device binding instead of SMS OTP

Exam Tip: CISSP exam focuses on CONCEPTS and PRINCIPLES, not specific vendor implementations. Understand WHY controls work, not just HOW. When choosing answers, think about security tradeoffs: confidentiality vs. availability vs. integrity.

From Manager to CISO: Strategic Leadership

Differentiating Factor: User experience excellence with zero-trust, not security that frustrates users.

Key Points:

- Exceptional CISOs design IAM experiences so seamless that users barely notice security
- Risk-based authentication strengthens security for suspicious activities while streamlining normal patterns
- SSO eliminates password fatigue across dozens of applications
- Biometrics and device trust enable transparent authentication
- User frustration drives shadow IT and workarounds, undermining security

Measurable Impact:

- Reduce helpdesk password reset requests by 60-70% (millions in support cost savings)
- Authentication in seconds, not minutes (productivity gains across thousands of daily logins)
- Improved security posture + operational efficiency + user satisfaction

- IAM becomes a competitive advantage for talent acquisition

Strategic Capabilities:

- Translate authentication technologies into business enablement.
- Anticipate future needs (customer identity, partner access, API security)
- Design federated identity architectures supporting cloud adoption
- Navigate regulatory requirements (DPDP Act, RBI mandates, sector-specific guidelines)

Indian Context:

- Banking conglomerates: millions of customers + thousands of employees + hundreds of partners
- Cost-conscious IAM: phased approaches, open-source solutions, subscription models
- Hierarchical structures require executive support for customer-impacting changes
- Change resistance requires patient education and gradual rollouts

Implementation Wisdom:

- Risk-based authentication balances security and usability
- Identity lifecycle automation prevents access creep
- Build vs. buy decisions consider organisation size, expertise, and customisation needs
- Federation enables SSO but creates concentration risk

Leadership Competencies:

- User experience understanding prevents security workarounds
- Vendor management beyond feature lists (security practices, compliance, data residency, viability)
- Learning from authentication failures accelerates development
- Industry engagement through identity standards bodies and peer networks

Exam Tip: CISSP values strategic thinking. For scenario questions, consider business impact, user experience, and operational efficiency alongside security. The best answer often balances multiple competing concerns.

Domain 6: Security Assessment and Testing

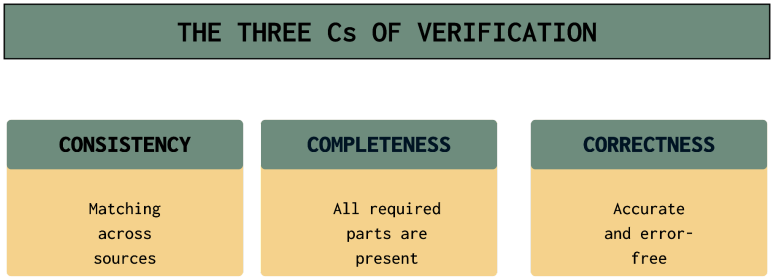
Validation vs Verification

Verification
Are you building the **Product RIGHT**?

Validation
Are you building the **RIGHT Product**?

Key Points:

- Validation: "Are we building the right product?" - ensures security aligns with business needs
- Verification: "Are we building the product correctly?" - confirms proper implementation to specifications
- Three Cs of Verification: Completeness (all use cases covered), Correctness (use cases match requirements), Consistency (functionality uniform across system)



Exam Tip: Validation is about purpose and business fit; Verification is about technical accuracy. Remember: Validation first, then Verification.

Testing Perspectives: Internal vs External

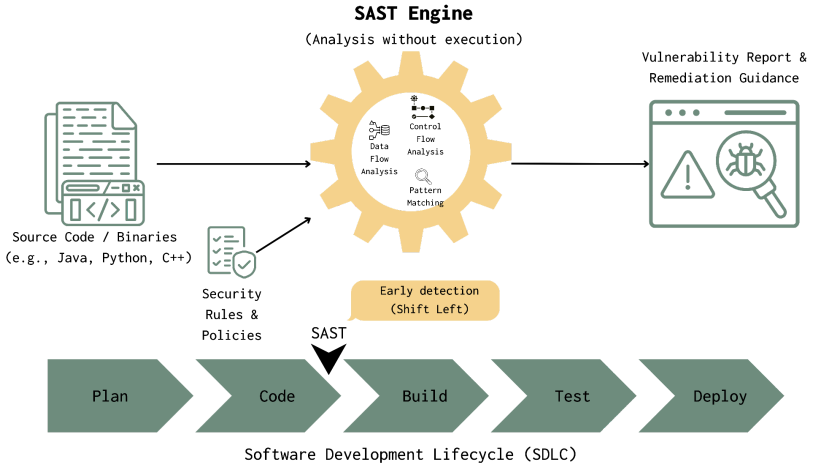
Aspect	Internal Testing (Glass Box / White Box)	External Testing (Black Box / Grey Box)
Team	Employees, Developers, QA	Third-party, users, hackers
Focus	Code, logic, bugs, integration	UX, security, performance, real-world usage
Knowledge Level	Full system access	Limited or no access
Key Benefit	Early detection	Unbiased perspective
Testing View	Inside-out	Outside-in
GOAL: Comprehensive Quality & Security Assurance		

Key Points:

- Internal testing: Simulates insider threats or compromised systems, tests lateral movement and privilege escalation
- External testing: Simulates attacks from outside perimeter, tests boundary defences and public-facing services
- Four combinations: Internal/Employee, External/Employee, Internal/Third-party, External/Third-party
- Each perspective reveals different vulnerabilities

Exam Tip: Internal testing assumes the attacker already has access; External testing starts from the internet. Choose based on threat model.

Static Application Security Testing (SAST)



Key Points:

- White-box testing - analyses source code, byte code, or binary without running it

- Performed early in SDLC - finds vulnerabilities before deployment
- Identifies SQL injection, buffer overflows, and logic errors through code analysis
- Cost-effective - issues found early when fixes are cheap
- Integrates into developer workflows

Indian Context:

- Critical for IT services companies developing applications for global clients
- Mandated by many regulatory frameworks for critical systems

Exam Tip: SAST is "white-box", and analyses code WITHOUT running it. Think "Static = Stationary code review."

Dynamic Application Security Testing (DAST)

Key Points:

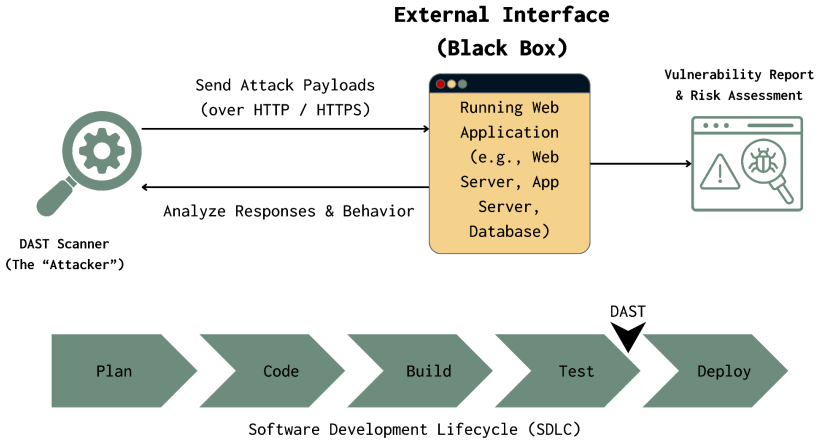
- Black-box testing - tests running the application without source code access
- Tests application as attacker sees it - focuses on inputs, outputs, behaviour
- Evaluates runtime security controls in realistic environments
- Fuzz testing: Submits random/malformed data to find buffer overflows and boundary issues

Indian Context:

- Essential for testing e-governance portals and public-facing government services
- Required for UPI payment systems and digital banking platforms

Exam Tip: DAST is "black-box" and tests RUNNING applications. Think "Dynamic = Application in motion."

Penetration Testing Phases



Penetration Testing Phases:

- Planning: Define scope, rules of engagement, and obtain authorisation
- Reconnaissance: Gather intelligence using OSINT techniques
- Scanning (Enumeration): Identify live systems, open ports, and services
- Vulnerability Assessment: Identify and prioritise security weaknesses

- Exploitation: Attempt to exploit vulnerabilities, demonstrate business impact
- Reporting: Document findings with remediation recommendations

1. Planning Phase	2. Reconnaissance	3. Scanning (Enumeration)	4. Vulnerability Assessment	5. Exploitation	6. Reporting
• Define scope and rules of engagement • Obtain proper authorization and legal clearance • Establish communication protocols and emergency contacts • Define success criteria and testing objectives	• Gather information about the target • Use OSINT (Open Source Intelligence) techniques • Research company structure, employees, technologies used • Identify potential attack vectors and entry points	• Identify live systems and open ports • Discover services and versions running • Map the attack surface systematically • Document network topology and service configurations	• Identify potential security weaknesses • Prioritize based on exploitability and impact • Analyze findings for false positives • Develop exploitation strategies	• Attempt to exploit identified vulnerabilities • Gain unauthorized access to systems • Escalate privileges where possible • Demonstrate business impact of vulnerabilities	• Document all findings comprehensively • Provide remediation recommendations • Present results to management in business terms • Include executive summary and technical details

Indian Context:

- RBI requires annual penetration testing for banks and NBFCs
- Must use CERT-In empanelled auditors for regulatory compliance

Exam Tip: Remember "PRSVER" - Planning, Reconnaissance, Scanning, Vulnerability assessment, Exploitation, Reporting. Always start with authorisation.

Penetration Testing Knowledge Levels

Aspect	Black Box Testing	Grey Box Testing	White Box Testing
Focus	Inputs & outputs only	Inputs, outputs, and limited internal logic	Internal structure & code logic
Knowledge Level	No internal system knowledge	Partial system knowledge	Full system knowledge
Perspective	External user	Hybrid (attacker / tester)	Internal developer
Visibility	No visibility into internals	Partial visibility	Full visibility
Examples	Functional testing, UI testing	Integration testing, Security assessment	Unit testing, Code coverage, Static analysis

Key Points:

- Black Box (Zero Knowledge): No prior information, simulates an external attacker, most realistic but time-consuming
- White Box (Full Knowledge): Complete information, including source code, network diagrams, credentials - efficient but less realistic
- Grey Box (Partial Knowledge): Limited information, simulates insider threat or compromised vendor - balances realism and efficiency

Exam Tip: Black = outsider, White = complete insider, Grey = compromised user. Match testing type to threat scenario.

Penetration Testing Scope Types

Key Points:

- Network Testing (Internet-facing): External perimeter, firewalls, public services
- Network Testing (Internal/DMZ): Internal segmentation, lateral movement, privilege escalation
- Wireless Testing: Wi-Fi security, encryption protocols (WPA2/WPA3)
- Physical Testing: Unauthorised physical access, tailgating, badge systems
- War Dialling: Historical technique using modems (exam-relevant but largely obsolete)

Exam Tip: Wardialling is outdated, but appears on the exam. The modern equivalent is VoIP/remote access testing.

Vulnerability Assessment vs Penetration Testing

Regulation/Standard	Vulnerability Assessment	Penetration Testing	Modern Best Practice
PCI-DSS v4.0	Quarterly (external & internal)	Annual	Continuous scanning + quarterly compliance scans
RBI (India Banking)	Quarterly minimum	Annual (semi-annual for critical)	Monthly VA + continuous monitoring
ISO 27001	Risk-based (typically quarterly)	Risk-based (typically annual)	Continuous scanning + annual PT
NIST Cybersecurity Framework	Ongoing (continuous preferred)	Risk-based	Continuous vulnerability management
SOC 2 Type II	Periodic (typically quarterly)	Annual	Monthly minimum + continuous monitoring

Vulnerability Assessment:

- Identifies potential weaknesses using automated scanning
- Provides broad coverage quickly
- Generates vulnerability inventory with CVSS severity ratings
- Creates baseline security posture

Penetration Testing:

- Validates identified weaknesses through exploitation
- Confirms real vs false positives
- Demonstrates actual business impact
- More time-intensive, deeper analysis

Exam Tip: Assessment finds vulnerabilities; Testing proves they're exploitable. Assessment is breadth, Testing is depth.

Vulnerability Scanning: Credentialed vs Uncredentialed

Aspect	Credentialed (Authenticated) Scans	Uncredentialed (Unauthenticated) Scans
Credentials Used	Uses valid credentials to log into systems	No credentials provided
Viewpoint	Internal system perspective	External attacker perspective
Accuracy	Provides deeper, more accurate results	May miss many vulnerabilities
Coverage	Can check patch levels and configurations	Limited to externally visible issues
Assessment Type	Comprehensive internal security assessment	Perimeter security assessment
Usefulness	Ideal for internal vulnerability management	Useful for external exposure testing
Example	Scanning internal servers with domain admin credentials to assess patch compliance and configuration drift	Scanning public-facing systems without authentication

Credentialed (Authenticated) Scans:

- Uses valid credentials to log into systems
- Provides deeper, more accurate results
- Checks patch levels and configurations
- Comprehensive internal security assessment

Uncredentialed (Unauthenticated) Scans:

- No credentials provided
- Simulates an external attacker viewpoint
- May miss many vulnerabilities
- Limited to externally visible issues

Exam Tip: Credentialed scans are more thorough. Uncredentialed scans show the attacker's view.

