MCA 106 - Cyber Security & Information System

Course Goals

1. Ensure **Confidentiality, Integrity, and Availability (CIA)** of systems.
2. Help organizations make **strategic decisions** with the aid of information systems.

COURSE OBJECTIVES

- Prevent/mitigate harm to networks, apps, devices, data.
- Support safe **cloud & mobile collaboration**.
- Enable **secure, scalable systems**.
- Provide **long-term planning & holistic view** of organizations.
- Help decision-making with **MIS**.

COURSE OUTCOMES

At the end, students should be able to:

- Protect **confidential data** & **intellectual property**.
- Test, detect & mitigate **security vulnerabilities**.
- Analyze **post-compromise** scenarios.
- Understand evolving **cybersecurity strategies**.
- Use **MIS for competitive advantage**.
- Evaluate **strategic alternatives**.

UNIT-WISE SYLLABUS

UNIT I – Introduction

- **Information Systems**: Definition, Types (TPS, MIS, DSS, ESS, etc.)
- **Development of IS**
- **Information Security**: Need & Importance
- **Threats to IS**
- **Information Assurance**
- **Cyber Security** Basics
- **Security Risk Analysis**

◇ UNIT II – Security Technologies & Threats

- **Application Security**: Database, E-mail, Internet
- **Data Security**: Backups, Archival Storage, Disposal
- **Security Technologies**: Firewall, VPNs, IDS (Intrusion Detection Systems), Access Control
- **Threats**:
  - Viruses, Worms, Trojan Horses, Logic Bombs, Trapdoors
  - Spoofing, E-mail & Macro Viruses
  - DoS/DDoS Attacks
- **E-Commerce Threats**:
  - e-Cash, Credit/Debit Cards, Digital Signatures, PKC (Public Key Cryptography)

◇ UNIT III – Secure Information Systems

- **Developing Secure IS**
- **Application Development Security**
- **Governance & Risk Management**
- **Security Architecture & Design**
- **Hardware/Data/Device Issues**
- **Physical Security**: CCTV, Access Control, IDS
- **Backup Security**

◇ UNIT IV – Policies & Cyber Laws

- **Security Policies**: Need, Types (WWW, Email), Review Process, Corporate Samples
- **Standards**: ISO, IT Act, Copyright Act, Patent Law, IPR
- **Cyber Laws in India**: IT Act 2000 Provisions
- **IPR Laws**: Copyright, Software License, Semiconductor Law, Patent Law

◇ UNIT V – Business Applications & Advanced IS

- **IT in Business**:
  - Internet, E-commerce, Intranet, Extranet, Enterprise Solutions
  - IS for Business Operations, Decision Support, Strategic Advantage
- **Planning & Control**:
  - Organizational Planning, Planning Process
  - Computational Support for Planning
  - Control Processes in Organizations
- **Managing IT**: Enterprise & Global Management, Security & Ethical Challenges, Implementing Change
- **Advanced IS Concepts**:
  - ERP (Enterprise Resource Planning)
  - SCM (Supply Chain Management)
  - CRM (Customer Relationship Management)
  - Procurement Management

Unit I — Introduction to Information Systems & Information Security

1. What is an Information System (IS)?

Definition: An Information System (IS) is a coordinated set of components that collect, process, store, and distribute information to support decision making and control in an organization.

Core components (6 P's):

- **People** — users, managers, IT staff
- **Processors (Hardware)** — servers, PCs, mobile devices
- **Programs (Software)** — applications, system software
- **Procedures** — workflows, policies, operating procedures
- **Data** — raw facts, databases, transaction logs
- **Networks (Communication)** — LAN, WAN, internet, cloud

Primary functions: Input → Process → Output → Feedback → Storage

---

2. Types of Information Systems (with examples)

- **TPS — Transaction Processing System**
  - Handles routine transactions (sales, payroll).
  - Example: POS billing system.
- **MIS — Management Information System**
  - Summarizes TPS output for middle management.
  - Example: Monthly sales summary reports.
- **DSS — Decision Support System**
  - Interactive tools for ad-hoc decision making (what-if analysis).
  - Example: Investment scenario simulator.
- **ESS / EIS — Executive Support / Information System**
  - High-level summaries for senior executives (dashboards, KPIs).
  - Example: CEO dashboard showing revenue vs target.
- **OAS — Office Automation System**
  - Supports daily office work (email, word processing).
  - Example: Email + document collaboration tools.
- **ERP — Enterprise Resource Planning**
  - Integrated modules across functions (finance, HR, inventory).
  - Example: SAP / Oracle ERP.
- **CRM — Customer Relationship Management**
  - Manages customer data & interactions.
- **SCM — Supply Chain Management**
  - Manages procurement, production, distribution.

---

3. Development of Information Systems

Common system development life-cycles / models:

- **SDLC (Waterfall)** — Phases: Requirement → Analysis → Design → Implementation → Testing → Deployment → Maintenance.
- **Prototype Model** — Build quick prototype, refine with user feedback.
- **RAD — Rapid Application Development** — Component-based, fast.
- **Agile** — Iterative sprints, continuous delivery, close user involvement.

Key activities in IS development:

1. Feasibility study / planning
2. Requirement gathering & analysis
3. System design (logical + physical)
4. Implementation / coding
5. Testing (unit, integration, system, UAT)
6. Deployment + training
7. Maintenance & evolution

4. Introduction to Information Security

Information Security: Protection of information and its supporting systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

The CIA Triad — fundamentals:

- **Confidentiality** — keep information secret (only authorized access).
- **Integrity** — correctness & completeness of information.
- **Availability** — information & systems available when needed.

Other security goals:

- **Authentication** — verify identity.
- **Authorization** — grant permissions.
- **Non-repudiation** — prevent denial of actions (e.g., digital signatures).
- **Privacy** — personal data protection.

5. Need for Information Security (why it matters)

- Protects **sensitive & confidential data** (customer, financial, IP).
- Ensures **business continuity** — prevents downtime and loss.
- Maintains **trust & reputation** with customers/partners.
- Meets **legal & regulatory** obligations (privacy, data protection).
- Prevents financial loss from fraud, theft, or ransomware.
- Enables **safe adoption of cloud & mobile services**.

