CISSP

Introduction: To enhance our organization's cybersecurity capabilities, we're rolling out a structured CISSP certification prep program for key personnel. The CISSP is a globally recognized standard for information security leadership, and this initiative aligns with our strategic goal of building in-house security expertise.
Our approach is streamlined and outcome-focused. We'll begin with a clear overview of the exam and its eight domains. The study guide we're using is fully aligned with the latest CISSP exam objectives and includes real-world scenarios to contextualize learning. To reinforce retention and track progress, we're integrating an interactive online platform that offers practice tests, flashcards, and analytics. Each topic is directly mapped to exam objectives, ensuring a focused and measurable learning journey.

This structured path not only prepares our team for certification but also strengthens our overall security posture through deeper domain knowledge and improved decision-making at all levels.

Flow of Contents

Capabilities
Secure Design Principles
Techniques for Ensuring CIA
Understand the Fundamental Concepts of Security Models
Select Controls Based on Systems Security Requirements
Understand Security Capabilities of Information Systems
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures
Shared Responsibility
Data Localization and Data Sovereignty
Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
Client-Based Systems
Server-Based Systems
Industrial Control Systems
Distributed Systems
High-Performance Computing (HPC) Systems
Real-Time Operating Systems
Internet of Things
Edge and Fog Computing
Embedded Devices and Cyber-Physical Systems
Microservices
Infrastructure as Code
Immutable Architecture
Virtualized Systems
Containerization
Mobile Devices
Essential Security Protection Mechanisms
Common Security Architecture Flaws and Issues
Chapter 10: Physical Security Requirements
Apply Security Principles to Site and Facility Design
Implement Site and Facility Security Controls
Implement and Manage Physical Security
Chapter 11: Secure Network Architecture and Components
OSI Model
TCP/IP Model
Analyzing Network Traffic
Common Application Layer Protocols
Transport Layer Protocols
Domain Name System
Internet Protocol (IP) Networking
ARP Concerns
Secure Communication Protocols
Implications of Multilayer Protocols
Segmentation
Edge Networks
Wireless Networks
Satellite Communications
Cellular Networks
Content Distribution Networks (CDNs)
Secure Network Components

Chapter 12: Secure Communications and Network Attacks
Protocol Security Mechanisms
Secure Voice Communications
Remote Access Security Management
Multimedia Collaboration
Monitoring and Management
Load Balancing
Manage Email Security
Virtual Private Network
Switching and Virtual LANs
Network Address Translation
Third-Party Connectivity
Switching Technologies
WAN Technologies
Fiber-Optic Links
Prevent or Mitigate Network Attacks
Chapter 13: Managing Identity and Authentication
Controlling Access to Assets
The AAA Model
Implementing Identity Management
Managing the Identity and Access Provisioning Life Cycle
Chapter 14: Controlling and Monitoring Access
Comparing Access Control Models
Implementing Authentication Systems
Zero-Trust Access Policy Enforcement
Understanding Access Control Attacks
Chapter 15: Security Assessment and Testing
Building a Security Assessment and Testing Program
Performing Vulnerability Assessments
Testing Your Software
Training and Exercises
Implementing Security Management Processes and
Collecting Security Process Data
Chapter 16: Managing Security Operations
Apply Foundational Security Operations Concepts
Address Personnel Safety and Security
Provision Information and Assets Securely
Apply Resource Protection
Managed Services in the Cloud
Perform Configuration Management (CM)
Manage Change
Manage Patches and Reduce Vulnerabilities
Chapter 17: Preventing and Responding to Incidents
Conducting Incident Management
Implementing Detection and Preventive Measures
Logging and Monitoring
Automating Incident Response
Chapter 18: Disaster Recovery Planning
The Nature of Disaster
Understand System Resilience, High Availability, and Fault
Tolerance

Recovery Strategy
Recovery Plan Development
Training, Awareness, and Documentation
Testing and Maintenance

Chapter 19: Investigations and Ethics

Investigations
Major Categories of Computer Crime
Ethics

Chapter 20: Software Development Security

Introducing Systems Development Controls
Establishing Databases and Data Warehousing
Storage Threats
Understanding Knowledge-Based Systems

Chapter 21: Malicious Code and Application Attacks

Malware
Malware Prevention
Application Attacks
Injection Vulnerabilities
Exploiting Authorization Vulnerabilities
Exploiting Web Application Vulnerabilities
Application Security Controls
Secure Coding Practices

DOMAIN-1

CHAPTER 1

1. Understand and Apply Security Concepts

- **CIA Triad**: Ensuring **Confidentiality**, **Integrity**, and **Availability** in all systems.
- **Security Controls**: Understand administrative, technical, and physical controls and their categories (preventive, detective, corrective, deterrent, recovery, compensating).
- **Defense in Depth**: Layering multiple controls across IT systems.
- **Authentication, Authorization, and Accountability (AAA)**
- **Principle of Least Privilege**, **Need to Know**
- **Data Classification and Handling**
- **Security Models**: Bell-LaPadula (confidentiality), Biba (integrity), Clark-Wilson, Brewer-Nash (conflict of interest)

🧱 2. Security Boundaries

- **Isolation and Segmentation** of systems/networks based on trust levels.
- **Trusted vs. Untrusted Zones** (e.g., internet, DMZ, intranet)
- **Network Boundaries**: Firewalls, gateways, routers
- **Logical and Physical Segregation** of environments (e.g., development vs. production)
- **Air Gaps and Sandboxing** as advanced boundary techniques

---

🏛️ 3. Evaluate and Apply Security Governance Principles

- **Security Governance vs. Management**: Governance sets direction, management executes.
- **Security Frameworks**: ISO/IEC 27001, COBIT, NIST CSF
- **Due Care** (implementing best practices) vs. **Due Diligence** (ongoing oversight)
- **Security Roles**:
    - Data Owner
    - Data Custodian
    - System Owner

    - End User
- **Separation of Duties**, **Rotation of Duties**, **Least Privilege**
- **Regulatory and Legal Compliance**: GDPR, HIPAA, SOX, etc.
- **Strategic Alignment of Security with Business Objectives**

🛡 4. Manage the Security Function

- **Security Program Management**: Building and maintaining an enterprise security program
- **CISO Responsibilities**: Governance, risk, compliance, incident management
- **Security Metrics & KPIs**
- **Security Budgeting and Resource Allocation**
- **Internal & External Audits**
- **Awareness and Training Programs** for culture building