Vulnerability Scanning Frequencies

PCI-DSS v4.0:

- External scans: Quarterly by PCI ASV (Approved Scanning Vendor)
- Internal scans: Quarterly
- Penetration testing: Annual (network and application layer)
- Additional scans: After significant changes

RBI (Reserve Bank of India):

- Vulnerability Assessment: Quarterly for all IT systems
- Penetration Testing: Annual minimum (semi-annual for critical systems)
- Must use CERT-In empanelled auditors

- Post-implementation testing after major changes

ISO 27001:

- Risk-based approach (no fixed frequency mandated)
- Industry best practice: Monthly for critical systems, quarterly for standard systems
- Annual penetration testing minimum

Modern Best Practice:

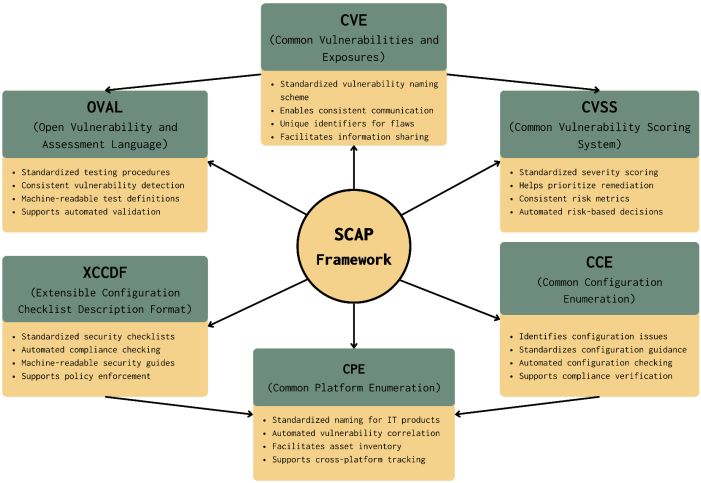
- Continuous vulnerability scanning (daily/weekly automated scans)
- Replace periodic scans with continuous monitoring
- On-demand scans triggered by deployment pipelines

Indian Context:

- CERT-In empanelled auditors preferred by regulators
- Budget constraints often limit testing to a minimum compliance frequency
- Data localisation requirements affect tool selection

Exam Tip: Know that PCI-DSS requires quarterly scans and annual penetration testing. Modern practice is continuous scanning for security, periodic for compliance.

SCAP Framework Components

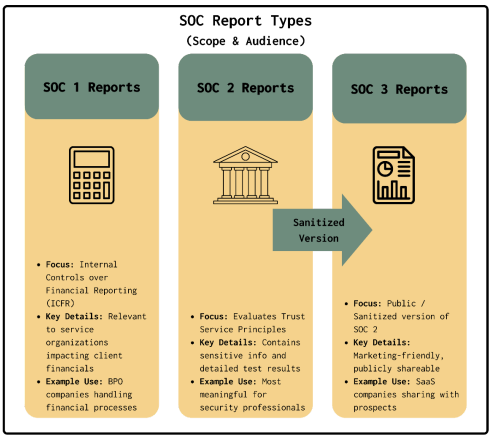


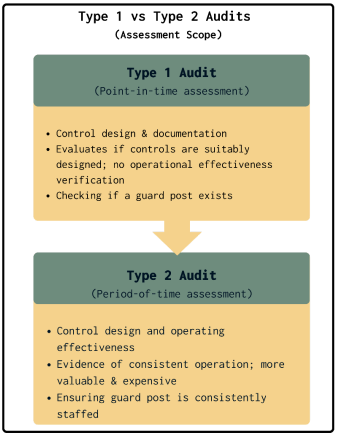
SCAP Components:

- CVE (Common Vulnerabilities and Exposures): Standardised vulnerability naming - unique identifiers for security flaws
- CVSS (Common Vulnerability Scoring System): Standardised severity scoring (0-10 scale)
- CCE (Common Configuration Enumeration): Identifies security configuration issues
- CPE (Common Platform Enumeration): Standardised naming for IT products and platforms
- XCCDF (Extensible Configuration Checklist Description Format): Machine-readable security checklists
- OVAL (Open Vulnerability and Assessment Language): Standardised vulnerability testing procedures

Exam Tip: Remember "CVE CVSS CCE CPE XCCDF OVAL" - CVE names it, CVSS scores it, CCE configures it, CPE identifies products, XCCDF checks it, OVAL tests it.

SOC Reports: Types and Purposes





SOC 1 Reports:

- Focus on financial reporting controls
- Relevant for service organisations affecting client financials
- Address Internal Controls over Financial Reporting (ICFR)

SOC 2 Reports:

- Evaluate five trust service principles: Security, Availability, Processing Integrity, Confidentiality, Privacy
- Most meaningful for security professionals
- Contains sensitive organisational information (restricted distribution)

SOC 3 Reports:

- Sanitised version of SOC 2
- Publicly shareable marketing document

- No sensitive control details

Indian Context:

- Critical for BPO companies handling financial processes for international clients
- SaaS companies use SOC 2/3 to demonstrate compliance to global customers

Exam Tip: SOC 2 is the security-focused report. SOC 3 is a public SOC 2 summary. SOC 1 is for financial controls.

Type 1 vs Type 2 Audits

Type 1 Audits:

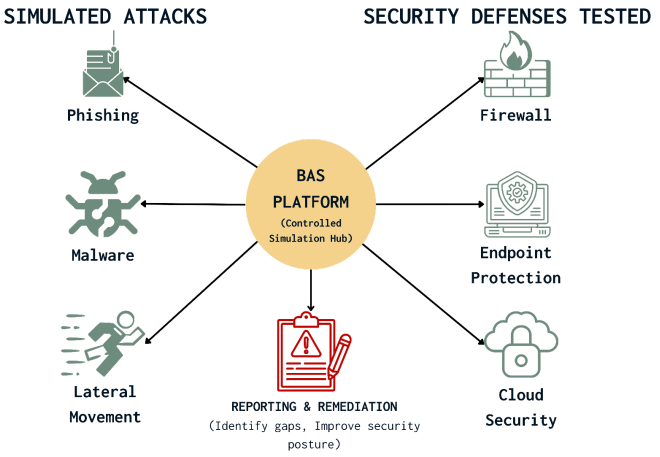
- Point-in-time assessment
- Evaluates control design only
- Checks if controls are suitably designed
- Does NOT verify operational effectiveness

Type 2 Audits:

- Period-of-time assessment (typically 6-12 months)
- Tests both design AND operating effectiveness
- Provides evidence of consistent control operation
- More expensive but more valuable

Exam Tip: Type 1 = "Does it exist on paper?" Type 2 = "Does it work consistently over time?" Type 2 is always more valuable.

Breach Attack Simulations (BAS)



Key Points:

- Automated, continuous attack simulations running 24/7/365
- Combines red team and blue team approaches (purple teaming)
- Provides real-time security posture visibility
- Enables continuous security validation vs periodic penetration tests

Indian Context:

- Major banks use BAS during high-transaction periods (festival bonus payments, tax seasons)
- Cost-effective alternative to frequent manual penetration testing

Exam Tip: BAS is automated continuous testing. Traditional pentest is manual, periodic testing.

Log Management: NIST SP 800-92

Logs to Collect:

- Network Security: Antivirus, IDS/IPS, VPN, web proxy, firewall, router logs
- Operating System: System events, security audit records, user activity
- Application: Client requests, server responses, usage patterns, errors

Five Mistakes of Log Analysis (Anton Chuvakin):

- Logs are not reviewed regularly
- Insufficient retention periods
- Lack of standardisation across systems
- Missing prioritisation (alert fatigue)
- Focus only on "bad stuff" (no baseline establishment)

Log Management Strategies:

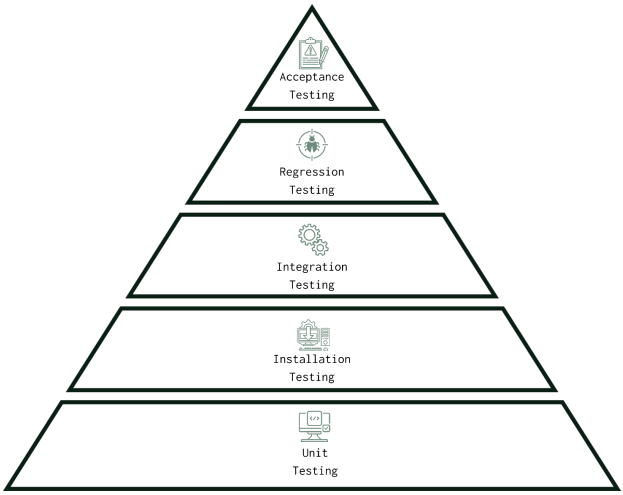
- Circular Overwrite: Oldest logs deleted when limit reached (simple but risky)
- Clipping Levels: Selective logging based on severity
- Centralised Logging: Scalable monitoring, correlation, tamper protection, enables SIEM

Indian Context:

- Banks must centralise logs for RBI regulatory compliance
- Retention requirements vary by regulation (typically 90 days to 7 years)

Exam Tip: Know the five log management mistakes. Centralised logging prevents tampering and enables correlation.

Software Testing Levels



Testing Hierarchy:

- Unit Testing: Tests individual components/functions in isolation - foundation of testing strategy
- Installation Testing: Verifies correct deployment on target hardware/environment
- Integration Testing: Tests component interactions - incremental or "Big Bang" approach
- Regression Testing: Ensures changes don't break existing functionality - critical after updates
- Acceptance Testing: Validates against business requirements - UAT involves actual users, final gate before production

Exam Tip: Remember the hierarchy: Unit (smallest) → Installation → Integration → Regression → Acceptance (final gate).

Specialised Testing Techniques

Combinatorial Testing:

- Tests unique input combinations using pairwise testing
- Reduces test cases intelligently while maintaining coverage
- Most bugs are triggered by single inputs or pairs

Misuse Case Testing:

- Simulates abnormal/malicious user behaviour
- Negative test scenarios are critical for security validation
- Example: Attempting to bypass OTP verification or use expired tokens

Test Coverage Analysis:

- Measures the percentage of code tested
- Identifies untested code paths
- Challenging with large codebases

Interface Testing Types:

- API Testing: REST/SOAP service validation
- Web Services Testing: Service interoperability
- GUI Testing: User interface functionality
- Database Testing: Data operations validation
- Hardware Interface Testing: Device communication

Indian Context:

- Misuse case testing is critical for UPI payment systems and digital wallets.
- Interface testing is essential for interoperable government services

Exam Tip: Misuse case testing simulates attacker behaviour. Interface testing validates component boundaries.

Requirements Traceability Matrix (RTM)

DYNAMIC AND ITERATIVE RTM USAGE MATRIX		
Requirement ID	**Requirement Description**	**Test Case ID(s)**
REQ_001	User authentication via MFA	TC_001, TC_002
REQ_001	–	TC_001, TC_002
REQ_002	Data encryption in transit	TC_003
REQ_003	–	TC_00
REQ_004	Session timeout (5 min inactivity)	TC_004, TC_005
REQ_004	Audit logs for admin actions	TC_006

Key Points:

- Maps requirements to test cases, ensuring comprehensive coverage
- Many-to-many relationship (one requirement → multiple test cases; one test case → multiple requirements)
- Living document that evolves with the project
- Enables impact analysis when requirements change

- Critical for regulatory compliance

RTM Benefits:

- Forward Traceability: Requirement changes → identify affected test cases
- Backward Traceability: Defects found → trace to originating requirements
- Coverage Metrics: Measure test coverage across requirement types

Modern RTM Practices:

- Automated integration with Jira, Azure DevOps, and TestRail
- Real-time dashboards showing coverage gaps
- Continuous updates in Agile/DevSecOps environments

Indian Context:

- Essential for distributed teams across multiple development centres
- Required for regulatory documentation and audit trails

Exam Tip: RTM ensures every requirement has test cases. It's bidirectional tracing - requirements to tests AND tests to requirements.