6. Threats to Information Systems (classification & examples)

By origin:

- **External threats:** Hackers, cybercriminals, competitors.
- **Internal threats:** Disgruntled employees, careless users, insider abuse.

Common threats & attack types:

- **Malware:** Viruses, worms, Trojans, ransomware, spyware.
- **Social engineering:** Phishing, pretexting, baiting.
- **Network attacks:** Man-in-the-middle (MITM), sniffing, session hijacking.
- **Denial of Service (DoS/DDoS)** — exhausting resources to disrupt services.
- **Unauthorized access / privilege escalation.**
- **Physical theft / loss** — stolen laptop, removable media.
- **Software vulnerabilities / zero-days** — unpatched bugs exploited.
- **Insider threats** — data exfiltration, sabotage.
- **Advanced Persistent Threats (APT)** — targeted, stealthy long-term intrusions.

7. Information Assurance (IA)

Definition: Ensuring that information is **reliable, available, confidential, and trustworthy** through policies, processes, and controls.

Key IA pillars: Confidentiality, Integrity, Availability, Authentication, Non-repudiation, Privacy.

IA activities: risk assessment, security policy, incident response, audits, compliance, business continuity planning.

8. Cyber Security — overview & relation to IS security

Cybersecurity focuses on protecting networks, systems, applications, and data that are accessed or transferred via cyberspace. It overlaps heavily with information security but emphasizes technical controls for internet-connected assets.

Layers of defense (defence-in-depth):

- Perimeter (firewalls, VPN)
- Network (IDS/IPS, segmentation)
- Host (endpoint protection, hardening)
- Application (secure coding, WAF)
- Data (encryption, DLP)
- People (training, awareness)
- Policies & governance

9. Security Risk Analysis — basics & method

Key terms:

- **Asset:** Anything of value (data, hardware, people).
- **Threat:** Potential cause of an unwanted incident.
- **Vulnerability:** Weakness that can be exploited.
- **Control (Countermeasure):** Measure to reduce risk.
- **Risk:** Likelihood × impact of a threat exploiting a vulnerability.

Risk analysis steps:

1. **Identify assets & value** (business impact).
2. **Identify threats & vulnerabilities.**
3. **Assess likelihood** of occurrence.
4. **Assess impact** (financial, operational, reputational).
5. **Calculate risk** and prioritize.
6. **Decide treatment:** Accept, mitigate (implement controls), transfer (insurance), or avoid.
7. **Monitor & review.**

Qualitative vs Quantitative:

- **Qualitative:** Low/Medium/High, risk matrix, expert judgement.
- **Quantitative:** Numerical — SLE, ARO, ALE.

Sample quantitative formulas (explained step-by-step):

- **SLE (Single Loss Expectancy)** = Asset Value × Exposure Factor (EF)
- **ARO (Annualized Rate of Occurrence)** = Expected frequency per year
- **ALE (Annualized Loss Expectancy)** = SLE × ARO

Worked example (digit-by-digit as required):

- Asset Value = ₹100,000
- Exposure Factor = 30% = 0.30
  → SLE = 100,000 × 0.30 = 30,000.
- Suppose expected occurrence = once every 5 years → ARO = 1 / 5 = 0.2.
  → ALE = SLE × ARO = 30,000 × 0.2 = 6,000.
  So expected annual loss = ₹6,000.

Controls classification:

- **Preventive** — stop incidents (firewalls, access control).
- **Detective** — discover incidents (IDS, logs, monitoring).
- **Corrective** — restore after incident (backups, patching).
- **Deterrent** — discourage attackers (policies, signage).
- **Recovery** — BCP / DR plans.

10. Quick Checklist — What to remember for Unit I

- Components and functions of an IS (People, Hardware, Software, Data, Procedures, Networks).
- Types of IS and their purposes (TPS, MIS, DSS, ESS, ERP).
- SDLC phases and common development models (Waterfall, Prototype, Agile).
- CIA triad and other security goals (Authentication, Non-repudiation).
- Major threats (malware, phishing, DoS, insider, APT).
- Difference between Information Security and Cybersecurity (overlap and emphasis).
- Risk analysis basics and SLE / ARO / ALE formulas (with one worked example).
- Controls: preventive, detective, corrective.

11. Short practice questions (for quick revision / PYQ style)

1. Define an Information System and list its main components.
2. Differentiate between TPS, MIS and DSS with examples.
3. Explain the CIA triad with real-world examples.
4. Describe the steps in SDLC. Why is testing important?
5. Calculate the ALE if asset value is ₹50,000, EF is 40%, and expected occurrence is once every 10 years.
   - (Quick calc: SLE = 50,000 × 0.4 = 20,000. ARO = 0.1. ALE = 20,000 × 0.1 = 2,000.)

Unit II — Application & Data Security; Security Technologies; Threats

1. Application Security (Database, E-mail, Internet)

Database Security

Goals: Confidentiality, integrity, availability of stored data; prevent unauthorized access and data leakage.

Controls & best practices

- **Authentication & authorization:** Strong DB accounts, roles, least privilege, use of RBAC.
- **Encryption:**
    - *At rest* (TDE — Transparent Data Encryption; disk-level encryption).
    - *In transit* (TLS for DB connections).
- **Input validation & parameterised queries:** Prevent SQL Injection (use prepared statements / stored procedures).
- **Auditing & logging:** Record DDL/DML changes, privileged actions, login attempts.
- **Backups & secure storage:** Encrypted backups, offsite copies, tested restores.
- **Patching & hardening:** Minimise DB services, remove default accounts, patch DB engine.
- **Separation of duties:** Admin vs developer privileges.
- **Row/column-level security** for sensitive fields (PII/financial).
- **Masking & tokenization** for production-like nonproduction datasets.

Example attacks: SQL injection, privilege escalation, data exfiltration via misconfigured backups.

E-mail Security

Threats: Phishing, spoofing, malware attachments, business email compromise (BEC).