📜 5. Security Policy, Standards, Procedures, and Guidelines

- **Hierarchy**: Policies (what) → Standards (how much) → Procedures (how) → Guidelines (recommendations)
- **Policy Lifecycle**: Develop → Communicate → Enforce → Review
- **Acceptable Use Policy (AUP)**, BYOD Policies
- **Policy Enforcement and Disciplinary Measures**
- **Stakeholder Involvement and Approval**

⚠️ 6. Threat Modeling

- **Identify Threat Agents**: Internal, external, partners, competitors, nation-states
- **Common Methodologies**:
    - **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
    - **DREAD** (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)
    - **PASTA**, **OCTAVE**
- **Attack Surface Analysis**
- **Use of DFDs (Data Flow Diagrams)** to visualize threat paths
- **Prioritize Risks for Mitigation**

🔗 7. Supply Chain Risk Management (SCRM)

- **Third-Party Risk Management**: Due diligence before onboarding vendors
- **Security Clauses in Contracts**
- **Vendor Assessments and SLAs**
- **Supply Chain Threats**: Counterfeit components, firmware tampering, software backdoors
- **Trusted Delivery and Secure Sourcing**
- **Chain of Custody and Component Tracking**
- **Risk Transfer via Cyber Insurance**
- **Monitoring and Auditing** of vendors and suppliers

CHAPTER 2

👥 Personnel Security Policies and Procedures

- **Hiring Practices**: Background checks, screening, employment agreements
- **Onboarding**:
  - Security training
  - Role-based access provisioning
- **Roles and Responsibilities**: Defined clearly in job descriptions
- **Termination Procedures**:
  - Exit interviews
  - Revocation of access rights
  - Return of assets
- **Employee Lifecycle Management**:
  - Transfers, promotions, and job rotations
  - Least privilege and need-to-know principle enforcement
- **Policy Enforcement**:
  - Acceptable Use Policy (AUP)
  - Code of Conduct
  - Disciplinary processes

📉 Understand and Apply Risk Management Concepts

- **Risk Components**:
  - Assets, Threats, Vulnerabilities, Impact, Likelihood
- **Risk Assessment**:
  - Qualitative (using risk matrix, expert judgment)
  - Quantitative (calculating SLE, ARO, ALE)
- **Risk Response Strategies**:
  - Mitigate (reduce)
  - Transfer (insurance, outsourcing)
  - Avoid (remove asset or threat)
  - Accept (when cost > impact)

- **Risk Register**: Central documentation of risks, owners, actions
- **Ongoing Risk Monitoring and Review**
- **Business Impact Analysis (BIA)** and alignment with risk posture

---

🎭 Social Engineering

- **Definition**: Psychological manipulation to trick individuals into compromising security
- **Common Techniques**:
    - Phishing (emails, SMS)
    - Pretexting (posing as someone trusted)
    - Baiting (malicious USBs or software)
    - Tailgating / Piggybacking
    - Dumpster Diving
- **Targeted Attacks**: Spear phishing, whaling (executive targeting)
    - Awareness programs
    - Technical controls (email filtering, MFA)
    - Clear reporting channels for suspected attacks

📚 Establish and Maintain a Security Awareness, Education, and Training Program

- **Awareness**:
    - Broad-based campaigns (e.g., posters, emails)
    - Goal: Change user behavior and mindset
- **Training**:
    - Role-specific (e.g., developers on secure coding, HR on PII)
    - Delivered through LMS, workshops, tabletop exercises
- **Education**:
    - Formal programs (certifications, degrees)
    - Supports long-term career development
- **Program Lifecycle**:
    - Needs assessment → Design → Delivery → Evaluation
- **Metrics and KPIs**:

    - Completion rates, phishing simulation results, behavioral improvements
- **Regulatory Compliance**:
    - Align with standards like ISO/IEC 27001, NIST SP 800-50

CHAPTER 3

1. Project Scope and Planning

- **Define Objectives**: Ensure resilience of critical business operations.
- **Establish the BCP Team**: Cross-functional representation (IT, HR, Legal, Operations).
- **Management Support**: Secure executive sponsorship and funding.
- **Define Scope**:
    - Boundaries (locations, departments, processes)
    - Dependencies (third parties, cloud providers)
- **Resource Allocation**: Tools, training, and time commitment

---

2. Business Impact Analysis (BIA)

- **Identify Critical Business Functions**
- **Determine Impact of Disruption**:
    - Financial, legal, reputational, operational
- **Calculate Key Metrics**:
    - **RTO (Recovery Time Objective)**
    - **RPO (Recovery Point Objective)**
- **Dependencies and Interdependencies**
- **Prioritize Recovery Efforts**: Based on risk, impact, and time sensitivity

---

3. Continuity Planning

- **Develop Recovery Strategies**:
    - Alternate sites: hot, warm, cold
    - Redundant systems, failover designs
- **Data Backup Solutions**
- **Communication Plans**:
    - Internal and external stakeholders
    - Crisis communication templates

- **Incident Response Integration**
- **Manual Workarounds for Critical Processes**

---

4. Plan Approval and Implementation

- **Executive Review and Sign-Off**
- **Formal Documentation**:
    - Roles and responsibilities
    - Step-by-step procedures
- **Integration with Enterprise Policies**
- **Communication of Plan** to staff and stakeholders

---

5. Ongoing Maintenance and Testing

- **Regular Testing**:
    - Tabletop exercises
    - Full-scale simulations
- **Training and Awareness**
- **Review and Updates**:
    - After changes in business, technology, or regulations
- **Continuous Improvement Loop**

CHAPTER 4

1. Categories of Laws

CISSP emphasizes understanding global legal systems and their implications for information security:

- **Criminal Law** – Addresses offenses harmful to society (e.g., cybercrime, hacking).
- **Civil Law** – Deals with disputes between individuals or organizations (e.g., privacy violations, intellectual property).
- **Administrative Law** – Enforced by regulatory agencies (e.g., compliance with HIPAA, GDPR).
- **Common Law** – Based on judicial precedent.
- **Customary Law / Religious Law** – May influence international operations and data handling.

🔹 2. Core Laws Related to InfoSec

Professionals must know relevant laws in their jurisdiction and industry:

- **Computer Fraud and Abuse Act (CFAA)** – U.S. law criminalizing unauthorized access.
- **Electronic Communications Privacy Act (ECPA)**
- **HIPAA, SOX, GLBA** – Sector-specific U.S. regulations.
- **EU GDPR** – Global benchmark for privacy compliance.
- **Intellectual Property Laws** – Copyrights, patents, trademarks, and trade secrets.
- **Cybersecurity Laws in India, China, etc.** – Vary widely by country and affect global data flow.