Cloud and Hybrid Environment Auditing

IaaS Auditing:

- Customer: OS, applications, data

- Provider: Physical infrastructure, hypervisor

PaaS Auditing:

- Customer: Applications, data
- Provider: OS, middleware, runtime, infrastructure

SaaS Auditing:

- Customer: Data, user access management
- Provider: Everything else (application, platform, infrastructure)

Hybrid Environment Challenges:

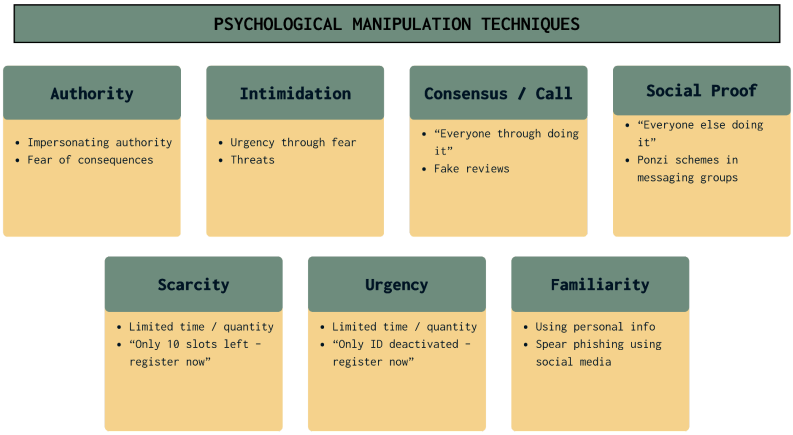
- Consistent security across on-premise and cloud
- Secure connectivity and data synchronisation
- Identity federation and API security
- Data residency compliance (especially critical in India)
- Coordinated incident response across environments

Indian Context:

- Government cloud (MeghRaj) auditing for e-governance applications
- Data localisation requirements under the IT Act and the DPDP Act
- Auditing multi-cloud deployments across Indian and global data centres

Exam Tip: The Shared Responsibility Model varies by service level. In IaaS, you audit more; in SaaS, you audit less. Know who's responsible for what.

Social Engineering Testing Techniques



Psychological Manipulation Techniques:

- Authority: Impersonating authority figures (most effective with impersonation, whaling, vishing)
- Intimidation: Creating urgency through fear of consequences
- Consensus/Social Proof: "Everyone else is doing it" mentality
- Scarcity: Limited time/quantity offers (FOMO)
- Urgency: Immediate action required, bypasses rational thinking
- Familiarity: Building rapport using personal information from social media

Testing Approaches:

- War Dialling: Historical modem access technique (exam-relevant, largely obsolete)

- War Driving: Mapping wireless access points, identifying insecure networks
- Physical Social Engineering: Tailgating, dumpster diving, USB drop tests, impersonation
- Phishing Campaigns: Email-based testing with click-through and credential submission tracking

Indian Context:

- Fake "regulatory official" calls targeting bank customers
- Ponzi schemes are spreading through WhatsApp groups using social proof
- Phishing attacks impersonating government agencies (tax, Aadhaar)

Exam Tip: War dialling is obsolete, but on the exam. Social engineering exploits psychology, not technology. Authority and Urgency are most common.

Security Metrics: Account Management

Key Performance Indicators:

- Account provisioning time
- Deprovisioning compliance rate (target: within 24 hours of termination)
- Orphaned account detection rate
- Privilege escalation frequency

Manager Responsibilities (NIST 800-53r5):

- System account managers: Create and manage accounts

- Employee managers: Approve access requests, notify of role changes within 24 hours

Indian Context:

- Critical for organisations with high employee turnover (BPO, IT services)
- Regulatory requirement for timely access revocation

Exam Tip: 24-hour rule for deprovisioning and role change notification. Orphaned accounts are a major security risk.

Backup Verification Metrics

Key Metrics:

- RPO (Recovery Point Objective): Maximum acceptable data loss measured in time
- RTO (Recovery Time Objective): Maximum acceptable downtime
- WRT (Worst-Case Recovery Time): Maximum possible recovery time accounting for Murphy's Law

Verification Requirements:

- "You don't have a backup until you've restored it"
- Regular restoration drills are required
- Ransomware recovery validation is essential

Indian Context:

- Stock exchanges maintain near-zero RPO (real-time replication)

- Payment systems require RTO in minutes for business continuity
- Rising ransomware attacks make backup testing critical

Exam Tip: RPO = data loss, RTO = downtime. Always test backups through restoration - verification without testing is worthless.

Vulnerability Disclosure Models

Disclosure Approaches:

- Private Disclosure: Inform vendor privately, allow time for patch development (standard responsible disclosure)
- Full Disclosure: Release details publicly immediately (controversial, forces vendor action, enables attacks)
- Coordinated Disclosure: Work with vendor on timeline, coordinate patch and disclosure (industry best practice)

Ethical Responsibilities:

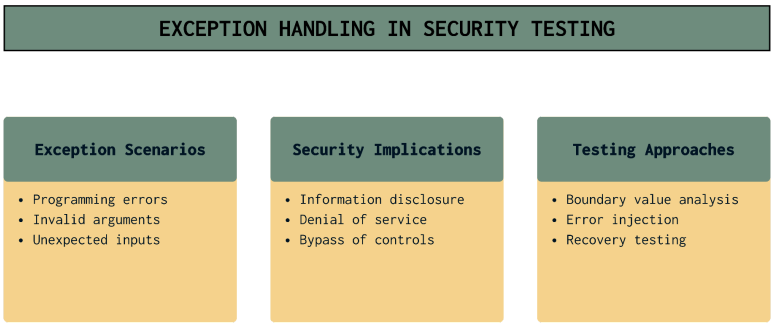
- Act in the public interest
- Maintain appropriate confidentiality
- Report vulnerabilities responsibly
- Avoid causing harm
- Implement compensating controls while waiting for patches

Indian Context:

- CERT-In provides a vulnerability disclosure framework
- Security researchers must follow responsible disclosure for national ID/critical infrastructure vulnerabilities

Exam Tip: Coordinated disclosure balances transparency and security. Full disclosure is controversial. Always follow responsible disclosure.

Exception Handling Testing



Exception Scenarios:

- Programming errors (divide by zero, null pointer)
- Invalid arguments and unexpected inputs
- Resource exhaustion
- State corruption

Security Implications:

- Information disclosure through verbose error messages
- Denial of service potential
- Bypass of security controls
- System state corruption

Testing Approaches:

- Boundary value analysis
- Error injection testing
- Resource exhaustion tests
- Recovery testing

Exam Tip: Poor exception handling reveals system information and can bypass security controls. Test all error paths.

Testing Best Practices Summary

Risk-Based Testing:

- Focus on high-value assets and critical systems
- Consider threat likelihood and business impact
- Allocate resources based on risk prioritisation

Defence in Depth Validation:

- Test multiple security layers
- Verify compensating controls
- Ensure no single point of failure

Documentation Standards:

- Clear scope definition with authorisation
- Detailed findings with CVSS ratings
- Actionable remediation recommendations
- Executive summaries for management

Legal and Compliance:

- Always obtain written authorisation before testing
- Understand legal boundaries and jurisdiction
- Respect data privacy regulations (IT Act 2000, DPDP Act)
- Consider data localisation requirements

Indian Context:

- Compliance with IT Act 2000 Section 43, 66, 70 (unauthorised access penalties)
- DPDP Act 2023 implications for testing with personal data
- National Critical Information Infrastructure Protection Centre (NCIIPC) guidelines for critical infrastructure

Exam Tip: Authorisation comes FIRST before any testing. Risk-based prioritisation optimises limited resources.

Key Exam Distinctions

Critical Differences:

- Validation (right product) vs Verification (product right)
- Static (code without running) vs Dynamic (running application)
- Assessment (identifies) vs Testing (exploits/validates)
- Audit (measures against standards) vs Review (examines configurations)
- Type 1 (design at point-in-time) vs Type 2 (operating effectiveness over time)
- Black Box (no knowledge) vs White Box (full knowledge) vs Grey Box (partial knowledge)
- Internal (insider perspective) vs External (outsider perspective)
- Credentialed (authenticated) vs Uncredentialed (unauthenticated) scans

- RPO (data loss) vs RTO (downtime)

Exam Tip: Know these distinctions cold. Many exam questions test your ability to differentiate between similar concepts.

Key Takeaways for Exam

Essential Knowledge:

- SAST = white-box, static code analysis; DAST = black-box, running application testing
- Penetration testing phases: Planning, Reconnaissance, Scanning, Vulnerability Assessment, Exploitation, Reporting
- SCAP framework: CVE (naming), CVSS (scoring), CCE (config), CPE (products), XCCDF (checklists), OVAL (testing)
- SOC 2 Type 2 = most valuable security audit (tests operating effectiveness over time)
- Requirements Traceability Matrix maps requirements to test cases bidirectionally
- Shared Responsibility Model varies by cloud service type (IaaS/PaaS/SaaS)
- Social engineering exploits psychology using Authority, Urgency, Scarcity, and Familiarity
- PCI-DSS: Quarterly vulnerability scans, annual penetration testing
- Continuous scanning is the modern best practice; periodic scanning is the compliance minimum

Common Exam Traps:

- War dialling appears on the exam despite being obsolete - know it

- Don't confuse vulnerability assessment (broad identification) with penetration testing (deep exploitation)
- Type 1 audits don't verify operational effectiveness - only Type 2 does
- Black box testing is most realistic but most time-consuming
- SCAP components - memorise what each acronym means and does
- Authorisation required before ANY testing - legal liability if skipped

Remember: This domain is 12% of the exam. Focus on testing methodologies, audit types, SCAP framework, and legal/ethical considerations.

Domain 7: Security Operations

Overview

Key Points:

- Security Operations = practical implementation of cybersecurity in day-to-day activities
- Covers operational aspects: maintaining security posture, responding to incidents, ensuring business continuity
- Bridges the gap between security policies and real-world implementation
- Exam weight: 13% of the CISSP examination

Exam Tip: Security Operations is about DOING security, not just planning it. Focus on processes, timelines, and who does what.

Administrative Personnel Security Controls

Principle of Least Privilege

Key Points:

- Give users the minimum access needed to perform job functions
- Prevents privilege creep (accumulation of permissions over time)
- Implementation: DAC, MAC, or RBAC systems
- Requires regular access reviews and time-limited privileges

Exam Tip: Least Privilege = "minimum necessary access." Different from Need to Know, which is about information boundaries.

Need to Know Principle

Key Points:

- Access to information based on specific job requirements
- Focuses on information boundaries, not just system permissions employee may have clearance but should only view data relevant to the current assignment
- Least Privilege = what doors you CAN open; Need to Know = which doors you SHOULD enter

Exam Tip: High clearance ≠ automatic access to all information. Need to Know adds a second layer of restriction.

Separation of Duties (SoD)

Key Points:

- Prevents a single person from having complete control over critical processes
- Requires conspiracy rather than individual action for fraud
- Implementation: Transaction authorisation, system administration, development vs. production
- Improves error detection through multiple validation checkpoints

Indian Context:

- RBI requires different individuals for loan origination and approval
- Government procurement mandates separate officials for request, evaluation, and approval

Exam Tip: SoD prevents fraud; it requires collusion of multiple people to compromise the process.

Job Rotation

Key Points:

- Regularly rotating employees through different positions
- Prevents long-term fraudulent schemes
- Distributes knowledge (prevents single points of failure)
- Fresh eyes often discover discrepancies left by predecessors

Indian Context:

- Government and banks follow a mandatory 2-3 year rotation for sensitive positions

Exam Tip: Rotation is PREVENTIVE (stops fraud from starting) and DETECTIVE (new person finds issues).

Mandatory Leave/Forced Vacation

Key Points:

- Detective control requiring consecutive leave (10-14 days)
- Fraudulent activities often require daily maintenance to hide
- Employee must have NO system access during leave
- Someone else fully takes over responsibilities during the absence

Indian Context:

- RBI mandates 10 consecutive working days leave annually for banking employees in sensitive positions

Exam Tip: Mandatory leave is DETECTIVE control; it exposes fraud when the perpetrator cannot maintain concealment.

Non-Disclosure Agreements (NDAs)

Key Points:

- Legal foundation for protecting confidential information
- Components: definition of confidential info, permitted use, duration (2-5 years post-employment), penalties
- Enforceable under contract law and the IT Act
- Whistleblower provisions override NDAs for reporting illegal activities

Background Verification

Key Points:

- Educational verification (critical due to fake degrees)
- Employment history and criminal record checks
- Financial background for financial positions
- Depth varies by role: Level 1 (Basic), Level 2 (Enhanced), Level 3 (Comprehensive)

Privileged Account Management (PAM)

Key Points:

- MFA is mandatory for all privileged accounts

- Just-In-Time access (granted only when needed, auto-revoked)
- Session recording for all privileged sessions
- Dedicated Privileged Access Workstations
- Real-time alerting for suspicious privileged activity

Exam Tip: Privileged accounts = "keys to the kingdom." Require enhanced security beyond standard users.