Controls & standards

- **Transport security:** TLS (STARTTLS) for SMTP delivery.
- **Authentication & anti-spoofing:** SPF, DKIM, DMARC (prevent spoofing & improve deliverability).
- **End-to-end message security:** S/MIME, PGP for encryption/signing.
- **Gateway protections:** Anti-spam, anti-malware scanning, URL rewriting/sandboxing attachments.
- **User controls:** Attachments blocking (exe), safe-link previews, mailbox quotas.
- **Awareness & training:** Phishing simulations, reporting mechanisms.
- **Email archiving & retention** policies, encrypted archives.

Internet / Web Application Security

Threats: XSS, CSRF, SQLi, broken authentication, insecure direct object references, insecure configurations.

Secure development practices

- **OWASP top-10 awareness** and mitigation.
- **Input validation & output encoding.**
- **Session management:** secure cookies, SameSite, short lifetimes, token revocation.
- **Use HTTPS everywhere:** HSTS, secure TLS configurations (avoid obsolete ciphers).
- **WAF (Web Application Firewall):** block known attack patterns.
- **Secure deployment:** container hardening, secrets management, least privilege.
- **Static & Dynamic testing:** SAST, DAST, penetration testing.
- **Dependency management:** scan for vulnerable libraries, apply patches.

2. Data Security Considerations — Backups, Archival Storage & Disposal

Backups

- **Types:** Full, Incremental, Differential.
    - *Full* — complete copy.
    - *Incremental* — only changes since last backup.
    - *Differential* — changes since last full backup.
- **Backup strategy:** 3-2-1 rule — 3 copies, on 2 media types, 1 offsite.
- **Frequency & RPO/RTO:** Define Recovery Point Objective (max data loss) and Recovery Time Objective (downtime tolerance).
- **Encryption & access controls** on backup media.
- **Testing:** Regular restore drills to validate backups.
- **Immutable backups / WORM** to defend against ransomware.

Archival Storage

- **Purpose:** Long-term retention, compliance, historical records.
- **Characteristics:** Lower cost, slower access, integrity verification (checksums).
- **Media & formats:** Tape, cold cloud storage, encrypted archives; retention policies.

Secure Disposal

- **Logical erasure:** Overwriting with secure wipes (multiple passes not always necessary if using modern standards and full-disk encryption).
- **Cryptographic erasure:** Destroy encryption keys to render data unreadable.
- **Physical destruction:** Shredding, degaussing (for magnetic media), incineration for high-sensitivity.
- **Sanitization policies** based on sensitivity & regulation (e.g., PCI/PII rules).

3. Security Technologies — Firewall, VPNs, Intrusion Detection, Access Control

Firewalls

Types

- **Packet-filtering (stateless):** Filters by IP/port; fast but limited context.
- **Stateful inspection:** Tracks connections; better security.
- **Proxy/Application-layer (Layer 7):** Understands application protocols (HTTP/FTP).
- **Next-Gen Firewall (NGFW):** App awareness, user identity, integrated IPS/antivirus.
- **Cloud / Host-based firewalls** for virtualised environments.

Placement & rules

- Perimeter vs internal segmentation (microsegmentation).
- Deny-by-default; explicit allow rules; log dropped packets.

VPNs

Purpose: Secure remote access & encrypted site-to-site tunnels.

Types

- **IPsec VPN:** Site-to-site, transport/tunnel modes; strong for network-level tunnels.
- **SSL/TLS VPN:** Client or browser-based remote access (granular app access).
- **MPLS / SD-WAN:** For enterprise WANs with integrated security.

Considerations

- Strong authentication (MFA), key management, split-tunneling policies, rekeying/crypto-suite selection.

Intrusion Detection & Prevention

- **IDS vs IPS**
  - **IDS:** Monitors & alerts (detective).
  - **IPS:** Actively blocks traffic (preventive).
- **Types**
  - **Network IDS (NIDS):** Monitors network traffic (e.g., Snort, Suricata).
  - **Host IDS (HIDS):** Monitors file integrity, logs on host (e.g., OSSEC).
- **Detection methods**
  - **Signature-based:** Known patterns (fast, low false positives for known attacks).
  - **Anomaly-based / behavioral:** Learns normal baseline and flags deviations (good for unknown attacks but higher false positives).
- **SIEM integration:** Collect logs/events, correlation, alerting, forensic support.

Access Control

Models

- **DAC (Discretionary Access Control):** Owners set permissions.
- **MAC (Mandatory Access Control):** System-enforced policies (labels, e.g., military classification).
- **RBAC (Role-Based Access Control):** Access by role; scalable for enterprises.
- **ABAC (Attribute-Based Access Control):** Policies use attributes (user, resource, environment).

Principles & mechanisms

- **Least privilege, separation of duties, need-to-know.**
- **Authentication:** Passwords, tokens, certificates, biometric, MFA (TOTP, push).
- **Authorization:** OAuth, OAuth2, scopes, claims.
- **Directory & federation:** LDAP, Active Directory, SAML, OpenID Connect, Single Sign-On (SSO).
- **Account lifecycle management:** Provisioning, deprovisioning, periodic reviews, privileged access management (PAM).

4. Malware & Other Security Threats

Malware types

- **Virus:** Attaches to host files; needs user action to propagate.
- **Worm:** Self-replicates across networks without host action.
- **Trojan Horse:** Appears benign but contains payload (backdoor).
- **Logic Bomb / Time Bomb:** Triggered by condition/time.
- **Rootkit:** Hides processes & files, provides persistent covert access.
- **Ransomware:** Encrypts data & demands payment; backup immunity required.
- **Spyware/Adware:** Data exfiltration or intrusive ads.
- **Macro viruses:** Use office macros (e.g., malicious Word/Excel macros).

Mitigations

- Endpoint protection (antivirus/EPP/EDR), application whitelisting, patching, least privilege, attachment sandboxing, user training.

Network Attacks & DoS/DDoS

- **Sniffing / MITM:** Intercepting traffic (mitigate with TLS, VPN).
- **SYN flood, UDP flood:** Exhaust resources (mitigate via rate limiting, scrubbing).
- **Amplification attacks:** DNS/NTP reflection (mitigate with ingress filtering, disabling recursion).
- **Segmentation, rate limits, CDN/anti-DDoS services** for resilience.