🔹 3. State Privacy Laws

CISSP stresses understanding that **compliance isn't only federal**:

- **CCPA (California Consumer Privacy Act)** – U.S. gold standard for state-level privacy rights.
- **Virginia CDPA, Colorado CPA, others** – Each with unique data rights and breach notification rules.
- Important for multi-jurisdictional organizations to track evolving **state-level legislation**.

🔹 4. Compliance

Security must align with **legal, regulatory, and contractual obligations**:

- **Security Frameworks and Standards**:
  - ISO/IEC 27001
  - NIST 800-53 / 800-171
  - PCI DSS (for payment systems)
- **Compliance Program Elements**:
  - Gap assessments
  - Audit readiness
  - Policy alignment
- **Penalties for Non-Compliance**:
  - Legal fines
  - Business restrictions
  - Reputational damage

🔹 5. Contracting and Procurement

Key for **supply chain security and third-party risk management**:

- **Security Clauses in Contracts**:
  - Data ownership, confidentiality, breach notification
  - Service Level Agreements (SLAs)
- **Right to Audit**, compliance reporting
- **Due Diligence and Vendor Risk Assessments**
- **Procurement Compliance**:
  - Avoiding conflicts of interest
  - Ensuring legal and ethical sourcing
  - Tracking licenses and warranties

DOMAIN-2

CHAPTER 5

1. Identifying and Classifying Information and Assets

- **Asset Identification**:
  - Includes data, hardware, software, people, systems, and facilities.
- **Data Classification**:
  - Based on **sensitivity, value, criticality**.
  - Common levels: Public, Internal, Confidential, Restricted.
- **Owner Responsibilities**:
  - Assigning classification.
  - Ensuring protection and correct use.
- **Asset Inventory**:
  - Maintained, accurate, and regularly updated.
  - Linked to asset management policies and risk assessments.

---

2. Establishing Information and Asset Handling Requirements

- **Access Control Requirements**:
  - Based on classification (e.g., only certain roles can view confidential data).
- **Labeling, Storage, Transmission, and Disposal**:
  - E.g., Encrypted transmission for sensitive data.
  - Secure shredding or wiping of classified data before disposal.
- **Policy Alignment**:
  - Handling requirements must align with **regulatory** and **business policies** (e.g., GDPR, HIPAA).

---

3. Data Protection Methods

- **Encryption** (at rest, in transit, end-to-end)
- **Masking and Tokenization** – for PII and sensitive fields
- **Data Loss Prevention (DLP)** – to detect/prevent unauthorized disclosure

- **Access Control Models**:
    - DAC, MAC, RBAC
- **Media Sanitization** – Clearing, purging, destruction techniques (as per NIST SP 800-88)

🔹 4. Understanding Data Roles

- **Data Owner**:
    - Responsible for data classification and defining protection requirements.
- **Data Custodian**:
    - Implements and maintains protections.
- **Data User**:
    - Follows policies and handles data responsibly.
- **Data Controller & Processor** (GDPR context):
    - Controller defines purposes and means; Processor acts on behalf of controller.

🔹 5. Using Security Baselines

- **Definition**: Minimum required security settings/configurations for systems and assets.
- **Baseline Development**:
    - Based on industry standards (e.g., CIS Benchmarks, NIST, ISO).
- **Application Areas**:
    - OS configurations, network devices, cloud environments
- **Continuous Improvement**:
    - Regular updates based on threats, patches, and organizational change.
- **Baseline Drift Management**:
- Ensure systems don’t deviate from approved configurations over time.

DOMAIN-3

CHAPTER 6

1. Cryptographic Foundations

- **Core Principles**:
  - **Confidentiality**, **Integrity**, **Authentication**, **Non-repudiation**
- **Historical Background**:
  - Classical ciphers (Caesar, Vigenère) to understand evolution
- **Mathematical Basis**:
  - Prime numbers, modulo arithmetic, hashing, entropy
- **Types of Attacks**:
  - Brute force, cryptanalysis, frequency analysis

🔹 2. Modern Cryptography

CISSP Focus:

- **Encryption Categories**:
  - **Symmetric**: Same key (e.g., AES, DES)
  - **Asymmetric**: Public/private key pairs (e.g., RSA, ECC)
- **Key Applications**:
  - Secure communications, digital signatures, email encryption (PGP), VPNs
- **Hashing Functions**:
  - SHA-2, SHA-3, HMAC for integrity checking
- **Key Exchange Protocols**:
  - Diffie-Hellman, ECDH for secure key sharing
- **Zero-Knowledge Proofs, Homomorphic Encryption** (advanced topics)

🔹 3. Symmetric Cryptography

CISSP Focus:

- **Use Cases**:
  - Fast, bulk data encryption (e.g., file systems, VPN tunnels)

- **Block Ciphers**:
    - AES, 3DES – encrypt fixed-size blocks (ECB, CBC, GCM modes)
- **Stream Ciphers**:
    - RC4 – encrypt bit-by-bit or byte-by-byte
- **Modes of Operation**:
    - Important for controlling IV reuse, error propagation, and integrity
- **Key Management**:
    - Secure generation, storage, distribution, rotation, and destruction

---

🔹 4. Cryptographic Life Cycle

CISSP Focus:

- **Phases**:
    1. **Planning** – Selecting appropriate algorithms and key sizes.
    2. **Implementation** – Securely integrating into applications/systems.
    3. **Operation** – Managing key use and ensuring performance/compliance.
    4. **Monitoring** – Detecting misuse, logging activity, periodic review.
    5. **Decommissioning** – Secure key destruction and algorithm retirement.
- **Compliance**:
    - FIPS 140-3, NIST SP 800-57 (Key Management), 800-131A (Algorithm transition)
- **Algorithm Agility**:
    - Ability to switch algorithms quickly as threats evolve

CHAPTER 7

1. Asymmetric Cryptography

Focus: Uses a **public/private key pair** for encryption and decryption.

- Common algorithms: **RSA**, **ECC (Elliptic Curve)**, **ElGamal**
- Supports **confidentiality**, **authenticity**, **non-repudiation**
- Typically used for:
    - Key exchange (e.g., SSL/TLS)
    - Digital signatures
    - Email encryption (e.g., PGP/GPG)

🔹 2. Hash Functions

Focus: Generate a **fixed-length digest** from variable input.

- Ensures **integrity** of data.
- Algorithms: **SHA-2**, **SHA-3**, **MD5 (deprecated)**, **HMAC**
- Hashes are:
    - Deterministic
    - One-way
    - Collision-resistant (good ones are)
- ---

🔹 3. Digital Signatures

Focus: Prove **origin, authenticity, and integrity** of a message.