Digital Forensics and Investigations

Digital Forensic Process

Identification Phase:

- Identify systems, media, and data relevant to the investigation
- Document the initial state of all digital devices
- Consider cloud storage and social media accounts

Preservation Phase:

- Create forensically sound copies using write-blockers
- Generate cryptographic hashes (MD5, SHA-256) for integrity
- Document the chain of custody meticulously

Indian Context:

- Section 65B certification crucial for electronic evidence admissibility in Indian courts

Collection Phase (Order of Volatility):

- CPU registers and cache
- RAM contents
- Network connections
- Running processes
- Disk drives
- Backup media

Examination and Analysis Phase:

- Analyse collected data for relevant evidence
- Reconstruct timelines and user activities
- Identify deleted or hidden data

Presentation Phase:

- Prepare reports for technical and non-technical audiences
- Include Section 65B certificate for electronic evidence
- Expert witnesses explain technical findings clearly

Exam Tip: Chain of custody MUST remain unbroken from crime scene to courtroom. Order of volatility: most volatile first (RAM before disk).

Types of Forensic Data

Key Points:

- Allocated Space: Active data visible to OS
- Unallocated Space: Areas marked available; often contains deleted files not yet overwritten
- Slack Space: Unused space within allocated clusters; can contain remnants of previous data

- Bad Blocks/Sectors: Areas marked defective; attackers may artificially mark to hide data

Exam Tip: Unallocated and slack space are goldmines for forensic investigators deleted data lives here.

Network Forensics

Key Points:

- Catch-it-as-you-can: Capture all traffic for later analysis (requires substantial storage)
- Stop, look, and listen: Real-time analysis with selective storage

Indian Context:

- Interception requires authorisation under the IT Act Section 69
- Organisations can monitor their own networks with proper policies

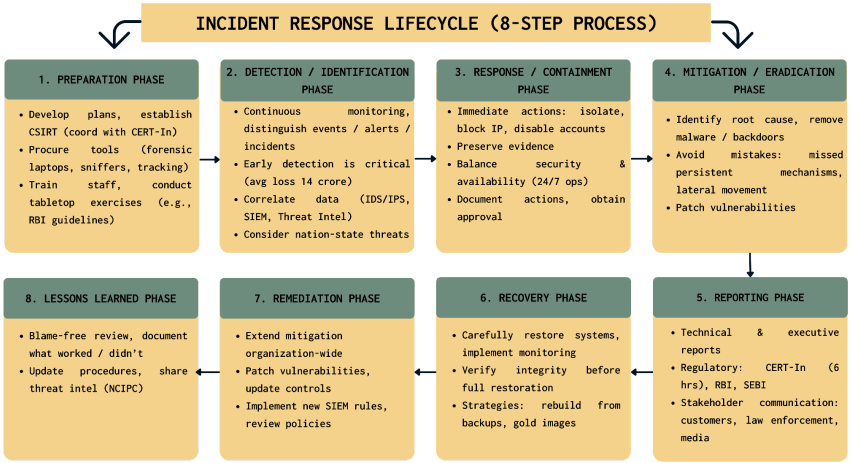
E-Discovery

Key Points:

- EDRM Process: Information Governance → Identification → Preservation → Collection → Processing → Review → Analysis → Production → Presentation
- Legal hold implementation to preserve ESI (Electronically Stored Information)
- De-duplication to reduce data volume

Exam Tip: E-discovery is a civil litigation discovery process for electronic records. Different from criminal forensics, but it uses the same preservation techniques.

Incident Management



Incident Response Lifecycle (8 Phases)

1. Preparation:

- Develop incident response plans
- Establish CSIRT (Computer Security Incident Response Team)
- Procure tools: forensic laptops, write-blockers, network sniffers, incident tracking systems
- Conduct tabletop exercises

Indian Context:

- Coordinate with CERT-In (Indian Computer Emergency Response Team)

2. Detection/Identification:

- Continuous monitoring for security events
- Distinguish between events, alerts, and actual incidents
- Correlation of IDS/IPS alerts, SIEM notifications, user reports, and threat intelligence

3. Response/Containment:

- Isolate affected systems
- Block malicious IP addresses
- Disable compromised accounts
- Preserve evidence for investigation
- Balance security with availability

4. Mitigation/Eradication:

- Identify root cause
- Remove malware and backdoors completely
- Patch vulnerabilities that enabled an attack
- Check for lateral movement

5. Reporting:

- Technical reporting for IT teams
- Executive summaries for management
- Regulatory reporting (CERT-In: within 6 hours; RBI for banks; SEBI for listed companies)
- Communication with customers, law enforcement, media

Indian Context:

- CERT-In mandate: Report incidents within 6 hours

6. Recovery:

- Restore systems from clean backups or gold master images
- Implement additional monitoring during recovery
- Verify system integrity before full restoration
- Gradual service restoration

7. Remediation:

- Extend mitigation beyond affected systems
- Organization-wide patching
- Update security controls based on lessons learned
- Implement new SIEM detection rules

8. Lessons Learned:

- Conduct blame-free post-incident review
- Document what worked and what didn't
- Update incident response procedures
- Share threat intelligence with industry peers

Exam Tip: Know all 8 phases in order. Containment comes BEFORE eradication. Reporting happens during response, not just at the end.

Root Cause Analysis

Key Points:

- Prevents incident recurrence by identifying underlying vulnerabilities

- Techniques: 5 Whys Method, Fishbone Diagram, Timeline Analysis, Fault Tree Analysis
- Common root causes: unpatched systems, weak passwords, insufficient training, shadow IT, and third-party vendor vulnerabilities.

Exam Tip: Root cause analysis finds WHY the incident happened, not just WHAT happened.

Preventive and Detective Controls

Intrusion Detection and Prevention Systems (IDS/IPS)

Network-Based (NIDS/NIPS):

- Deployed at the network perimeter and critical segments
- Monitor traffic patterns for suspicious activity
- Detect port scans, malware communication, data exfiltration, and DDoS attacks

Host-Based (HIDS/HIPS):

- Installed on critical servers and workstations
- Monitor system calls, file integrity, and log files
- Detect privilege escalation, unauthorised file modifications, and suspicious processes

Detection Methodologies:

- Signature-Based: Matches against known attack patterns; fast and accurate for known threats; ineffective against zero-day threats
- Anomaly-Based: Establishes a baseline of normal behaviour; detects deviations; can identify zero-day; higher false positive rate

Exam Tip: IDS = detective (alerts only). IPS = preventive (blocks attacks). Know the difference.

False Positives vs. False Negatives

Predicted Class \ Actual Class	Positive	Negative
Positive	True Positive (TP) - Correctly predicted positive (e.g., sick person tests positive)	False Positive (FP) - Incorrectly predicted positive (Type I Error; e.g., healthy person tests positive)
Negative	False Negative (FN) - Incorrectly predicted negative (Type II Error; e.g., sick person tests negative)	True Negative (TN) - Correctly predicted negative (e.g., healthy person tests negative)

Key Points:

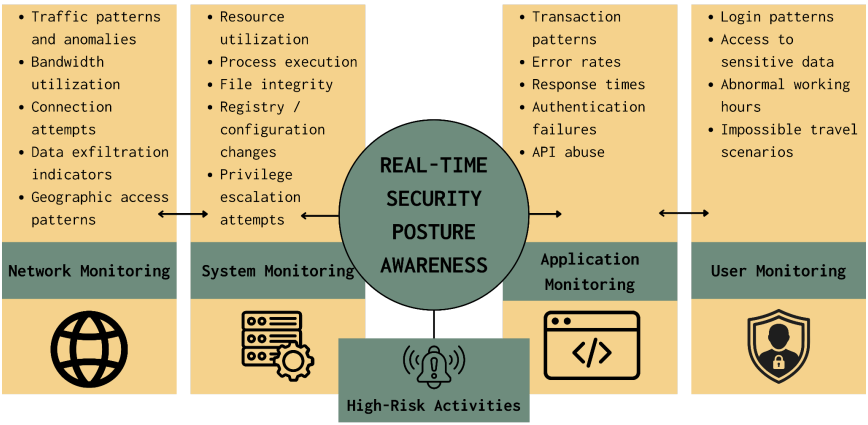
- False Positive (FP): Alert incorrectly flags benign activity as an attack (cry wolf problem; causes alert fatigue)
- False Negative (FN): System misses actual attack (more dangerous; undetected breaches)
- True Positive (TP): Alert correctly identifies actual attack
- True Negative (TN): System correctly allows legitimate activity

Impact:

- High false positives → alert fatigue → analysts ignore real threats
- False negatives → undetected breaches → maximum damage

Exam Tip: A False Negative is worse than a False Positive. Missing real attack > crying wolf.

SIEM (Security Information and Event Management)



Key Points:

- "Single pane of glass" for security monitoring
- Capabilities: log collection, normalisation, correlation, alerting, reporting, retention
- Collects from: Windows/Linux servers, network devices, security appliances, applications, cloud services

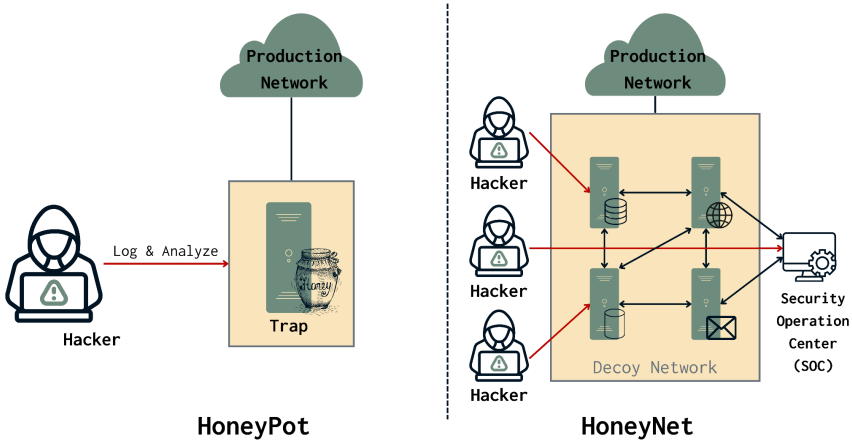
- Real-time notification of security events

Indian Context:

- Compliance with IT Act log retention requirements
- Integration with India Stack services

Exam Tip: SIEM = correlation engine. Connects dots across multiple log sources to detect attacks that no single log shows.

Honeypots and Honeynets



Key Points:

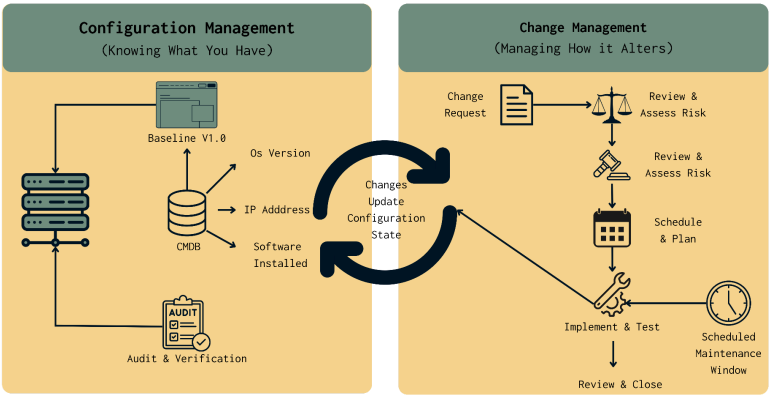
- Decoy systems to attract and study attackers
- External Honeypots: Placed in DMZ; simulate vulnerable services; early warning
- Internal Honeypots: Deployed within the internal network; detect lateral movement and insider threats
- Should NEVER contain real data

Indian Context:

- Legal considerations: Entrapment vs. Enticement
- Liability if a honeypot is used to attack others
- Always consult the legal team before deployment

Exam Tip: Honeypot = deception technology. Legitimate users have no reason to access it; any access = investigation.

Configuration and Change Management



Configuration Management

Key Points:

- Ensures systems maintain secure baselines throughout the lifecycle
- Baseline establishment: Vendor security guides + organisational customisation + compliance requirements

- Hardening process: Remove unnecessary services, disable unused ports, configure security settings, apply patches, and implement logging
- Configuration drift detection: Automated scanning comparing current vs. approved baselines
- Tools: Ansible, Puppet, Chef, SCCM

Configuration Management Database (CMDB)

Key Points:

- Single source of truth for all IT assets and relationships
- Configuration Items (CIs): Hardware, software, documentation, services, locations
- Relationships: Physical dependencies, logical dependencies, business dependencies
- Attributes: Identification, ownership, lifecycle, compliance

Exam Tip: CMDB tracks WHAT you have and HOW it's configured. Critical for impact analysis during changes.