5. Security Threats to E-Commerce & Electronic Payment Systems

Threats

- **Card fraud:** Skimming, stolen card data, Card-Not-Present (CNP) fraud.
- **Phishing & social engineering** to capture credentials.
- **Payment gateway compromise** or API misuse.
- **Man-in-the-middle** during payment flows (if insecure).
- **Chargebacks & friendly fraud.**

Protections & standards

- **PCI DSS:** Cardholder data protection standard (encryption, access controls, logging).
- **Tokenization:** Replace card numbers with tokens to reduce exposure.
- **3-D Secure (3DS):** Additional authentication for cardholders (friction but reduces fraud).
- **TLS/HTTPS** enforced for payment pages.
- **Secure payment gateways & PCI-compliant processors.**
- **Fraud detection:** Velocity checks, ML-based scoring, device fingerprinting.
- **Secure coding:** Avoid storing PAN, mask data, use secure redirects or hosted payment pages.

6. Digital Signatures & Public Key Cryptography (PKC)

Asymmetric cryptography basics

- **Key pair:** Public key (shareable) + Private key (secret).
- **Common algorithms:** RSA, ECC (Elliptic Curve Cryptography).
- **Use cases:** Confidentiality (encrypt with recipient’s public key), Authentication & non-repudiation (sign with sender’s private key).

Digital Signature process (conceptual)

1. **Hash the message** using a cryptographic hash (SHA-256).
2. **Encrypt the hash** with sender’s private key → this is the digital signature.
3. **Receiver** decrypts signature with sender’s public key and compares hash to locally computed hash to verify integrity & authenticity.

Properties: Integrity, authenticity, non-repudiation.

Public Key Infrastructure (PKI)

- **Components:** CA (Certificate Authority), RA (Registration Authority), Certificates (X.509), CRL/OCSP (revocation checks).
- **Certificate chain:** End-entity → intermediate CA → root CA (trusted).
- **Usage:** SSL/TLS certificates, code signing, email signing (S/MIME), client auth.

Practical notes

- Key management and secure storage of private keys (HSMs) is critical.
- Certificate expiry & revocation handling (OCSP stapling).
- Use appropriate key lengths and algorithms (e.g., RSA 2048+, ECC 256+).

7. Summary — Key Takeaways (Unit II)

- Application security covers secure coding, DB hardening, web app best practices, and email safeguards.
- Backups must be planned (RPO/RTO), encrypted, and tested; archival & secure disposal are essential for compliance.
- Firewalls, VPNs, IDS/IPS, and strong access control models form layered defenses.
- Malware types and DoS attacks require endpoint controls, network protections, logging and response plans.
- E-commerce security demands PCI compliance, TLS, tokenization, and fraud detection.
- Digital signatures + PKI provide integrity, authentication, and non-repudiation—key for secure transactions.

8. Quick Revision Checklist

- Prevent SQL injection → use prepared statements.
- Email anti-spoofing → SPF, DKIM, DMARC.
- Backups → Full/Incremental/Differential; 3-2-1 rule.
- Firewalls → stateful vs application layer.
- VPN → IPsec vs SSL/TLS.
- IDS → signature vs anomaly; IDS vs IPS.
- Access control → DAC/MAC/RBAC/ABAC; least privilege.
- Malware → differences among virus, worm, trojan, ransomware.
- E-commerce → PCI DSS, tokenization, TLS, 3DS.
- PKC → public/private keys, digital signature steps, CA role.

9. Practice / Short Questions (PYQ style)

1. Explain SQL injection attack and list three prevention techniques.
2. Differentiate between firewall, IDS and IPS.
3. Describe Full, Incremental and Differential backups with advantages.
4. What are SPF, DKIM and DMARC? How do they protect e-mail?
5. Explain how digital signatures provide non-repudiation.
6. What is tokenization and how does it reduce PCI scope?
7. Describe the difference between symmetric and asymmetric cryptography.
8. Explain the role of PKI in SSL/TLS certificate validation.

Unit III — Developing Secure Information Systems, Governance, Architecture & Physical Security

1. Developing Secure Information Systems (Secure SDLC / S-SDLC)

Goal: Build security in, not bolt it on.

Phases with security activities

1. **Requirements & Planning**
   - Security requirements, compliance, data classification, threat surface.
2. **Design**
   - Threat modeling (STRIDE / PASTA), secure architecture, trust boundaries, dataflow diagrams (DFD).
3. **Implementation**
   - Secure coding standards, input validation, use of prepared statements, least privilege.
4. **Verification / Testing**
   - SAST (static code analysis), DAST (dynamic testing), IAST, manual code review, penetration testing.
5. **Deployment**
   - Hardened configurations, secrets management, secure CI/CD pipelines, container hardening.
6. **Maintenance / Operations**
   - Patching, monitoring, incident response, vulnerability management, dependency scanning.

Threat modelling (basic)

- STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege.
- Identify assets → enumerate threats → rate severity → propose mitigations.

Secure coding practices (checklist)

- Input validation & output encoding.
- Use parameterized queries / ORM.
- Proper session management, CSRF tokens.
- Avoid storing secrets in code; use vaults/HSM.
- Handle errors securely (no sensitive info in logs).
- Validate third-party libraries & pin versions.
- Enforce TLS, HSTS, secure cookies.

CI/CD security

- Signed artifacts, vulnerability scanning, least privilege service accounts, immutable deploys, rollback plan, pipeline secrets stored in vaults.

---

2. Application Development Security (Detailed Controls)

Authentication & Authorization

- Strong password policies, account lockout, MFA (TOTP / push).
- Use established protocols: OAuth2 / OIDC / SAML for SSO.
- Role-based or attribute-based access checks at server-side.

Data protection

- Encrypt sensitive data at rest (TDE, file system encryption) and in transit (TLS 1.2+/TLS 1.3).
- Tokenization & masking for sensitive fields (PII, PAN).
- Logging: redact sensitive data before logging.

Dependency & supply-chain security

- SBOM (software bill of materials), dependency scanning (OSS vuln scanners), signed packages, repository hardening.

Runtime protections

- WAF, RASP, rate-limiting, circuit breakers, API gateways with authentication & throttling.

3. Information Security Governance & Risk Management

Governance components

- **Frameworks:** ISO/IEC 27001, NIST CSF, COBIT — provide structure for policy, controls and continuous improvement.
- **Roles:** Board → defines risk appetite; CISO → oversees security program; DPO/Compliance → privacy & compliance; IT/SecOps → implement controls.
- **Policies:** Info security policy, acceptable use, data classification, incident response, BYOD, access control, backup & retention.