- Combines hashing + asymmetric encryption
- Sender signs the hash with their **private key**
- Recipient verifies with sender's **public key**
- Common in:
    - Email security
    - Code signing
    - Document validation

🔹 4. Public Key Infrastructure (PKI)

Focus: Framework for managing digital certificates and public keys.

- Components:
    - **Certificate Authority (CA)** – issues certificates
    - **Registration Authority (RA)** – verifies identities
    - **Certificate Revocation List (CRL)** or **OCSP**
- Supports **SSL/TLS**, secure email, smart cards, digital identities

---

🔹 5. Asymmetric Key Management

Focus: Managing lifecycle of public-private key pairs.

- Includes:
    - Key generation
    - Secure distribution (e.g., via certificates)
    - Storage (e.g., HSMs)
    - Rotation and expiration
    - Revocation (CRL, OCSP)
- Keys must be protected to prevent impersonation or compromise

---

🔹 6. Hybrid Cryptography

Focus: Combines strengths of symmetric and asymmetric methods.

- Example: **SSL/TLS handshake**
    - Asymmetric encryption is used to **exchange a symmetric key**
    - Then, symmetric encryption secures the session
- Efficient and secure approach used in real-world systems

🔹 7. Applied Cryptography

Focus: Use of cryptography in **real-world applications**.

- Secure communications: **VPNs, HTTPS**
- File protection: **BitLocker, VeraCrypt**
- Messaging: **Signal, WhatsApp**
- Identity: **Biometric encryption, Smart Cards**
- Compliance: Ensures data protection laws are met

🔹 8. Cryptographic Attacks

Focus: Threats that target weaknesses in cryptographic systems.

- **Brute-force** – trying all possible keys
- **Man-in-the-Middle (MITM)** – intercepting key exchange
- **Replay Attacks** – resending captured messages
- **Chosen Ciphertext/Plaintext** – inputting known values to study output
- **Side-channel Attacks** – exploiting hardware leakage (timing, power usage)
- **Quantum Threats** (future): Can break RSA/ECC — post-quantum cryptography is emerging

CHAPTER 8

1. Secure Design Principles

Goal: Build security into systems **from the ground up** using foundational principles.

Key principles include:

- **Least Privilege** – users/processes have only the access needed
- **Defense in Depth** – layered controls across systems
- **Fail-Safe Defaults** – deny by default, allow by exception
- **Separation of Duties** – avoid conflicts of interest
- **Economy of Mechanism** – keep designs simple and manageable
- **Complete Mediation** – every access request is checked
- **Open Design** – security through transparency, not obscurity

---

🔹 2. Techniques for Ensuring CIA *(Confidentiality, Integrity, Availability)*

- **Confidentiality**:
  - Access control, encryption, data classification
- **Integrity**:
  - Hashing, checksums, digital signatures, change management
- **Availability**:
  - Redundancy (RAID, failover), backups, anti-DDoS, capacity planning

CISSP focus: **Balance CIA based on system risk profile** and business needs.

🔹 3. Understand the Fundamental Concepts of Security Models

Security models define how systems enforce security:

- **Bell-LaPadula** – focus on **confidentiality** (no read up, no write down)
- **Biba** – focus on **integrity** (no write up, no read down)
- **Clark-Wilson** – ensures **integrity through well-formed transactions**
- **Brewer-Nash** (Cohesion model) – dynamic access control, prevents conflicts of interest
- **Take-Grant** – analyzes how access rights can be transferred
- **Lattice Models** – represent security labels in MAC environments

These guide **access control, policy enforcement, and system design**.

🔹 4. Select Controls Based on System Security Requirements

CISSP approach:

- Perform **risk assessments** to determine control needs
- Match controls to:
  - **System sensitivity**
  - **Regulatory/compliance requirements**
  - **Business mission**
- Types of controls:
  - **Preventive**: Firewalls, access control
  - **Detective**: IDS, logs, audits
  - **Corrective**: Patching, backups, incident response
  - **Technical, Administrative, Physical** categories

🔹 5. Understand Security Capabilities of Information Systems

Systems may include built-in security capabilities such as:

- **Access Control Enforcement** (DAC, MAC, RBAC)
- **Trusted Computing Base (TCB)** – the core components enforcing security
- **Security Labels and Classifications**
- **Hardware Security** – TPMs, HSMs, secure boot
- **Virtualization Security** – isolation, hypervisor integrity
- **Cloud Security Features** – native encryption, identity federation

CHAPTER 9

Shared Responsibility

In **cloud and hybrid environments**, security is a **shared model**:

- **Provider**: Secures infrastructure (hardware, network, hypervisor)
- **Customer**: Secures data, applications, access, identity
- Key to **risk allocation and SLA design**

🔹 **Data Localization & Sovereignty**

- **Data Localization**: Legal requirement to **store/process data in a specific region**
- **Data Sovereignty**: Data subject to the laws of the country where it resides
- Impacts **cloud adoption**, **compliance** (e.g., GDPR, HIPAA)

🔹 **Assess & Mitigate Architectural Vulnerabilities**

Evaluate design elements to avoid:

- Misconfigured controls
- Insecure default settings
- Lack of segmentation
- Weak cryptographic implementations

Use **threat modeling**, **penetration testing**, **architecture reviews**.

🖥️ **System-Specific Architecture & Security**

🔸 **Client-Based Systems**

- Risks: Malware, insecure apps, local storage
- Protections: Hardening, endpoint protection, patching

🔸 **Server-Based Systems**

- Risks: Unauthorized access, configuration drift
- Controls: Access control, logging, secure boot, patch management

🔸 **Industrial Control Systems (ICS)**

- Includes SCADA, PLCs; sensitive to downtime
- Focus: Isolation, network segmentation, OT-specific protocols

🔸 **Distributed Systems**

- Risk: Data inconsistency, insecure inter-process comms
- Secured via: API management, encryption, trust models

🔸 **High-Performance Computing (HPC) Systems**

- Sensitive to availability; targeted for compute abuse
- Protect through: Access control, segmentation, usage policies

🔸 **Real-Time Operating Systems (RTOS)**

- Critical for **timing precision** (e.g., avionics, medical)
- Require: Minimal overhead, certified secure builds

📡 **Emerging & Embedded Architectures**

🔸 **Internet of Things (IoT)**

- Risks: Weak credentials, unpatchable firmware
- Secure with: Network isolation, device lifecycle control

🔸 **Edge & Fog Computing**

- Computation near data source
- Concerns: Local compromise, data integrity, latency attacks

🔸 **Embedded & Cyber-Physical Systems**

- Combine software with physical components
- Common in healthcare, automotive—need strict **access control**, **safety checks**