Documentation and Approval Requirements

Mandatory Documentation:

- Change Request ID
- Business justification
- Technical details
- Impact assessment
- Risk analysis
- Testing evidence
- Rollback procedures

- Implementation timeline

Multi-Level Approval Framework:

- Level 1 - Technical Approval: System administrators verify technical accuracy
- Level 2 - Service Approval: Service owners confirm business alignment
- Level 3 - Security Approval: Security team validates compliance
- Level 4 - Executive Approval: Senior management for high-impact changes

Exam Tip: Documentation and approval are MANDATORY. Undocumented changes = unauthorised changes.

Change Advisory Board (CAB)

Key Points:

- Governance oversight for IT changes
- Core Members: Change Manager, IT Service Manager, Security Manager, Business Representative, Technical Architect
- Extended Members: SMEs, Vendor Reps, Compliance Officers (invited as needed)
- Reviews: risk assessment, resource availability, conflict detection

Change Types:

- Standard Changes: Pre-approved, low-risk with documented procedures (auto-approval)

- Normal Changes: Standard approval process through designated authorities
- High-Risk Changes: Enhanced approval with CAB review and executive sign-off
- Emergency Changes: Expedited approval with post-implementation review

Exam Tip: CAB reviews NORMAL and HIGH-RISK changes. Standard changes are pre-approved. Emergency changes get fast-tracked but still need post-review.

Patch Management

Patch Management Lifecycle:

- Identification: Monitor vendor advisories
- Classification: Critical (24-48 hours), High (1 week), Medium (1 month), Low (next window)
- Testing: Verify patches don't break systems
- Deployment: Staged rollout
- Verification: Confirm successful installation
- Documentation: Update configuration records

Indian Context:

- Average 97 days to patch critical vulnerabilities
- The 2017 WannaCry outbreak affected many unpatched Indian organisations

Exam Tip: Test patches before deployment. Staged rollout minimises risk. Critical patches within 24-48 hours.

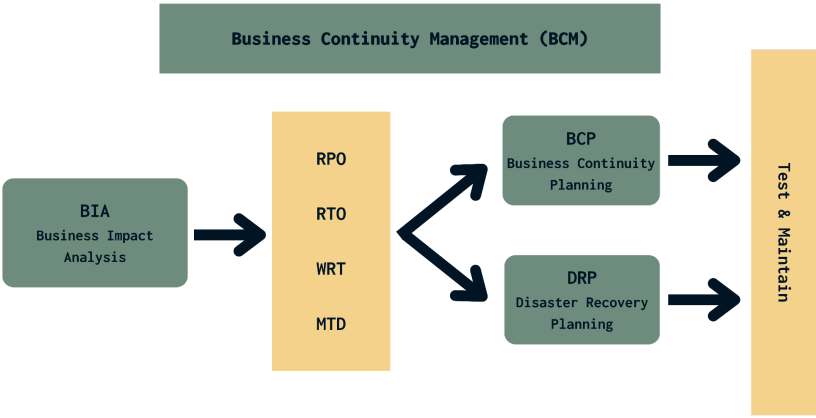
Zero-Day Vulnerability Management

Key Points:

- Zero-day vulnerability: Unknown to the vendor
- Zero-day exploit: Code targeting the vulnerability
- Zero-day attack: Active exploitation
- Mitigation: Defence in depth, behavioural detection, network segmentation, application sandboxing, virtual patching through IPS/WAF

Exam Tip: Can't patch zero-days (no patch exists). Use compensating controls: segmentation, IPS, and behavioural detection.

Business Continuity and Disaster Recovery



Business Continuity Management (BCM)

Key Components:

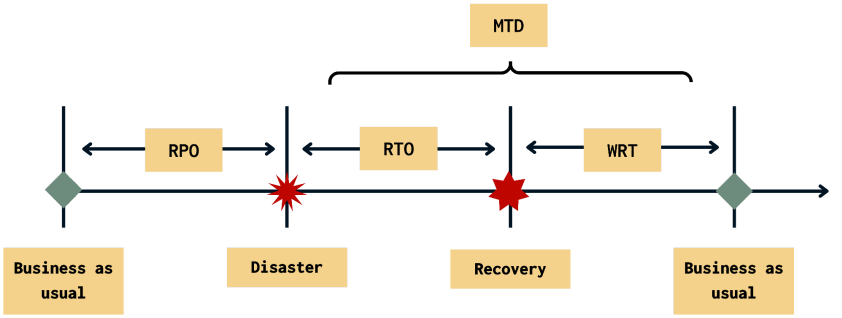
- BCP (Business Continuity Planning): Long-term strategic planning for organisational resilience
- DRP (Disaster Recovery Planning): Tactical IT system recovery procedures
- Crisis Management: Leadership and decision-making during emergencies
- Emergency Response: Immediate actions to protect life and property

Indian Context:

- Natural disasters: Cyclones, earthquakes, floods (monsoon)
- Human-caused: Cyber attacks, terrorism
- Environmental: Power grid failures, internet cable cuts

Exam Tip: BCP = strategic (whole organisation). DRP = tactical (IT systems). BCP is broader than DRP.

Business Impact Analysis (BIA)



- **RPO** : Recovery Point Objective
- **RTO** : Recovery Time Objective
- **WRT** : Work Recovery Time
- **MTD** : Maximum Tolerable Downtime

Key Metrics:

- MTD (Maximum Tolerable Downtime): Total time the system can be down before irreparable harm
- RTO (Recovery Time Objective): Time to restore hardware and systems
- WRT (Work Recovery Time): Time to configure and verify recovered systems
- RPO (Recovery Point Objective): Maximum acceptable data loss measured in time
- Relationship: MTD = RTO + WRT

Indian Sector Requirements:

- Banking (RBI): Core banking RTO < 2 hours, RPO < 15 minutes
- Stock exchanges (SEBI): Trading systems RTO < 30 minutes, near-zero RPO
- Telecom (TRAI): Network availability > 99.5%

Exam Tip: MTD = business limit. RTO = IT target. RTO must be less than MTD. RPO determines backup frequency.

Recovery Sites

Recovery Site Type	Description	RTO	Replication	Used By / Examples	Cost / Notes	
Redundant Site	Exact replica with zero downtime and failover	Zero	Real-time	Stock exchanges, major banks	Highest cost; near-zero RTO/RPO	
Hot Site	Fully equipped, ready to operate	< 4 hours	Near real-time	Tier-1 banks, stock exchanges	Very high cost	
Warm Site	Equipment available; data restored from backups	24-72 hours	Restored from backups	Mid-size enterprises, government departments	Medium cost	
Cold Site	Facility only; no equipment	Weeks	None (data from offsite backups)	Rare in India due to procurement delays	Lowest cost	
Reciprocal Agreement	Mutual aid between organizations	Variable	Varies	PSU banks, government departments	Low cost; depends on partner	
Mobile Sites	Containerized / portable data centers	Variable	Varies	Temporary recovery locations	Used during disasters/lockdowns	
Cloud-based Recovery (DRaaS)	Disaster Recovery as a Service	Minutes to hours	Cloud replication	Indian startups, AWS/Azure users	Growing adoption; concerns: data residency & compliance	

Recovery Site Options:

- Redundant Site: Replica, real-time replication, zero downtime, highest cost (100% of primary)
- Hot Site: Fully equipped, ready to operate, RTO < 4 hours, near real-time replication
- Warm Site: Equipment available, needs configuration, RTO 24-72 hours, data restored from backups
- Cold Site: Facility only, no equipment, RTO weeks, lowest cost
- Reciprocal Agreements: Mutual aid between organisations; challenges with compatibility
- Mobile Sites: Containerised data centres; useful for temporary recovery
- Cloud-based Recovery: DRaaS (Disaster Recovery as a Service); growing adoption

Indian Context:

- NSE (stock exchange) maintains a fully redundant DR site

- Common among PSU banks and the government for reciprocal agreements

Exam Tip: Redundant/Hot for critical (financial). Warm for mid-size. Cold is rarely used due to long RTO. Match the site to the MTD requirement.

Backup Strategies

Backup Types:

- Full Backup: Complete copy of all data; clears archive bits; recovery needs 1 tape
- Incremental Backup: Changes since last backup (any type); clears archive bits; recovery needs full + all incrementals
- Differential Backup: Changes since last full; doesn't clear archive bits; recovery needs full + latest differential

Recovery Comparison:

- Full backup Sunday, daily incrementals Monday-Wednesday, recovery Thursday needs: Sunday + Monday + Tuesday + Wednesday (4 tapes)
- Full backup Sunday, daily differentials Monday-Wednesday, recovery Thursday needs: Sunday + Wednesday (2 tapes)

3-2-1 Backup Rule:

- 3 copies of important data
- 2 different storage media types
- 1 offsite copy

Indian Context:

- RBI: Financial data retention 10 years
- GST: Invoice data 6 years
- Companies Act: Board meeting records are permanently

Exam Tip: Incremental = fastest backup, slowest recovery. Differential = balanced. Full = slowest backup, fastest recovery.

Specialised Recovery Techniques

Key Points:

- Remote Journaling: Transaction logs sent to a remote site; can reconstruct the database; lower bandwidth
- Database Shadowing: Real-time replication to shadow database; immediate failover; minimal data loss
- Electronic Vaulting: Automated backup to a remote location; scheduled or triggered

Exam Tip: Journaling < Shadowing in terms of data currency but lower cost. Shadowing = near-zero RPO.

RAID Technologies

RAID Level	Technique	Fault Tolerance	Capacity Efficiency	Performance	Pros	Cons
RAID 0	Striping	None	100%	Very High	High performance, full capacity	No redundancy, failure = data loss
RAID 1	Mirroring	1 disk	50%	Fast read, slower write	Fault tolerance, fast reads	50% capacity, slower writes
RAID 5	Distributed parity	1 disk	~67%	Good read, slower write	Balanced performance, good capacity	Slower writes due to parity
RAID 6	Dual distributed parity	2 disks	~50~67%	Good read, slower write	High fault tolerance, survives 2 failures	Slower writes, lower capacity
RAID 10	Stripe of mirrors	1 disk per mirror	50%	Very High	High performance, high fault tolerance	High cost, 50% capacity

Common RAID Levels:

- RAID 0 (Striping): No redundancy, performance only; single disk failure loses all data
- RAID 1 (Mirroring): Complete duplication; 50% storage efficiency; tolerates one disk failure
- RAID 5 (Striping with Parity): Balance of performance/redundancy/cost; tolerates one disk failure; minimum 3 disks
- RAID 6 (Dual Parity): Tolerates two disk failures; important for large storage arrays
- RAID 10 (1+0): Mirroring + Striping; high performance and redundancy; 50% efficiency; expensive

Exam Tip: RAID 0 = no redundancy (risky). RAID 1 = mirroring. RAID 5 = most common (parity). RAID 6 = dual parity. RAID 10 = performance + redundancy.

Testing and Maintenance

Testing Methodologies (Progressive Confidence):

- Document Review: Basic completeness check; quarterly; low confidence
- Walkthrough/Tabletop: Discussion-based; identifies procedure issues; bi-annual
- Simulation: Simulated disaster scenario; tests communication/coordination; annual minimum
- Parallel Processing: Run recovery systems alongside production; high confidence
- Full Interruption: Complete failover to recovery site; highest confidence but risky; rarely done

Exam Tip: Test regularly. Untested plan = no plan. Document Review < Walkthrough < Simulation < Parallel < Full Interruption (increasing confidence and risk).

Crisis Management

Key Points:

- Emergency Operations Centre (EOC): Centralised command/control, communication hub, decision-making authority
- Call Trees: Hierarchical notification; each person calls 2-3 others; redundancy in paths
- Automated Notification: Mass notification systems (SMS, voice, email, app)
- Stakeholder management: employees, customers, suppliers, regulators, media

Indian Context:

- WhatsApp groups for faster communication

- Coordination with local administration and district collectors

Security Operations Metrics and Monitoring

Mean Time Metrics (Critical for Exam)

MTTD (Mean Time to Detect):

- Average time from incident occurrence to detection
- Global average: 378 days; Indian average: 225 days; Best practice: < 24 hours
- Improvement: SIEM, EDR, threat hunting, behavioural analytics

MTTR (Mean Time to Respond):

- Average time from detection to containment
- Target by severity: Critical (< 15 min), High (< 1 hour), Medium (< 4 hours), Low (< 24 hours)
- SOAR platforms reduce MTTR by 50-70%

MTTE (Mean Time to Eradicate):

- Average time from detection to complete threat removal
- Includes malware removal, backdoors closed, and credentials rotated
- Target: < 7 days most incidents, < 24 hours critical threats

MTTI (Mean Time to Investigate):

- Average time investigating and analysing incidents

- Target: < 30 minutes automated triage, < 4 hours detailed investigation

Dwell Time:

- Duration attacker remains undetected
- Externally detected: 54 days; Internally detected: 17 days
- Goal: Reduce to < 7 days

Exam Tip: MTTD = detection capability. MTTR = response speed. MTTE = complete cleanup. Lower is better for all.