Risk Management process

1. Asset identification & valuation.
2. Threat & vulnerability identification.
3. Risk assessment (qualitative/quantitative).
4. Risk treatment: mitigate / accept / transfer / avoid.
5. Monitoring & review.

Business Impact Analysis (BIA)

- Identify critical processes, RTO, RPO, dependencies & single points of failure.

Business Continuity & Disaster Recovery

- BCP: maintain operations.
- DR plan: recovery of IT systems (site failover, replication, runbooks).
- Regular DR drills & tabletop exercises.

Incident Response (IR) lifecycle

- **Prepare → Detect & Analyze → Contain → Eradicate → Recover → Post-Incident (lessons learned)**.
- Metrics: MTTD (mean time to detect), MTTR (mean time to recover), number of incidents, time to containment.

Compliance & Audits

- Regular internal/external audits, gap analysis, continuous monitoring, evidence collection for regulators.

4. Security Architecture & Design

Core design principles

- **Least privilege**, **defense-in-depth**, **fail-safe defaults**, **separation of duties**, **secure by design**, **minimise attack surface**, **economy of mechanism**.

Architectural controls

- **Network segmentation** (VLANs, subnetting, microsegmentation).
- **DMZ** for public-facing services; internal segmentation for sensitive systems.
- **Zero Trust** principles: never trust, always verify (strong auth, continuous validation).
- **Encryption**: data-in-transit & data-at-rest; proper key lifecycle management.
- **Secure defaults & baselines** (OS, middleware, database).
- **Design patterns**: API gateway, broker, adapter with secure authentication and throttling.

Hardware & platform security

- Secure boot, measured boot, firmware signing, TPM, secure enclave/TEE for key protection.
- Supply-chain assurance: provenance, firmware validation, vendor security posture.

5. Security Issues in Hardware, Data Storage & Downloadable Devices

Hardware threats

- Tampering, malicious firmware, side-channel attacks, counterfeit components.
- Mitigations: secure supply chain, hardware attestation (TPM), firmware update signing, hardware inventory & asset tagging.

Data storage concerns

- Misconfigured cloud storage (S3 buckets), insecure file shares, unencrypted removable backups.
- Mitigations: strong access control, encryption, lifecycle policies, storage access logs.

Downloadable devices (USB, external drives, mobile)

- Malware propagation via USB, data leakage, lost/stolen devices.
- Controls: disable/limit USB ports, endpoint DLP, anti-malware, device encryption, MDM enrollment, removable media policy.

Bring Your Own Device (BYOD)

- MDM, containerization of corporate data, conditional access, policy enforcement (jailbroken/rooted device restrictions).

6. Physical Security of IT Assets, Access Control, CCTV & Intrusion Detection Systems

Physical security controls

- **Perimeter controls:** fencing, manned gates, visitor management.
- **Building controls:** locks, badge access, turnstiles, security guards.
- **Environmentals:** fire detection & suppression, HVAC, UPS, generator, flood protection.
- **Secure racks & cages** in data centers.

Access control (physical ↔ logical integration)

- Badge & biometrics for logical access tie-in (logical accounts mapped to physical identities).
- Separation of privileged areas (server rooms), dual control for sensitive actions, visitor escorting.

CCTV (design & best practice)

- Camera types: fixed, PTZ, dome, thermal.
- Placement: entrances/exits, server rooms, loading bays, power rooms (avoid private areas).
- Retention: define retention period per policy, secure storage, tamper detection.
- Privacy & legal: signage, access logs, restricted viewing, compliance with local laws.

Intrusion Detection Systems (physical)

- Motion sensors, door/window contacts, glass-break detectors, alarm monitoring, integration with access logs and CCTV.

7. Backup Security Measures (detailed)

Backup strategy & security

- **3-2-1 rule**: at least 3 copies, 2 different media, 1 offsite.
- **Encryption**: backups encrypted at rest and in transit; manage backup encryption keys securely (do not store keys with backups).
- **Immutable backups / snapshots**: WORM or cloud immutability to resist ransomware.
- **Access control**: dedicated backup accounts, least privilege, multi-person approval for restores of critical backups.
- **Segregation & network isolation**: backup systems should be isolated from production to avoid lateral spread of malware.
- **Regular restore testing**: scheduled restore drills and validation checks; test RTO/RPO.
- **Retention & retention policies**: align with regulatory requirements; lifecycle & archival processes.
- **Integrity checks & checksums**: verify backup integrity periodically.
- **Offsite / Air-gapped backups**: periodic air-gapped copies reduce online compromise risk.
- **Logging & monitoring**: alert on unusual backup activity (large deletions, failed backups, retention changes).

8. Practical Checklists & Templates (quick)

S-SDLC quick checklist

- Security requirements documented and approved.
- Threat model & DFD created.
- Dependency & license review done; SBOM created.
- SAST/DAST scans passed; pen test scheduled.
- Secrets stored in vault; no creds in repo.
- Hardened images & baseline configs.
- CI/CD pipeline signed builds & vulnerability gates.
- Production monitoring & alerting configured.

Hardware procurement checklist

- Vendor security posture & SLA.
- Support for secure boot / firmware signing.
- Patch/update policy & timeline.
- Tamper-evidence & asset tagging.
- Lifecycle & EOL policy documented.

Backup restore playbook (short)

- Identify restore owner & approve.
- Verify backup integrity & select correct snapshot.
- Restore to isolated environment → validate data → promote.
- Document restore time, success criteria, lessons learned.

9. Short Practice / PYQ-style Questions

1. Describe the Secure SDLC and list security tasks for each phase.
2. What is threat modelling? Explain STRIDE with examples.
3. Explain the role of TPM in hardware security.
4. List and explain five controls to secure backups against ransomware.
5. Describe the incident response lifecycle and key responsibilities of the CISO.
6. How does network segmentation improve security posture? Give an example.
7. What are the security risks with BYOD and how would you mitigate them?