⚙️ **Modern Software and Infrastructure Paradigms**

🔸 **Microservices**

- Modular, independently deployable services
- Secure via: API gateways, identity federation, input validation

🔸 **Infrastructure as Code (IaC)**

- Automates deployments; misconfig = systemic risk
- Controls: Versioning, secure templates, code scanning

🔸 **Immutable Architecture**

- Systems are **replaced**, not modified
- Benefits: Predictability, consistency, fast rollback

📦 Virtualization, Containers, and Mobility

🔸 Virtualized Systems

- Hypervisor risks, VM escape, snapshot leaks
- Defend with: Isolation, secure VM templates, strong access control

🔸 Containerization

- Lightweight, fast, but risk shared kernel
- Security: Image scanning, runtime protection, namespaces, cgroups

🔸 Mobile Devices

- Challenges: BYOD, varied OS, physical loss
- Controls: MDM, remote wipe, VPN, app sandboxing

🛡️ Fundamental Protection Mechanisms

Essential mechanisms that span all architectures:

- **Authentication & Authorization**
- **Encryption**
- **Audit & Monitoring**
- **Security Baselines & Config Hardening**
- **Patch Management**
- **Redundancy & Failover**

⚠️ Common Architecture Flaws

Be aware of:

- Implicit trust zones
- Overexposed APIs
- Flat networks
- Default passwords
- Missing logs or alerts

CHAPTER 10

Apply Security Principles to Site and Facility Design

Goal: **Embed security into facility architecture** to **protect assets**.

Key principles:

- **Physical Security Zones**: Separate critical areas (e.g., server rooms, data centers) from non-sensitive areas.
- **Layered Defense**: Use multiple physical barriers (e.g., fences, gates, security doors, biometric access) to prevent unauthorized access.
- **Redundancy & Resilience**: Ensure power, cooling, and network access have failovers and backups.
- **Natural Surveillance**: Position building entrances and windows to allow staff to monitor access points.

🔹 Implement Site and Facility Security Controls

Controls to mitigate physical threats:

- **Access Control Systems**:
  - Card access, biometrics, PIN codes
  - Multi-factor authentication for sensitive areas
- **Physical Barriers**:
  - Fencing, bollards, guard posts, security doors
  - Use of mantraps for high-security zones
- **Environmental Controls**:
  - Fire suppression systems (FM-200, sprinklers)
  - Temperature and humidity regulation
- **Surveillance Systems**:
  - **CCTV**, **motion detectors**, **intrusion alarms**
- **Visitor Management**:
  - **Visitor logs**, **escort policies**
  - **Background checks** for visitors and contractors

🔹 Implement and Manage Physical Security

Physical security management ensures that controls are operational:

- **Regular Audits**: Conduct **physical security assessments** and vulnerability scans.
- **Security Personnel**:
    - **Guards** for patrol and monitoring.
    - Ensure staff are trained in emergency protocols and access control.
- **Security Incident Management**: Have procedures in place to respond to **breaches** (e.g., unauthorized access, theft, or vandalism).
- **Employee Training**: Train staff on **secure behavior**—how to spot social engineering attacks, use of access cards, and emergency response.

DOMAIN-4

CHAPTER 11

🌐 OSI Model

- 7-layer structure: **Physical, Data Link, Network, Transport, Session, Presentation, Application**
- Functions of each layer
- Protocol examples per layer
- Encapsulation/decapsulation processes
- Troubleshooting using the OSI model

🌐 TCP/IP Model

- 4-layer model: **Network Access, Internet, Transport, Application**
- Mapping OSI to TCP/IP
- Protocols at each layer (e.g., IP, TCP, UDP, HTTP, FTP)
- IP addressing and subnetting concepts

📊 Analyzing Network Traffic

- **Packet sniffers** and **protocol analyzers** (e.g., Wireshark)
- Detecting abnormal or malicious traffic
- Flow analysis (NetFlow/sFlow)
- Packet-level inspection and logging
- Indicators of compromise (IOCs)

🖥️ Common Application Layer Protocols

- HTTP/HTTPS
- FTP/SFTP
- SMTP, POP3, IMAP
- Telnet, SSH
- DNS, SNMP
- Protocols' port numbers and default behaviors

- Inherent vulnerabilities (e.g., plaintext transmission, weak authentication)

🛠️ Transport Layer Protocols

- TCP vs. UDP
- TCP handshake (SYN, SYN-ACK, ACK)
- Port numbers and multiplexing
- Session management and state
- TCP flags and control mechanisms
- Flow control, sequencing, error detection

🌍 Domain Name System (DNS)

- DNS hierarchy and record types (A, AAAA, MX, CNAME, PTR, etc.)
- DNS resolution process
- DNS caching and TTL
- DNS over HTTPS (DoH), DNSSEC
- DNS poisoning and spoofing

🌐 Internet Protocol (IP) Networking

- IPv4 and IPv6 structure
- IP headers, addressing, subnetting
- Routing concepts: static vs. dynamic (RIP, OSPF, BGP)
- NAT, PAT
- ICMP usage and abuse (ping, traceroute, DoS vectors)

🧩 ARP Concerns

- ARP operation (broadcast, reply)
- ARP table and cache poisoning
- Man-in-the-middle attacks using ARP spoofing
- Detection and prevention mechanisms

🔐 Secure Communication Protocols

- HTTPS (SSL/TLS)

- IPSec (transport vs tunnel mode, AH vs ESP)
- SSH
- S/MIME, PGP
- VPN protocols (SSL VPN, IPsec VPN, L2TP, PPTP)
- Wireless security protocols (WPA2, WPA3, EAP)

📦 Implications of Multilayer Protocols

- Tunneling (VPNs, GRE, IP-in-IP)
- Encapsulation at different layers
- Protocol dependencies and inter-layer vulnerabilities
- Attack surface across protocol layers

✂️ Segmentation

- Network segmentation benefits (containment, performance)
- VLANs and subnets
- Firewalls and ACLs
- Microsegmentation in virtual environments
- Zero Trust Network Architecture (ZTNA)

🌐 Edge Networks

- Edge computing principles
- Risks at the edge: data exposure, latency
- IoT security at the edge
- Securing edge devices and traffic

📡 Wireless Networks

- Wi-Fi standards (802.11a/b/g/n/ac/ax)
- Wireless security protocols (WEP, WPA2, WPA3)
- Authentication and encryption (EAP, PEAP, PSK)
- Wireless attacks (evil twin, rogue AP, jamming)
- Site surveys and channel planning

🛰️ Satellite Communications

- Satellite types (GEO, MEO, LEO)
- Latency and bandwidth considerations
- Encryption and authentication challenges
- Susceptibility to signal interception and jamming