Detection Accuracy Metrics

Key Metrics:

- Precision = TP / (TP + FP): Of all alerts, what % are real? (measures false positive rate)
- Recall = TP / (TP + FN): Of all attacks, what % were detected? (measures detection capability)
- F1 Score = 2 × (Precision × Recall) / (Precision + Recall): Balanced measure; > 80% excellent, 60-80% good, < 60% poor

Targets:

- Precision > 60% (< 40% false positives)
- Recall > 90% for critical threats
- F1 Score > 0.6 for production use

Exam Tip: High Precision = fewer false alarms. High Recall = catch more attacks. F1 balances both. Know formulas.

Indian Regulatory Compliance Metrics

CERT-In 6-Hour Compliance:

- Report cybersecurity incidents within 6 hours
- Covers: data breaches, unauthorised access, malware, defacement, DDoS
- Target: 100% compliance
- Non-compliance: Legal penalties, regulatory scrutiny

RBI Cyber Incident Reporting:

- Report significant incidents within 2-6 hours by severity
- Monthly summary to the board

Exam Tip: Indian-specific; know the 6-hour CERT-In requirement for exam context questions.

Continuous Monitoring

Monitoring Domains:

- Network: Traffic patterns, bandwidth, connection attempts, data exfiltration, geographic access
- System: Resource utilisation, process execution, file integrity, configuration changes, privilege escalation
- Application: Transaction patterns, error rates, response times, authentication failures, API abuse
- User: Login patterns, sensitive data access, abnormal hours, impossible travel, high-risk activities

Exam Tip: Continuous monitoring = real-time security posture awareness. Automate monitoring; humans can't watch 24/7.

Emerging Challenges

Cloud Security Operations

Key Points:

- Multi-cloud management: different security models per provider
- Data residency and localisation requirements
- Cloud-native tools: CSPM, CWPP, CASB, Cloud SIEM

Indian Context:

- Indian data localisation laws impact cloud DR strategies

Supply Chain Security

Key Points:

- Third-party risk management: vendor assessments, continuous monitoring
- Software supply chain: code signing, dependency scanning, container security, CI/CD pipeline security
- Fourth-party risk consideration

IoT and OT Security

Key Points:

- Legacy systems without security features
- Availability over confidentiality priority
- Limited patching of windows
- Proprietary protocols

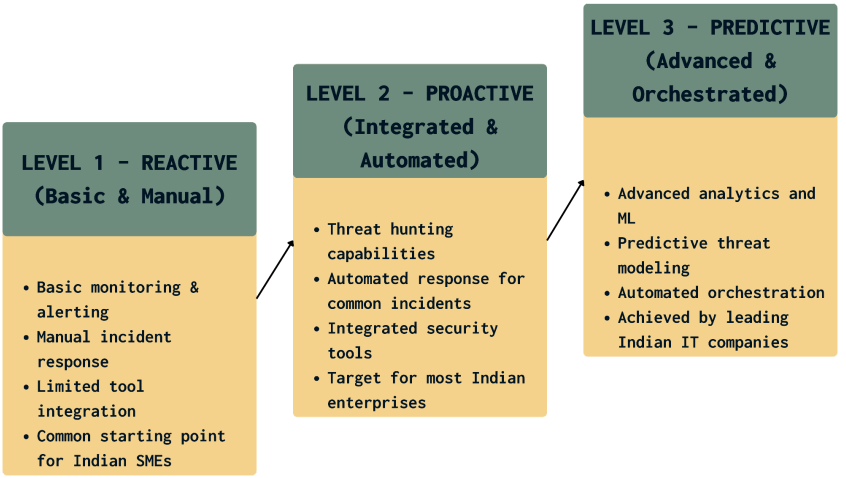
- Physical safety implications

Indian Context:

- Smart city initiatives, industrial automation, power grid modernisation, and smart meters

Practical Implementation

Building a SOC



SOC Maturity Levels:

- Level 1 - Reactive: Basic monitoring/alerting; manual response; limited integration
- Level 2 - Proactive: Threat hunting; automated response for common incidents; integrated tools
- Level 3 - Predictive: Advanced analytics/ML; predictive modelling; automated orchestration

Exam Tip: organisations target Level 2 (Proactive). Level 3 (Predictive) = advanced with ML/AI.

Key Exam Takeaways

Administrative Controls:

- Least Privilege = minimum access needed
- Need to Know = information boundaries
- Separation of Duties = prevents fraud through the multiple people requirement
- Job Rotation = preventive + detective
- Mandatory Leave = detective control

Forensics:

- The chain of custody must remain unbroken
- Order of volatility: most volatile first
- Section 65B certification for Indian court admissibility

Incident Response:

- 8 phases in order: Preparation → Detection → Response → Mitigation → Reporting → Recovery → Remediation → Lessons Learned
- CERT-In: Report within 6 hours

BCP/DRP:

- MTD = RTO + WRT
- RTO < MTD (always)
- RPO determines backup frequency

- Incremental = fast backup, slow recovery; Differential = balanced; Full = slow backup, fast recovery

Change Management:

- Documentation and approval are mandatory
- CAB for normal/high-risk changes
- Emergency changes need post-review

IDS/IPS:

- IDS = detective (alerts); IPS = preventive (blocks)
- Signature-based = known threats; Anomaly-based = zero-day
- False Negative > False Positive (missing an attack is worse than a false alarm)

Metrics:

- MTTD = detection capability
- MTTR = response speed
- Precision = TP/(TP+FP); Recall = TP/(TP+FN)
- F1 Score balances precision and recall

RAID:

- RAID 0 = no redundancy
- RAID 1 = mirroring
- RAID 5 = striping with parity (most common)
- RAID 6 = dual parity
- RAID 10 = mirroring + striping

CISSP Domain 8: Software Development Security

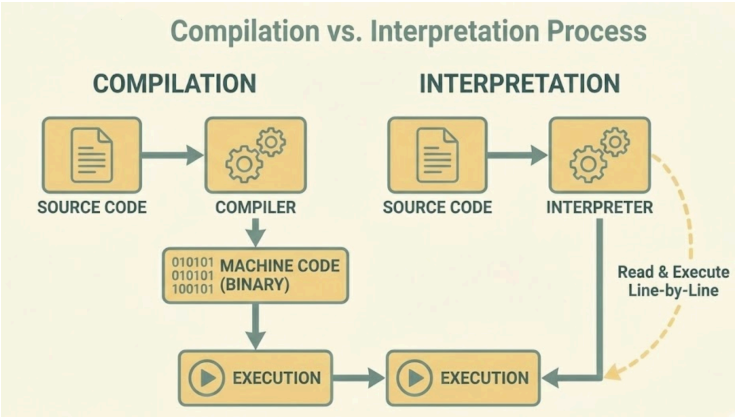
Overview

Key Points:

- 10% of the CISSP exam - critical domain
- Security must be "built in, not bolted on" - integrate at every SDLC phase
- Design flaws are costlier to fix than implementation bugs
- OWASP Top 10 2021 includes major changes: XSS merged into Injection, new categories added
- Parameterised queries = gold standard for SQL injection prevention

Exam Tip: Remember "SAST finds bugs in code, DAST finds bugs in runtime" - SAST is for early development, DAST for the testing phase.

Programming Concepts



Key Points:

- Machine Code: Binary (0s/1s), CPU-specific, maximum performance
- Assembly Language: Mnemonic instructions, one-to-one with machine code, platform-specific

- Compilers: Translate entire code before execution (C, C++, Rust) - faster runtime
- Interpreters: Translate line-by-line during execution (Python, JavaScript) - more flexible
- Bytecode: Middle ground - compile to bytecode, run on VM (Java, C#)

Programming Paradigms:

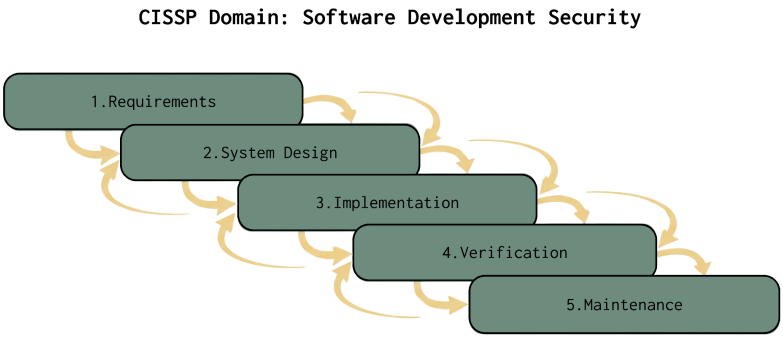
- Procedural: Sequential, functions separate from data (C, Pascal)
- Object-Oriented: Data + methods bundled (Java, Python, C++)
- 4GL: High-level, domain-specific (SQL, report generators)

Development Tools:

- IDE: Integrated environment with debugging, version control, and syntax highlighting
- CASE: Computer-Aided Software Engineering - tools, workbenches, environments

Exam Tip: "Compiler = whole meal prep before serving, Interpreter = cook as guests arrive"

Software Development Methodologies



Waterfall Model

Key Points:

- Sequential phases: Requirements → Analysis → Design → Coding → Testing → Operations
- Extensive documentation, limited flexibility
- Best for: Clear requirements, regulatory compliance, hardware dependencies
- Limitations: Rigidity, late integration issues, high cost of changes

Agile

Key Points:

- Core values: Individuals > processes, Working software > documentation, Customer collaboration > contracts, Responding to change > following plan
- Iterative 2-4 weeks sprints
- Continuous delivery and feedback
- Best for: Changing requirements, rapid delivery

Exam Tip: Waterfall = sequential phases, Agile = iterative sprints with continuous feedback

Scrum (Agile Framework)

Key Points:

- Roles: Product Owner (business value), Development Team (3-9 members), Scrum Master (facilitator)
- Events: Sprint Planning, Daily Stand-ups, Sprint Review, Sprint Retrospective
- Self-organising, cross-functional teams

Extreme Programming (XP)

Key Points:

- Pair Programming: Two developers, one computer - driver types, navigator reviews
- Test-Driven Development (TDD): Write tests before code - Red-Green-Refactor cycle
- Continuous Integration: Multiple daily integrations, automated testing
- Small releases, collective ownership, sustainable pace

Spiral Model

Key Points:

- Risk-driven development with iterative cycles
- Four quadrants: Planning → Risk Analysis → Engineering → Evaluation
- Best for: Large complex projects, unclear requirements, high-risk systems

RAD (Rapid Application Development)

Key Points:

- Phases: Requirements Planning → User Design → Construction → Cutover
- Visual tools, prototypes, code generators
- Best for: UI-critical projects, speed to market is crucial

DevOps & DevSecOps

Key Points:

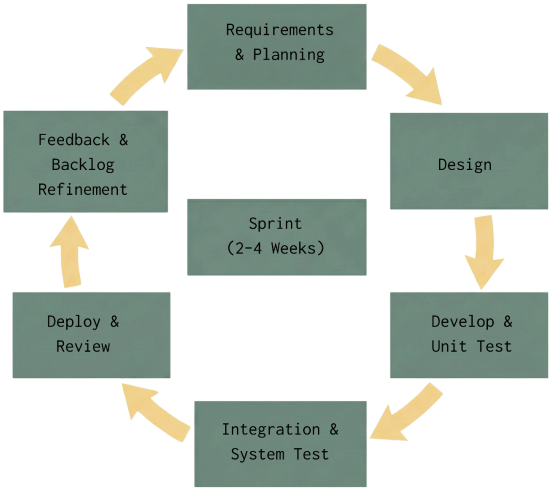
- CI/CD: Automated build, test, deploy - rapid production delivery
- Infrastructure as Code: Version-controlled infrastructure, automated provisioning
- DevSecOps: Security integrated throughout - threat modelling, automated security testing
- Breaks down silos between development and operations

Indian Context:

- Fintech deploys multiple times daily while maintaining PCI-DSS compliance

Exam Tip: DevSecOps = DevOps + Security integrated from day one, not bolted on later

SDLC Phases (Security Focus)



Key Points:

- Initiation/Planning: Threat modelling, security requirements, compliance analysis
- Development/Acquisition: Secure coding, vendor security assessment

- Implementation: Secure configuration, penetration testing, security monitoring
- Operations/Maintenance: Patch management, incident response, continuous monitoring
- Disposal: Data Sanitization, license management, and archival

Exam Tip: Every SDLC phase requires security - "security built in, not bolted on"

Databases

Relational Database Concepts

Key Points:

- Tables: Rows (records) and columns (attributes)
- Primary Key: Uniquely identifies each record, cannot be null
- Foreign Key: Links tables together, maintains relationships
- SQL: Universal language for database operations

Database Integrity

Key Points:

- Referential Integrity: Foreign keys match existing primary keys, preventing orphaned records
- Entity Integrity: Every table has a primary key, no nulls/duplicates in the primary key
- Semantic Integrity: Data values make contextual sense (types, ranges, formats)
- User-Defined Integrity: Business-specific rules, regulatory compliance

Indian Context:

- Banks use referential integrity for transaction consistency
- Telecom uses semantic integrity for mobile number validation

Database Normalization

Key Points:

- 1NF (First Normal Form): Eliminate repeating groups, atomic values only
- 2NF (Second Normal Form): Meets 1NF + no partial dependencies
- 3NF (Third Normal Form): Meets 2NF + no transitive dependencies
- Benefits: Reduced redundancy, improved integrity, easier maintenance

Exam Tip: Normalisation = organising data efficiently by eliminating redundancy

ACID Properties

Key Points:

- Atomicity: All-or-nothing - transactions complete entirely or not at all
- Consistency: Database moves from one valid state to another, and all rules are maintained
- Isolation: Transactions don't interfere with each other, preventing dirty reads
- Durability: Committed transactions survive system failures, and are persisted to storage

Exam Tip: ACID = financial transaction guarantee - money transfers complete fully or fail completely

Database Replication

Key Points:

- Master-Slave: One primary (writes), multiple secondaries (reads), auto-failover
- Master-Master: Multiple databases accept writes, synchronised, complex conflict resolution
- Two-Phase Commit: Phase 1 (Prepare) + Phase 2 (Commit/Abort) - consistency across distributed systems
- Shadow Databases: One-way backup, disaster recovery, minimal performance impact

Data Warehousing

Key Points:

- Subject-Oriented: Organised by business subjects (sales, customers)
- Integrated: Data from multiple systems, standardised formats
- Time-Variant: Historical data with timestamps for trend analysis
- Non-Volatile: Read-optimised, periodic batch loads
- Applications: Customer segmentation, fraud detection, predictive analytics

Alternative Database Models

Key Points:

- Hierarchical: Tree structure, parent-child (DNS, file systems)
- Network: Multiple parents allowed, more flexible than hierarchical

- Object-Oriented: Store objects directly with properties/methods (CAD/CAM)
- NoSQL: Document stores (MongoDB), Key-value (Redis), Column-family (Cassandra), Graph (Neo4j)

Exam Tip: NoSQL sacrifices some ACID properties for scalability and flexibility

Object-Oriented Programming (OOP)

Core OOP Principles

Key Points:

- Objects & Classes: Classes = blueprints, Objects = instances with unique values
- Encapsulation: Bundles data + methods, hides internals, controlled access (ATM interface)
- Inheritance: Child classes inherit from parents, promoting code reuse
- Polymorphism: Same method name, different behaviours for different objects
- Abstraction: Simplifies complexity by hiding unnecessary details

Advanced OOP Concepts:

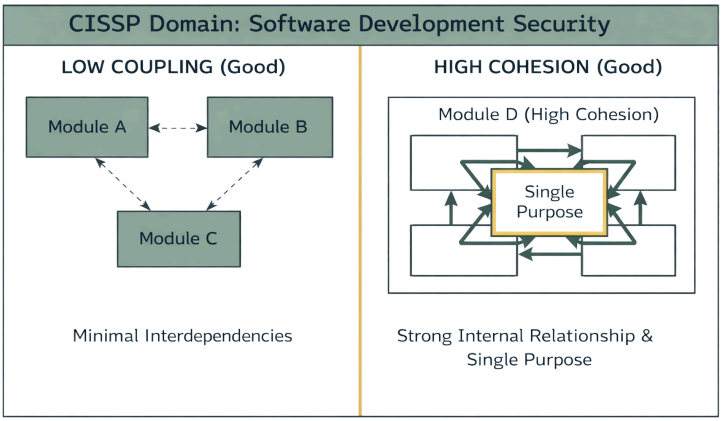
- Polyinstantiation: Multiple instances at different security levels (military systems)
- Delegation: Objects delegate tasks to suitable objects
- Messaging: Objects communicate through message passing

Object-Oriented Analysis & Design (OOAD)

Key Points:

- OOA (Analysis): Identify problem domain objects, attributes, relationships, operations
- OOD (Design): Define class hierarchies, interfaces, data structures, and security controls
- Design patterns solve common problems.

Coupling & Cohesion



Key Points:

- Coupling (Inter-module): LOW coupling = good (independent modules, localised changes)
- Cohesion (Intra-module): HIGH cohesion = good (related functionality grouped)
- Design Goal: Low coupling + high cohesion
- Types: Data coupling (best) → Content coupling (worst)

Exam Tip: Think "family bonds" - high cohesion (united goals) + low coupling (independent responsibilities)

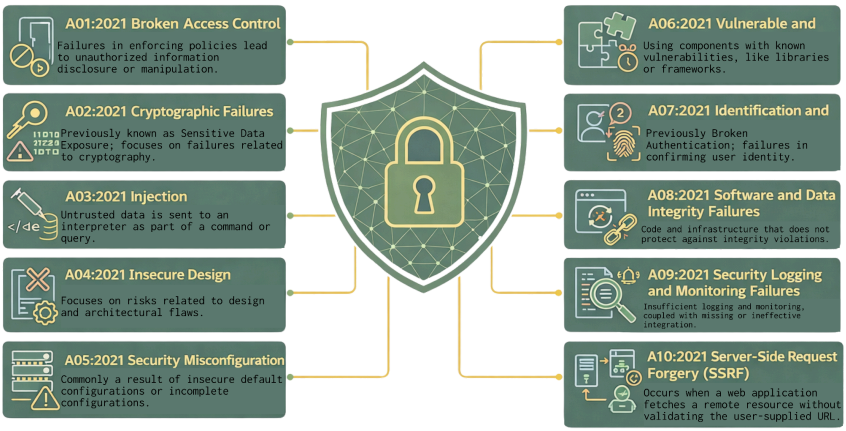
Object Request Brokers (ORBs)

Key Points:

- CORBA: Vendor-neutral, language-independent distributed objects
- COM/DCOM: Microsoft component architecture, single-machine (COM) or network (DCOM)
- Modern Alternatives: REST APIs, microservices, message queues, GraphQL, gRPC

Software Security: Vulnerabilities & Defences

OWASP Top 10 2021 - Major Changes



Key Points:

- NEW Categories: A04 Insecure Design, A08 Software & Data Integrity Failures, A10 SSRF
- Merged: XSS now part of A03 Injection (no longer standalone).
- Merged: XXE now part of A08 Software & Data Integrity Failures

- #1 Position: Broken Access Control (moved from #5)

Exam Tip: XSS and XXE are NO LONGER separate OWASP Top 10 categories as of 2021

A01: Broken Access Control

Key Points:

- Privilege escalation (horizontal/vertical), unauthorised data access
- IDOR (Insecure Direct Object References) - manipulating IDs
- Missing access checks on APIs
- Prevention: Deny by default, enforce ownership checks, disable directory listing, and rate limiting

Indian Context:

- E-commerce must prevent users from accessing other customers' order details via URL manipulation

A02: Cryptographic Failures

Key Points:

- Clear text transmission (HTTP, not HTTPS), weak algorithms (MD5, SHA1, DES)
- Missing encryption at rest, weak key management
- Prevention: Encrypt all sensitive data (transit + rest), use AES-256-GCM/SHA-256+, HSTS headers

Indian Context:

- RBI mandates encryption for payment card data
- DPDPA requires personal data encryption

A03: Injection (includes XSS)

Key Points:

- Types: SQL, NoSQL, OS Command, LDAP, XSS, Template, Expression Language
- Untrusted data sent to interpreter without validation/escaping

- Prevention: Parameterised queries, safe APIs, whitelist validation, escape special characters

Exam Tip: XSS is NOW part of the A03 Injection category (2021 change)

A04: Insecure Design

Key Points:

- Design/architectural flaws, NOT implementation bugs
- Missing security controls in the design phase
- Examples: Password recovery without rate limiting, business logic flaws
- Difference: A01 = implementation failure (forgot check), A04 = never designed secure mechanism
- Prevention: Threat modelling (STRIDE, PASTA), secure design patterns, abuse cases

Exam Tip: Insecure Design = "doing security wrong" vs "doing security insecurely" (implementation bug)

A05: Security Misconfiguration

Key Points:

- Default passwords, unnecessary features enabled, verbose error messages
- Cloud: S3 buckets public, security groups allow 0.0.0.0/0
- Prevention: Hardening, minimal platform, automated config management, security headers (CSP, HSTS)

Indian Context:

- CERT-In incidents often involve exposed admin panels and default credentials on IoT devices

A06: Vulnerable & Outdated Components

Key Points:

- Using libraries/frameworks with known vulnerabilities
- Examples: Equifax (Apache Struts), Log4Shell (Log4j)

- Prevention: Maintain SBOM (Software Bill of Materials), monitor CVE databases, use Snyk/Dependabot, remove unused dependencies

A07: Identification & Authentication Failures

Key Points:

- Permits brute force, weak passwords, and weak credential recovery
- Missing MFA, session IDs in URLs, doesn't invalidate sessions after logout
- Prevention: Implement MFA, weak password checks, limit failed logins, secure session management (httpOnly/secure cookies)

A08: Software & Data Integrity Failures (NEW, includes XXE)

Key Points:

- Insecure deserialization, unsigned software updates, and CI/CD compromise
- Examples: SolarWinds supply chain attack, Codecov compromise
- Prevention: Digital signatures, verify library integrity, CI/CD pipeline security

Exam Tip: XXE is NO LONGER a separate category - now part of A08 (2021 change)

A09: Security Logging & Monitoring Failures

Key Points:

- Missing logs for logins/failures/transactions, no SIEM integration
- No alerting on suspicious activities
- Impact: Average breach detection = 207 days globally
- Prevention: Log all security events, send to SIEM, establish monitoring/alerting, and an incident response plan

Indian Context:

- CERT-In 6-hour reporting requires robust logging/monitoring

A10: Server-Side Request Forgery (SSRF)

Key Points:

- Web app fetches a remote resource without validating the user-supplied URL
- Attack: Access internal services, port scan, read local files, bypass firewalls
- Cloud impact: Access metadata APIs (169.254.169.254), steal credentials
- Prevention: Sanitise URLs, whitelist schema/ports, disable redirects, network segmentation

Buffer Overflow

Key Points:

- Input exceeds allocated buffer, overflows into adjacent memory
- Consequences: Arbitrary code execution, crashes, privilege escalation
- Prevention: Input validation, safe library functions, modern languages with memory management, compiler protections (ASLR, stack canaries)

Exam Tip: Buffer overflow = "water exceeding dam capacity, cascading destructively"

Race Conditions (TOCTOU)

Key Points:

- Time-of-Check-Time-of-Use: Timing gap between security check and resource use
- Attacker modifies the resource during the gap.
- Prevention: Atomic operations, synchronisation/locking, minimising time gaps, thread-safe programming

Indian Context:

- Payment gateways must prevent double-charging during OTP validation

Cross-Site Scripting (XSS)

XSS Type	Description
Persistent / Stored	Injected code is stored on the server and embedded in the HTML page sent to all subsequent users.
Reflected	Injected code is passed to a vulnerable server via a URL and reflected back to the victim.
DOM-based	Client-side Document Object Model (DOM) environment is modified, and malicious code is executed in the browser.