10. Quick Revision Points

- Build security in: S-SDLC, threat modelling, SAST/DAST & pen testing.
- Governance: policies, BIA, DR, IR, roles (CISO).
- Architecture: least privilege, defense-in-depth, zero-trust & segmentation.
- Hardware: secure boot, TPM, supply-chain checks.
- Physical security: badge, CCTV, environmental controls.
- Backups: encryption, immutability, air-gap, regular restore testing.

Unit IV — Security Policies, Standards & Cyber Laws (exam-ready notes)

1. Security Policies — purpose & components

Purpose: A security policy defines management direction, assigns responsibilities, and sets acceptable behaviour for protecting information assets. It is the foundation of governance and compliance.

Core components of any security policy

- **Purpose & scope** (who/what is covered)
- **Policy statement(s)** (high-level rules & objectives)
- **Roles & responsibilities** (board, CISO, IT, users)
- **Standards & procedures** (how to implement)
- **Reporting & compliance** (audits, sanctions)
- **Definitions & glossary**
- **Review & version control** (date, owner, next review)

2. Types of policies (short descriptions + when to use)

- **Information Security Policy (umbrella policy)** — high-level objectives & governance.
- **Acceptable Use Policy (AUP)** — permitted uses of IT resources.
- **Password / Authentication Policy** — password complexity, expiry, MFA requirements.
- **Access Control Policy** — provisioning, review cycles, privileged access controls (PAM).
- **Data Classification & Handling Policy** — public / internal / confidential / restricted handling rules.
- **Backup & Retention Policy** — backup frequency, RPO/RTO, retention periods.
- **Incident Response Policy** — roles, escalation matrix, communication plan.
- **Email Security Policy** — allowed attachments, encryption, phishing reporting.
- **WWW / Internet Usage Policy** — permitted sites, streaming, downloads, monitoring disclaimers.
- **Remote Access / BYOD Policy** — MDM, containerization, conditional access rules.
- **Third-Party / Vendor Security Policy** — contractual security requirements, audits.
- **Physical & Environmental Security Policy** — server room access, CCTV rules.

3. Sample short policy clauses (copy-paste ready)

A. Email Security (sample clause)
“All corporate email must use the corporate mail gateway. Confidential attachments MUST be encrypted when sent outside @company domain. Users must not open suspicious attachments or links and must report suspected phishing to security@company. Use of personal email for business data is prohibited.”

B. WWW / Internet Usage (sample clause)
“Internet access is provided for business use. Excessive personal use, downloading executables, or visiting malicious/piracy sites is prohibited. The organisation monitors traffic for security and compliance; users consent to logging.”

C. Data Classification (sample clause)
“Classify all data as Public / Internal / Confidential / Restricted. Confidential/Restricted data must be stored on authorised systems, encrypted at rest and in transit, and access granted on need-to-know with periodic access reviews.”

D. Policy on Publishing & Notification
“Any external publication of technical security material (vulnerabilities, architecture diagrams) requires approval from CISO and Legal. Security incidents affecting customer data must be reported to the Incident Response Team within 4 hours and, if required by regulation, to affected parties and regulators as specified in the incident playbook.”

---

4. Policy Review Process — practical steps

1. **Owner assignment:** Each policy has an owner (CISO or department head).
2. **Scheduled review:** Annual review minimum (or earlier for major changes).
3. **Trigger reviews:** After incidents, legal changes, audits, or technology shifts.
4. **Stakeholder consultation:** IT, Legal, HR, Business units consulted for impact.
5. **Approval:** Formal approval by Senior Management/Board (or delegated committee).
6. **Communication & training:** Publish policy, run awareness sessions, require acknowledgement.
7. **Enforcement & metrics:** Track compliance metrics, exceptions register, and disciplinary actions.
8. **Versioning & archive:** Maintain version history and publication dates.

5. Publishing & Notification Requirements (best practice)

- **Where to publish:** Internal intranet (policy hub), email announcement, and optional printed quick-cards for sensitive rules.
- **Notification:** All staff notified on new or updated policies; critical updates require mandatory read/acknowledgement.
- **External disclosure:** Do not publish sensitive IT/security architecture or vulnerability details externally without Legal/CISO approval.
- **Breach notification:** Follow legal/regulatory timelines (see local laws/regulators). Maintain templates for customer/regulator notifications to speed response.

6. Information Security Standards & Frameworks (short summary)

- **ISO/IEC 27001** — internationally recognized standard for an Information Security Management System (ISMS); provides requirements to establish, implement, operate, monitor, review, maintain and continually improve an ISMS.
- **NIST CSF / COBIT** — commonly used frameworks for risk management, governance and operational controls (useful for mapping controls to ISO/27001). (Framework reference — not cited here.)

7. Cyber Laws & IPR — concise summary (India focus)

Information Technology Act, 2000 (IT Act) — provides legal framework for electronic records, digital signatures and cyber offences (e.g., unauthorized access, damage to computers, and intermediary liability). Important sections define civil liability for unauthorized access/damage and criminal penalties for hacking and related offences; intermediary safe-harbour rules are covered under Section 79 (subject to due diligence/notice-and-take-down). See the official act text for details. India CodeLex Partem

Copyright Act, 1957 — protects original literary, dramatic, musical and artistic works, including software (source and/or object code are protected as literary works); registration is optional but evidentiary. Copyright OfficeMizoram Dictionary

Patents Act, 1970 — protects inventions that are novel, involve inventive step (non-obvious) and are industrially applicable; patents give exclusive rights (generally up to 20 years) subject to statutory exceptions and procedure before the Patent Office. IP IndiaTaxTMI

Semiconductor Integrated Circuits Layout-Design Act, 2000 — protects layout designs of integrated circuits (ICs) and provides registration rights and remedies for infringement; protection terms and conditions are defined in the Act. iPleadersStratjuris Law Partners

Note: Laws are detailed and occasionally updated — for legal advice or precise compliance timelines always consult the latest official sources or legal counsel. (References above link to authoritative sources.)