📱 Cellular Networks

- 3G, 4G, 5G architecture and security
- Base stations, SIM authentication
- IMSI catchers (Stingrays) and threats
- Encryption of voice and data traffic
- Mobile network attacks (e.g., SS7 vulnerabilities)

🕸️ Content Distribution Networks (CDNs)

- CDN architecture and use cases
- Edge caching and latency reduction
- Secure delivery mechanisms (HTTPS, TLS)
- DDoS mitigation and load balancing
- CDN abuse and misconfiguration risks

🧱 Secure Network Components

- Firewalls (stateful, stateless, NGFW)
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Proxies, reverse proxies
- Load balancers and their security implications
- SIEM integration
- Network Access Control (NAC)
- Secure routers and switches (control plane protection, ACLs)

CHAPTER 12

Protocol Security Mechanisms

- Encryption (SSL/TLS, IPsec)
- Authentication methods (Kerberos, certificates)
- Protocol hardening (disabling insecure versions, enforcing strong ciphers)
- Replay prevention and session integrity
- Secure negotiation protocols (e.g., STARTTLS)

📞 **Secure Voice Communications**

- VoIP security (SIP, RTP encryption)
- SRTP (Secure Real-Time Transport Protocol)
- VoIP threat landscape (e.g., call hijacking, eavesdropping)
- Endpoint and server security
- Voice firewalls and VLANs

🌎 **Remote Access Security Management**

- VPN types (SSL, IPsec, L2TP)
- Secure tunneling protocols (SSH, RDP, VNC)
- Strong authentication (MFA, certificates)
- Endpoint compliance enforcement (posture checking)
- Split tunneling risks and controls

👨‍💼 **Multimedia Collaboration**

- Secure conferencing (WebEx, Zoom, MS Teams)
- End-to-end encryption (E2EE)
- Identity verification of participants
- Screen sharing and data leakage risks
- Logging and auditing sessions

📡 **Monitoring and Management**

- Network monitoring tools (SNMP, NetFlow, syslog)

- Security event monitoring (SIEM, NDR)
- Log aggregation and retention policies
- Alerts and anomaly detection
- Performance vs. security considerations

⚖️ Load Balancing

- Load balancing methods (round-robin, least connections)
- Secure session persistence
- Load balancer as security chokepoint (DDoS protection, TLS termination)
- Redundancy and failover
- Web Application Firewalls (WAFs) integration

📧 Manage Email Security

- Email authentication (SPF, DKIM, DMARC)
- Anti-spam and anti-malware filtering
- Email encryption (S/MIME, PGP)
- Phishing and spear-phishing defense
- Data Loss Prevention (DLP)

🔐 Virtual Private Network (VPN)

- VPN protocols (IPsec, SSL, OpenVPN)
- VPN client configurations and security policies
- Split vs. full tunneling
- Authentication mechanisms
- Logging and monitoring VPN access

🔁 Switching and Virtual LANs (VLANs)

- VLAN segmentation and tagging (802.1Q)
- VLAN hopping attacks and prevention
- Private VLANs for isolation
- Inter-VLAN routing and ACLs
- Trunking security and switch hardening

🌐 Network Address Translation (NAT)

- Types of NAT (Static, Dynamic, PAT)
- Security benefits (IP hiding, segmentation)
- Limitations for end-to-end encryption
- NAT traversal (STUN, TURN)
- Use in VPN/firewall integration

🔗 Third-Party Connectivity

- Vendor access controls and segmentation
- Secure tunnels for B2B communications
- Due diligence and third-party risk assessments
- Monitoring and auditing third-party activity
- Contractual obligations (SLAs, liability clauses)

🔄 Switching Technologies

- Layer 2 and Layer 3 switching
- MAC address table security (port security)
- Spanning Tree Protocol (STP) and loop prevention
- Redundancy protocols (HSRP, VRRP)
- QoS and traffic shaping

🛰️ WAN Technologies

- MPLS, leased lines, frame relay, VPN over Internet
- WAN acceleration and optimization
- Routing protocols (OSPF, BGP) in WAN
- High availability and failover
- Secure WAN design (encryption, segmentation)

💡 Fiber-Optic Links

- Fiber vs. copper advantages
- Intrusion detection (optical taps)

- Fiber attenuation and protection
- Secure trenching and physical cable security
- Fiber splicing vulnerabilities

Prevent or Mitigate Network Attacks

- Network intrusion detection and prevention (IDS/IPS)
- DoS/DDoS detection and mitigation (rate limiting, CDN, blackholing)
- Segmentation and microsegmentation
- Protocol-based attacks (ARP spoofing, DNS poisoning, IP spoofing)
- Secure baseline configurations and patching

DOMAIN-5

CHAPTER 13

1. The AAA Model

- **Authentication**: Proving user identity
    - Knowledge (passwords), Ownership (tokens), Inherence (biometrics)
    - Single-factor vs. multifactor authentication (MFA)
- **Authorization**: Granting access to resources based on policies
    - Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC)
- **Accounting (Auditing)**: Logging and monitoring usage
    - Log integrity and retention
    - Event correlation with SIEM systems

---

2. Implementing Identity Management

- **Identity Repositories**: Directories (LDAP, Active Directory), Federated Identity (SAML, OAuth, OpenID Connect)
- **Authentication Services**: Kerberos, RADIUS, TACACS+
- **Federated Identity Systems**: Single Sign-On (SSO), cross-domain identity
- **Biometrics & Smart Cards**: Benefits, drawbacks, spoofing risks
- **Cloud IAM Solutions**: Azure AD, AWS IAM, GCP IAM
- **Decentralized vs. Centralized Identity Models**

---

3. Managing the Identity and Access Provisioning Life Cycle

- **Provisioning**: Creating identities, assigning roles/access based on job function
- **Account Maintenance**: Review, recertification, and privilege audits
- **Deprovisioning**: Immediate revocation of access upon role change or termination
- **Automation**: Workflow automation and ticketing systems for approval chains
- **Access Review and Certification**: Periodic audits, least privilege enforcement
- **Separation of Duties (SoD)**: Preventing fraud by dividing responsibilities

CHAPTER 14

Comparing Access Control Models

- **Discretionary Access Control (DAC)**: Owner-based control, flexible but less secure.
- **Mandatory Access Control (MAC)**: Enforced by system, based on classifications (e.g., Top Secret).
- **Role-Based Access Control (RBAC)**: Access tied to job role; widely used in enterprises.
- **Rule-Based Access Control**: Uses conditional rules (e.g., time-based, location-based).
- **Attribute-Based Access Control (ABAC)**: Uses multiple attributes (user, action, resource, environment) — highly granular.
- **Risk-Adaptive Access Control (RAdAC)**: Access decisions adapt to risk levels and operational needs.