Key Points:

- Stored XSS: Malicious script stored on server (forum comments), executes for all visitors
- Reflected XSS: Script bounces off the server (malicious link), executes in the victim's browser.
- Prevention: Input validation, output encoding, Content Security Policy headers

Exam Tip: XSS = "fake ATM keypad over real one" - legitimate site, malicious addition

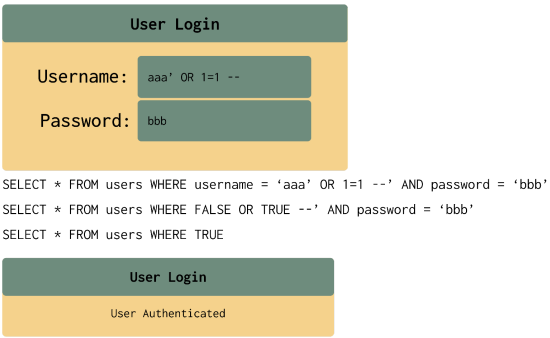
Cross-Site Request Forgery (CSRF)

Key Points:

- Tricks authenticated user into performing unintended actions
- User logs into the bank, visits a malicious site, and hidden forms submit to the bank with the user's cookies
- Prevention: CSRF tokens, SameSite cookies, verify referrer headers, re-authentication for sensitive ops

Exam Tip: XSS = pickpocket slipping malware, CSRF = photoshopping signature onto a cheque

SQL Injection



Key Points:

- Attacker inserts malicious SQL into application queries
- Example: admin'-- comments out password check
- Consistently top web app risk

Indian Context:

- Government websites experienced SQL injection attacks on citizen databases

Parameterised Queries (Gold Standard Defence)

Key Points:

- Completely separates SQL code from user data
- Database treats parameters as data only, never executable code
- Benefits: Complete protection, performance (cached query plans), type safety
- CRITICAL LIMITATIONS:
    - Table/column names CANNOT be parameterised - use WHITELIST validation
    - ORDER BY cannot use standard parameters - use WHITELIST
    - Dynamic WHERE with variable columns - use WHITELIST
    - IN clauses need dynamic placeholders
    - Stored procedures can STILL be vulnerable if using dynamic SQL internally

Example (Secure):
String query = "SELECT * FROM users WHERE username = ?";
PreparedStatement pstmt = connection.prepareStatement(query);
pstmt.setString(1, userInput);
Exam Tip: Parameterised queries protect DATA values, but table/column names require whitelist validation

ORM Frameworks

Key Points:

- Hibernate (Java), Entity Framework (NET), Django ORM (Python), Sequelize (Node.js)
- Automatic parameterisation by default
- Risks: False sense, dynamic query features can be vulnerable, raw SQL methods (.createNativeQuery())

Security Testing

Key Points:

- SAST (Static): Analyses source code without execution, finds hardcoded passwords, insecure patterns
- DAST (Dynamic): Tests running applications, simulates attacks, validates runtime security
- IAST (Interactive): Monitors from inside during testing, combines SAST + DAST
- Penetration Testing: Human testers simulate real attacks, find logical flaws

Exam Tip: SAST = early development (source code), DAST = testing phase (running app)

Secure Coding Practices

Key Points:

- Input Validation: Server-side, whitelist > blacklist, validate type/length/format/range.
- Output Encoding: Context-appropriate (HTML, URL, JavaScript), never insert user data directly.
- Authentication/Session: Strong hashed passwords, account lockouts, secure tokens, timeouts
- Error Handling: Don't expose system info, log for admins, generic messages for users, default deny
- Cryptography: Use established libraries, appropriate key lengths, protect keys, encrypt transit + rest

Software Assurance & Maturity Models

CMMI (Capability Maturity Model Integration)

Key Points:

- Level 1 (Initial): Unpredictable, reactive, individual heroics
- Level 2 (Managed): Basic planning/tracking, repeatable for similar projects
- Level 3 (Defined): Organisation-wide standards, tailored processes

- Level 4 (Quantitatively Managed): Statistical process control, measured quality
- Level 5 (Optimising): Continuous improvement, data-driven innovation

Indian Context:

- Large IT services companies achieve Level 3+ for client confidence and global contracts

BSIMM (Building Security In Maturity Model)

Key Points:

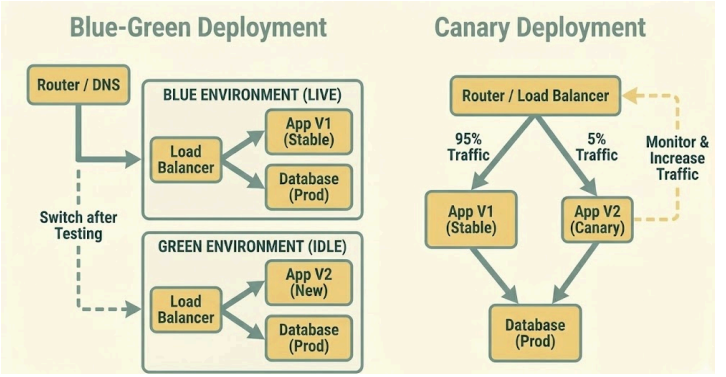
- Measures/improves software security by comparing to peers (descriptive, not prescriptive)
- Four Domains: Governance, Intelligence, SSDL Touchpoints, Deployment
- 119 activities across 12 practices
- Used for benchmarking against global peers

SAMM (Software Assurance Maturity Model)

Key Points:

- Prescriptive model - tells what to do at each maturity level
- Five Business Functions: Governance, Design, Implementation, Verification, Operations
- Each function has 3 security practices with 3 maturity levels
- Incremental improvement approach

Release & Deployment Management



Release Lifecycle Phases

Key Points:

- Plan: Scope, risk assessment, resource allocation, timeline, rollback planning
- Build: Secure coding, SAST/DAST integration, code review, dependency management
- Test: Unit, integration, security, penetration, UAT testing
- Deploy: Controlled rollout using deployment strategies
- Review: Evaluate success, lessons learned, and continuous improvement

Deployment Strategies

Key Points:

- Blue-Green: Two identical environments, switch traffic instantly, zero-downtime, instant rollback
- Canary: Gradual rollout to small subset (5% → 25% → 50% → 100%), early issue detection
- Rolling: Gradual replacement across servers, no extra infrastructure, service remains available

Indian Context:

- E-commerce uses blue-green for major sales events
- Banking canary deployments for UPI updates during festival seasons

Change Approval Process

Key Points:

- Change Advisory Board (CAB): Security, operations, business, and architecture representatives.
- Risk Levels: Standard (pre-approved), Normal (CAB review), Emergency (expedited), High-Risk (extended review)

Rollback Procedures

Key Points:

- Automated Triggers: Performance degradation, error rate spikes, security alerts, health check failures
- Validation: Database consistency, service dependencies, user impact, security posture

Indian Context:

- The railway booking system auto-rolls back within 2 minutes if booking failures exceed 1%
- Data localisation compliance for banking/payment data

Web Technologies & Security

CSS Security

Key Points:

- CSS Injection: Modify page appearance, redirect users, steal data via attribute selectors

- Clickjacking: Invisible elements over legitimate controls, z-index manipulation
- Prevention: CSP restricting CSS sources, sanitising user-provided CSS, and a whitelist for user-generated content

HTML Security

Key Points:

- XSS through HTML: Malicious tags execute JavaScript, improper encoding
- HTML Injection: Inject malicious HTML, modify content, leading to XSS/phishing
- Iframe Exploitation: Embed untrusted content, clickjacking, data theft
- Prevention: Output encoding (html special character), Content Security Policy headers

JavaScript Security

Key Points:

- DOM-Based XSS: Client-side JS processes untrusted data, executes in the browser
- Prototype Pollution: Manipulate object prototypes, which affects the entire application
- Prevention: Validate all inputs, sanitise DOM manipulation, use CSP, and avoid eval()

Indian Context:

- Banking websites experienced CSS injection for credential capture.

Key Takeaways for CISSP Exam

Critical Exam Points:

- Security integrated throughout SDLC, not an afterthought

- OWASP Top 10 2021: Know new categories (A04, A08, A10), XSS/XXE no longer standalone
- Parameterised queries = gold standard, but limitations for table/column names
- ACID properties for database integrity
- Database normalization: 1NF, 2NF, 3NF
- SAST (source code) vs DAST (running app) vs IAST (combined)
- OOP: Encapsulation, Inheritance, Polymorphism, Abstraction
- Coupling (LOW good) + Cohesion (HIGH good)
- CMMI maturity levels: Initial → Managed → Defined → Quantitatively Managed → Optimizing
- Deployment strategies: Blue-green (instant switch), Canary (gradual), Rolling (incremental)

Common Exam Traps:

- Confusing SAST/DAST timing and purpose
- Thinking XSS is still a separate OWASP Top 10 category (it's not - merged into Injection 2021)
- Assuming parameterised queries work for table/column names (they don't)
- Confusing A01 Broken Access Control (implementation) with A04 Insecure Design (architecture)

Indian Context for Real-World Application:

- RBI encryption mandates for payment data
- DPDPA personal data protection requirements
- CERT-In's 6-hour incident reporting needs robust logging
- Data localisation compliance for critical sectors
- Festival season scaling for e-commerce/banking
- Regional language support validation

Memory Aids:

- "Built in, not bolted on" = security at every SDLC phase
- "ACID = wedding vows" = unbreakable database transaction commitments
- "Coupling = family independence, Cohesion = family unity"

- "Compiler = prep before serving, Interpreter = cook as guests arrive"
- "Buffer overflow = water exceeding dam"
- "XSS = fake ATM keypad, CSRF = forged signature"

From CISSP to Leadership: The 60-Second Master Class

Close the Theory-Practice Gap

Concept	Reality Check
Least Privilege (theory)	Defense contractor: rigid + clearances. Startup: lightweight access. Both work.
Data Classification (theory)	Employees resist workflows. Legacy systems can't label. No DLP budget. Make it work anyway.

The 3 Wins:

1. Contextual Adaptation : Translate universal principles to org reality
2. Pragmatic Compromise : Good enough > perfect impossible
3. Incremental Progress : Quick wins build momentum (not big bang)

Compliance → Risk:

- Stop audit checkbox thinking
- Quantify risk in ₹: penalties + customer comp + brand damage + lost revenue
- Validate controls actually work (pentests > policies)
- Executives own risk acceptance (not security team)

India's Unique Context

Regulatory Maze

DPDP 2023 + RBI + CERT-In + SEBI + IRDAI + IT Act + data localization = map overlaps, implement once

Constraints → Solutions

Problem	Hack
Infra gaps (tier-1/2/3)	Enterprise controls in metros; simplified + 4G backup elsewhere
Talent scarcity	Train internally + automation + MSSPs + university pipeline
Cost pressure	Open-source + cloud Op-Ex model + risk-based prioritization

Cultural DNA

- Hierarchical: Get exec sponsorship FIRST
- Relationship-driven: Informal conversations matter more than formal processes
- Collectivist: Avoid public blame; frame as "system improvement"
- Loyalty-focused: Position controls as "employee protection," not surveillance

Influence > Authority

You have responsibility without direct control.

Learn this:

Tactic	Example

Stakeholder mapping	CFO = budget/financial risk. CMO = brand/CX.
Business translation	NOT: "Implement SIEM." YES: "Detect breaches in hours, not days."
Coalition building	Security champions in BUs + audit + exec governance
Negotiation	Collaborate, don't mandate. Rigid = dead on arrival.

Crisis Leadership

When systems burn:

- Calm = methodical thinking + clear comms despite chaos
- Decide fast = accept incomplete info (perfect data = never)
- Right message = Tech teams get detail. Execs get impact. Regulators get timelines.
- Learn hard = blameless post-mortems → systemic fixes → resilience

Next-Gen Programs

Reactive → Proactive

- Threat intel: Org-specific, not generic feeds
- Continuous validation: Red teams, breach sims, automated testing
- Adaptive controls: Risk-based auth, micro-seg triggered by anomalies

Zero Trust

Eliminate implicit trust. Verify everything.

- Phase 1: Stronger auth
- Phase 2: Micro-segment critical systems
- Phase 3: Enhanced monitoring
- Phase ∞: Full ZT (if budget/legacy allow)

Privacy by Design

- Minimize data collection
- Define & limit purpose
- Give users real control (access/correction/delete)

Automation Multiplier

What	Why
Auto-response	Malware isolation, account lockout → minutes, not hours
SOAR platforms	Multi-tool orchestration + consistent execution
ML/Behavioral analytics	Catch anomalies signature tools miss

Career Ladder

After CISSP:

- Certifications: CISM (mgmt), CCSP (cloud), CRISC (risk), PMP (projects)
- Conferences: c0c0n/nullcon (India) + RSA/Black Hat/DEF CON (global)
- Communities: ISACA, (ISC)², OWASP, Cloud Security Alliance
- Mentorship: Formal programs + informal + teaching

Leadership Mindset (The Differentiator)

Strategic thinking	Connect security to business
Business acumen	Speak finance, operations, competition
Emotional intelligence	Navigate politics, build teams
Resilience	Learn from failure, don't quit
Humility	Stay learnable, seek diverse views
Integrity	Principles > convenience

TL;DR: Certificate ≠ Leader

CISSP validates knowledge. Leadership = contextual wisdom + influence + cultural IQ + EQ + continuous learning.
You're not done. You're just starting.

Ravindra Gotavade

CISSP, CISM, SANS GIAC Defensible Security Architecture (GDSA) ISA/IEC 62443

The book is clearly meant for professionals into Cybersecurity planning to understand the Cissp 8 domains and clearing their exams with clear industry examples. The addition of diagrams, graphs and flowcharts are eye-catching and easy to remember. I would highly suggest this to anyone who is looking for a good book on CISSP.

Designed for professionals who want clarity over chaos, this CISSP guide focuses on core concepts, risk-based thinking, and exam-aligned decision making. It simplifies the domains into practical insights, strengthens your foundation, and helps you approach questions with confidence, maturity, and the mindset of a security leader.