8. Putting standards & law into policy (practical mapping)

- Map **ISO 27001** Annex controls → internal policy clauses (e.g., A.9 Access Control → Access Control Policy). ISO
- Include **legal requirements** in policy: data breach notification timelines, retention rules, and privacy controls — align Incident Response & Data Retention policies with applicable statutes (IT Act, sectoral rules). India Code
- For software/IP: ensure **Copyright & Patent** obligations are reflected in Acceptable Use, Software Licensing, and Procurement policies. Copyright OfficeIP India

9. Quick policy templates & checklists (one-line items)

Policy rollout checklist

- Owner assigned ✓
- Business impact and scope defined ✓
- Legal & regulatory requirements checked ✓
- Approval from management obtained ✓
- Communicated + training scheduled ✓
- Acknowledgement tracking enabled ✓
- Review date set ✓

Breach notification checklist (incident owner)

- Triage & classification ✓
- Containment steps executed ✓
- Legal & PR notified ✓
- Regulators / affected users notified per law ✓
- Evidence preserved & logs collected ✓
- Post-incident review & policy update ✓

---

10. Short practice / PYQ-style questions

1. What are the essential components of an Information Security Policy?
2. Explain the policy review process and why periodic reviews are needed.
3. List five sample clauses you would include in an Email Security Policy.
4. How does ISO/IEC 27001 help an organisation? Give two concrete examples.
5. State the role of Section 79 of the IT Act with respect to intermediaries.

Unit V — Business Applications of IT; Planning & Control; Managing IT; Advanced IS Concepts

1. Business Applications of Information Technology

Internet & Electronic Commerce

- **E-commerce types:** B2B, B2C, C2C, C2G, G2C.
- **Core components:** Web storefront, payment gateway, order management, inventory, logistics, CRM, analytics.
- **Benefits:** Wider market reach, 24×7 availability, lower transaction costs, personalised marketing.
- **Risks/Threats:** Fraud, data breaches, insecure payment flows, privacy issues — mitigations: HTTPS/TLS, PCI DSS, tokenization, secure APIs.

Intranet, Extranet & Enterprise Solutions

- **Intranet:** Internal network for collaboration, document management, HR portals, internal knowledge bases.
- **Extranet:** Controlled access to partners/suppliers/customers (project sharing, B2B portals).
- **Enterprise Solutions:** Integrated software suites (ERP, PLM, CRM) enabling cross-functional processes and single source of truth.

Information Systems for Business Operations

- **Operational systems:** Transaction Processing Systems (TPS), inventory control, manufacturing execution systems (MES), POS.
- **Goals:** Automate routine tasks, ensure accuracy, reduce cycle time, support large transaction volumes.

Information Systems for Managerial Decision Support

- **Management Information Systems (MIS):** Periodic reports, trending, operational summaries for middle management.
- **Decision Support Systems (DSS):** What-if, simulation, optimisation, scenario analysis for semi-structured decisions.
- **Business Intelligence (BI):** Data warehouses, ETL, dashboards, OLAP, visual analytics for insight and KPI tracking.

Information Systems for Strategic Advantage

- **Strategic IS use:** Create differentiation (unique customer experience), cost leadership (automation), and new business models (platforms).
- **Examples:** Amazon’s recommendation engine; Uber’s matching and surge pricing algorithms.
- **Sustaining advantage:** Continuous innovation, data-driven learning, network effects, strong IS governance.

---

2. Concepts of Planning & Control

Concept of Organizational Planning

- **Definition:** Systematic process of deciding goals, resources, and actions for future.
- **Levels:** Strategic (long-term), Tactical (medium-term), Operational (short-term).

The Planning Process (typical steps)

1. **Set objectives** (SMART goals).
2. **Environmental scan** (SWOT, PESTEL).
3. **Identify alternatives** and resources.
4. **Evaluate alternatives** (cost, risk, benefit).
5. **Choose plan & allocate resources.**
6. **Implement & monitor.**
7. **Review & adjust.**

Computational Support for Planning

- **Tools:** Forecasting models, linear programming, simulation, ERP planning modules (MRP/APS), BI and predictive analytics.
- **Benefits:** Handling large datasets, scenario analysis, improved forecasting accuracy, optimisation of resources.

Characteristics of the Control Process

- **Elements:** Set standard → Measure performance → Compare → Take corrective action.
- **Characteristics:** Continuous, feedback-driven, objective measurement, timely information, corrective mechanisms.
- **Types of control:** Feedforward (preventive), concurrent (real-time), feedback (after the fact).

The Nature of Control in an Organization

- **Formal vs Informal controls:** Policies, procedures vs culture.
- **Financial, clinical/operational, quality, and compliance controls.**
- **IT controls:** Access controls, change management, configuration control, audit trails.

---

3. Managing Information Technology

Enterprise & Global Management

- **Enterprise IT governance:** Align IT with business strategy (COBIT, ISO/IEC 38500).
- **Structures:** Centralized, decentralized, federated IT models — choose based on scale, standardization need, autonomy.
- **Global considerations:** Cross-border data flow, localization laws, multi-currency, multilingual support, time-zone operations.

Security & Ethical Challenges

- **Security challenges:** Protecting data, identity, continuity, supply chain vulnerabilities, cloud security.
- **Ethical challenges:** Privacy, algorithmic bias, surveillance, employee monitoring, responsible AI use.
- **Mitigations:** Privacy-by-design, ethical guidelines, impact assessments, transparency, strong legal/compliance teams.

Planning & Implementing Changes (IT change management)

- **Change lifecycle:** Initiation → Business case → Design & approval → Pilot → Rollout → Review.
- **Key practices:** Stakeholder engagement, communication plan, training, phased deployment, rollback plans, post-implementation review.
- **Measurement:** Adoption metrics, defect rates, business KPIs, ROI analysis.

4. Advanced Concepts in Information Systems

Enterprise Resource Planning (ERP)

- **Definition:** Integrated suite to manage core business processes (finance, HR, manufacturing, supply chain).
- **Major modules:** Finance (GL/AP/AR), Materials Management, Production Planning, Sales & Distribution, HR.
- **Benefits:** Single data model, process standardization, improved reporting, reduced redundancies.
- **Challenges:** High cost, long implementation, change resistance, data migration, customization vs standardization trade-offs.
- **Implementation steps:** Requirement analysis → Vendor selection → Blueprint/design → Data migration → Configure & customize → Testing → Training → Go-live → Stabilization.