---

2. Implementing Authentication Systems

- **Types of Authentication**:
  - Knowledge (passwords, PINs)
  - Ownership (smart cards, tokens)
  - Inherence (biometrics: fingerprint, iris)
  - Location and behavior-based factors
- **Authentication Protocols**:
  - Kerberos, RADIUS, TACACS+, LDAP
- **Single Sign-On (SSO)**:
  - Reduces login fatigue, requires tight security controls.
- **Federated Identity**:
  - SAML, OAuth 2.0, OpenID Connect
- **Adaptive/Contextual Authentication**:
  - Dynamic risk-based authentication (e.g., requiring MFA only under suspicious conditions)

---

3. Zero-Trust Access Policy Enforcement

- **Core Principle**: "Never trust, always verify."

- **Micro-Segmentation**:
  - Limiting lateral movement inside the network.
- **Least Privilege Enforcement**:
  - Users/systems have only the access needed to perform tasks.
- **Continuous Verification**:
  - Ongoing session evaluation based on behavior and context.
- **Context-Aware Policies**:
  - Access decisions based on device health, geolocation, time-of-day, etc.
- **Identity as the Perimeter**:
  - Users and devices are the new boundary in cloud-native environments.

---

4. Understanding Access Control Attacks

- **Password Attacks**:
  - Brute force, dictionary, credential stuffing
- **Privilege Escalation**:
  - Gaining higher access rights than assigned
- **Man-in-the-Middle (MITM)**:
  - Intercepting authentication or session tokens
- **Session Hijacking**:
  - Stealing session IDs to impersonate users
- **Phishing/Social Engineering**:
  - Trick users into revealing credentials
- **Bypassing Access Controls**:
  - Exploiting misconfigurations or software bugs

DOMAIN-6

CHAPTER15

1. Building a Security Assessment and Testing Program

- Define assessment objectives aligned with business risks
- Identify systems, applications, and processes to be tested
- Establish assessment cadence: continuous, periodic, event-driven
- Integrate assessments into SDLC and operational workflows
- Leverage automation for repeatable, scalable testing

---

2. Performing Vulnerability Assessments

- **Asset Discovery**: Inventory of systems and software
- **Vulnerability Scanning**: Tools (e.g., Nessus, Qualys) to find weaknesses
- **Analysis & Risk Ranking**: CVSS scoring, asset criticality
- **Remediation Planning**: Assigning fixes, timelines, owners
- **Revalidation**: Confirming patch effectiveness

---

3. Testing Your Software

- **Static Application Security Testing (SAST)**: Analyzes code without execution
- **Dynamic Application Security Testing (DAST)**: Tests running applications
- **Interactive Application Security Testing (IAST)**: Combines SAST + DAST
- **Fuzz Testing**: Randomized input to uncover unexpected behavior
- **Secure Code Reviews**: Manual or automated scanning for logic flaws

---

4. Training and Exercises

- **Tabletop Exercises**: Scenario-based discussion to validate response plans
- **Red Team / Blue Team**: Simulated attacks vs. real-time defense
- **Purple Teaming**: Collaborative offense-defense improvement
- **Incident Response Drills**: Technical and communication readiness
- **Continuous Awareness Training**: Role-based security training programs

---

5. Implementing Security Management Processes & Collecting Security Process Data

- **Security Metrics and KPIs**:
    - Patch time-to-close, mean time to detect/respond (MTTD/MTTR), training compliance
- **Audit Trails and Logging**:
    - Collection, retention, integrity, and centralized analysis (SIEM)
- **Risk Assessments**:
    - Periodic evaluations of security posture against evolving threats
- **Change Management Security Checks**:
    - Ensuring security reviews during updates or configuration changes
- **Compliance Checks**:
    - Verifying controls meet regulatory and policy requirements

DOMAIN-7

CHAPTER 16

1. Apply Foundational Security Operations Concepts

- **Need-to-Know / Least Privilege**: Restricting access to only what's necessary
- **Separation of Duties (SoD)**: Reducing fraud and error by dividing responsibilities
- **Job Rotation**: Mitigates insider threats and supports cross-training
- **Fail Secure / Fail Safe**: Secure states in failure scenarios
- **Data Remanence**: Secure data deletion and destruction
- **Logging and Monitoring**: Capturing events, alerts, and trends for analysis
- **Aggregation and Correlation**: Centralizing data for threat detection (SIEM)

---

2. Address Personnel Safety and Security

- **Employee Onboarding and Offboarding Security**: Identity lifecycle, access removal
- **Security Escorts and Access Controls**: Restrict physical access to sensitive areas
- **Travel Safety**: Securing devices and communications while on the move
- **Workplace Violence Policies**: Protecting personnel in high-risk scenarios
- **Incident Reporting Channels**: Anonymous reporting, hotlines

---

3. Provision Information and Assets Securely

- **Asset Tagging and Tracking**: Lifecycle monitoring of physical/digital assets
- **Secure Distribution**: Encrypted transfers, signed packages
- **Chain of Custody**: Provenance and integrity of asset handling
- **User Entitlement Reviews**: Ongoing validation of access rights

---

4. Apply Resource Protection

- **Media Storage and Disposal**: Wiping, degaussing, shredding

- **Backup Controls**: Frequency, integrity, and security of backups
- **Redundancy and Fault Tolerance**: HA, clustering, and load balancing
- **Environmental Controls**: Fire suppression, temperature, humidity management

---

5. Managed Services in the Cloud

- **Cloud Service Models**: IaaS, PaaS, SaaS security differences
- **Third-Party Risk Management**: Due diligence, audits, SLAs
- **Shared Responsibility Model**: Clarifying security roles between provider and customer
- **Cloud Logging & Visibility**: Securing, collecting, and reviewing cloud activity logs

---

6. Perform Configuration Management (CM)

- **Baseline Configurations**: Approved templates for secure deployment
- **Configuration Drift Management**: Detecting unauthorized changes
- **Version Control**: Maintaining traceability of configuration changes
- **Hardening Systems**: Disabling unused services, enforcing security settings

---

7. Manage Change

- **Change Management Process**: Request, assess, approve, implement, and review
- **Security Impact Analysis**: Evaluating risk before changes
- **Emergency Change Controls**: Streamlined but controlled responses to urgent needs
- **Rollback Procedures**: Ensuring recoverability from failed changes