Supply Chain Management (SCM)

- **Definition:** Management of flows of goods, information, finances from suppliers to customers.
- **Components:** Procurement, inventory management, warehousing, transportation, order fulfillment.
- **IS Role:** SCM systems, TMS (transportation), WMS (warehouse), demand forecasting, supplier portals, EDI/API integrations.
- **KPIs:** Fill rate, order cycle time, inventory turnover, on-time delivery.

Customer Relationship Management (CRM)

- **Definition:** Systems & processes to manage customer interactions across marketing, sales, and service.
- **Functions:** Lead management, opportunity tracking, case management, campaign management, customer analytics.
- **Types:** Operational CRM (process automation), Analytical CRM (analytics, segmentation), Collaborative CRM (channel integration).
- **Benefits:** Better customer retention, targeted marketing, sales productivity, improved customer service.

Procurement Management (in IS context)

- **Procurement cycle:** Requisition → Sourcing → Purchase order → Receipt → Invoice → Payment.
- **E-procurement systems:** Automate RFQs, supplier catalogs, e-auctions, contract management.
- **Controls:** Vendor evaluation, approvals, segregation of duties, contract compliance, audit trails.
- **Integration:** ERP integration for inventory & finance, supplier portals for collaboration.

5. Managing Change: Implementation & Post-Implementation Issues

- **Critical success factors (CSFs):** Executive sponsorship, clear objectives, user involvement, competent project team, effective communication.
- **Common failures:** Poor change management, inadequate testing, bad data migration, scope creep, insufficient training.
- **Post-implementation:** Hypercare/support, performance tuning, continuous improvements, governance for enhancements.

---

6. Emerging Trends (brief)

- **Cloud-native ERP & SaaS CRM** — shift to subscription models.
- **AI & ML in BI** — predictive insights, automation of decisions.
- **Low-code / no-code for rapid app development.**
- **Blockchain** for provenance in supply chain and secure contracts.
- **IoT integration** in operations and SCM for real-time telemetry.

---

7. Quick Revision Checklist — Unit V

- Know differences: internet vs intranet vs extranet.
- IS roles: operational (TPS), managerial (MIS/DSS), strategic (EIS/BI).
- Planning steps & computational tools (forecasting, LP, simulation).
- Control process: set standard → measure → compare → correct.
- ERP: modules, benefits, implementation lifecycle.
- SCM: components, IS tools, KPIs.
- CRM: operational vs analytical vs collaborative.
- Procurement cycle & e-procurement controls.
- Change management essentials and CSFs.

---

8. Short Practice / PYQ-style Questions

1. Distinguish between an intranet and an extranet with examples.
2. Explain the role of MIS and DSS in managerial decision-making.
3. List and explain the major modules of an ERP system.
4. What is the 3 steps in the planning-control cycle? Give a business example.
5. Describe how CRM helps in customer retention.
6. Explain key risks in e-commerce and measures to secure online payment transactions.
7. Outline the procurement cycle and list 4 controls to prevent fraud.

15 high-value, exam-oriented questions for **MCA 106**

1. **Explain the CIA triad (Confidentiality, Integrity, Availability).** *(5 marks)*
   — Hint: define each, give real-world examples and a short control for each.

2. **Describe the phases of the SDLC and compare Waterfall with Agile.** *(8–10 marks)*
   — Hint: list phases, pros/cons, when to use each + impact on security.

3. **Perform a quantitative risk calculation for a ransomware event using SLE, ARO and ALE (worked example).** *(6 marks)*
   — Hint: show digit-by-digit SLE = AV×EF, ARO, ALE = SLE×ARO and interpret results.

4. **What is SQL Injection? Explain three prevention techniques.** *(5 marks)*
   — Hint: prepared statements, input validation, least privilege DB user.

5. **Explain Public Key Infrastructure (PKI) and the process of creating & verifying a digital signature.** *(8 marks)*
   — Hint: keys, hashing, sign with private key, verify with public key, role of CA/CRL/OCSP.

6. **Compare IDS and IPS — types, working methods (signature vs anomaly), and deployment considerations.** *(6 marks)*
   — Hint: detection vs prevention, false positives, inline vs passive modes.

7. **List and explain types of firewalls (packet filter, stateful, application proxy, NGFW) and where you'd place them in an enterprise network.** *(5 marks)*
   — Hint: placement (perimeter, DMZ, internal segmentation) + rule principle (deny by default).

8. **Explain backup strategies: Full / Incremental / Differential; state the 3-2-1 rule and how immutable backups mitigate ransomware.** *(6 marks)*
— Hint: RPO/RTO definitions, restore testing importance.

9. **Describe Secure SDLC (S-SDLC) and demonstrate threat modelling using STRIDE on a simple web application dataflow.** *(8–10 marks)*
— Hint: map threats to design, propose mitigations.

10. **Outline an Incident Response (IR) plan for a mid-sized company: lifecycle stages, team roles and three key KPIs.** *(8 marks)*
— Hint: Prepare → Detect → Contain → Eradicate → Recover → Lessons; roles: CISO, IR lead, forensics, comms; KPIs: MTTD, MTTR, incidents closed.

11. **Explain the major provisions of the IT Act, 2000 relevant to cyber security and intermediary liability (brief).** *(5 marks)*
— Hint: offences (hacking, data damage), Section 79 safe-harbour basics, importance of due diligence.

12. **Draft the headings/contents of a Data Classification & Handling Policy (one-page template).** *(5 marks)*
— Hint: scope, classes (Public/Internal/Confidential/Restricted), handling rules, labeling, retention, exceptions.

13. **Describe security threats to e-commerce payments and list controls: PCI-DSS, tokenization, 3-D Secure, TLS, fraud detection.** *(8 marks)*
— Hint: card data flow, where PCI applies, merchant vs processor responsibilities.

14. **Explain Zero-Trust architecture principles and three practical steps to implement Zero Trust in an enterprise.** *(6 marks)*
— Hint: never trust, verify every request; microsegmentation, MFA, least privilege, continuous monitoring.

15. **Discuss ERP implementation lifecycle, major challenges and three controls to secure ERP systems.** *(8 marks)* — Hint: blueprint → config → data migration → testing → go-live; challenges: customization vs standardization, data quality, change mgmt; controls: segregation of duties, privileged access management, audit trails.