---

8. Manage Patches and Reduce Vulnerabilities

- **Patch Prioritization**: Based on CVSS scores, asset criticality
- **Patch Testing and Deployment**: Ensuring functionality and compatibility
- **Automated Patch Management Tools**: Centralized rollout and reporting
- **Vulnerability Management Lifecycle**: Discover, assess, remediate, and verify

CHAPTER 17

1. Conducting Incident Management

- Incident Response Process
- Incident Response Team (IRT)
- Incident Communication
- Incident Classification

2. Implementing Detection and Preventive Measures

- Threat Detection Mechanisms
- Vulnerability Management
- Access Control Mechanisms
- Preventive Measures
- Security Audits and Risk Assessment

3. Logging and Monitoring

- Log Management
- Monitoring Tools
- Incident Detection through Monitoring
- Log Analysis

4. Automating Incident Response

- Automation Tools
- Incident Response Playbooks
- Incident Response and Recovery Automation
- Integration with Other Security Tools
- Testing and Refining Automation

CHAPTER 18

1. The Nature of Disaster

- **Types of Disasters:**
  - **Natural Disasters:** Earthquakes, floods, hurricanes, fires, etc.
  - **Human-made Disasters:** Terrorist attacks, industrial accidents, cyberattacks, and warfare.
  - **Technological Failures:** Hardware malfunctions, power outages, network failures, etc.
- **Impact of Disasters:**
  - **Operational Impact:** Disruptions to business processes, production, or services.
  - **Financial Impact:** Loss of revenue, increased operational costs, regulatory fines.
  - **Reputational Impact:** Damage to customer trust, market share, and brand value.
- **Business Continuity vs. Disaster Recovery:**
  - Business Continuity ensures that critical business functions continue during and after a disaster.
  - Disaster Recovery focuses on recovering IT systems and data after an incident.

2. Understand System Resilience, High Availability, and Fault Tolerance

- **System Resilience:**
  - The ability of a system to withstand and quickly recover from disruptions.
  - **Techniques**: Redundancy, failover mechanisms, and disaster recovery planning.
- **High Availability (HA):**
  - Ensuring systems and services remain operational with minimal downtime.
  - **Approaches**: Clustering, load balancing, redundant power and network connections, and geographic failover.
- **Fault Tolerance:**
  - Designing systems to continue functioning even if a component fails.
  - **Methods**: Using redundant hardware, error-correcting codes, and self-healing software.

- **Key Concepts:**
    - **Uptime Guarantees**: SLAs (Service Level Agreements) that define availability.
    - **Redundancy**: Duplication of critical components to minimize downtime.

3. Recovery Strategy

- **Recovery Point Objective (RPO):**
    - The maximum acceptable amount of data loss in terms of time.
    - **Implications**: Defines the frequency of backups or snapshots.
- **Recovery Time Objective (RTO):**
    - The maximum time allowed to restore service after an outage.
    - **Implications**: Determines the priority of systems to recover and the resources required.
- **Backup and Redundancy Strategies:**
    - Use of off-site backups, cloud-based storage, or replication to ensure data availability.
    - Implementation of Continuous Data Protection (CDP) for near-zero data loss.
- **Disaster Recovery as a Service (DRaaS):**
    - Outsourcing disaster recovery functions to third-party cloud service providers to reduce costs and ensure timely recovery.

4. Recovery Plan Development

- **Disaster Recovery Plan (DRP):**
    - A formal document that defines procedures for responding to and recovering from disasters.
    - **Contents**: Specific recovery steps, team responsibilities, communication protocols, and contact information.
- **Business Continuity Plan (BCP):**
    - A broader plan that includes maintaining business operations, not just IT systems, during a disaster.
- **Business Impact Analysis (BIA):**
    - Analyzing critical business functions, identifying dependencies, and determining the potential impact of disruptions.
- **Resource Identification:**
    - Identifying key resources (hardware, software, personnel, etc.) necessary for recovery and continuity.

5. Training, Awareness, and Documentation

- **Employee Training:**
    - Regular training programs for staff to ensure they understand their roles during a disaster or outage.
    - **Simulation Drills**: Hands-on exercises and mock disaster recovery tests.
- **Awareness Programs:**
    - Raising awareness across the organization about disaster recovery and business continuity procedures.
- **Documentation:**
    - Ensuring all recovery procedures, plans, and configurations are well-documented and accessible.
    - Documenting roles and responsibilities, communication channels, and recovery steps.

6. Testing and Maintenance

- **Testing Disaster Recovery Plans:**
    - Regular testing of recovery procedures through tabletop exercises, walkthroughs, and full-scale drills.
    - Testing different scenarios to validate recovery time objectives (RTOs) and recovery point objectives (RPOs).
- **Post-Incident Reviews:**
    - After testing or an actual disaster, reviewing the effectiveness of the response and identifying areas for improvement.
- **Updating Plans:**
    - Continual updating of the DRP and BCP based on lessons learned, technological changes, and evolving risks.
- **Vendor and Third-Party Testing:**
    - Ensuring that third-party vendors and partners have their own recovery strategies and plans that integrate with your organization’s recovery efforts.
- **Plan Maintenance:**
    - Ensuring that the disaster recovery and business continuity plans are kept current with the latest technologies, regulatory changes, and business requirements.

CHAPTER 19

1. Investigations

- Incident Investigation Process
- Forensic Investigations
- Evidence Collection and Preservation
- Legal and Regulatory Compliance
- Reporting and Documentation
- Incident Response and Follow-up

2. Major Categories of Computer Crime

- Hacking and Unauthorized Access
- Malware and Viruses
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Data Theft and Fraud
- Cyberstalking and Harassment
- Intellectual Property (IP) Theft
- Phishing and Social Engineering

3. Ethics

- Ethical Principles in Information Security
- Privacy Concerns
- Professional Conduct
- Ethical Dilemmas in Cybersecurity
- Regulatory Compliance and Ethical Boundaries

DOMAIN-8

CHAPTER 20

1. Introducing Systems Development Controls

- Systems Development Life Cycle (SDLC)
- Secure Software Development Practices
- Change Management Controls
- Code Reviews and Static Analysis
- Testing and Validation
- Security Requirements in Development
- Risk Management in Development

2. Establishing Databases and Data Warehousing

- Database Design and Architecture
- Data Modeling and Schema Design
- Data Warehousing Concepts
- Database Security Controls
- Data Integrity and Quality
- Database Access and Permissions
- Data Backup and Recovery in Databases

3. Storage Threats

- Physical Security of Storage Devices
- Data Loss and Corruption Risks
- Data Theft and Breach Risks
- Insider Threats
- Encryption of Stored Data
- Backup Security
- Cloud Storage Security

4. Understanding Knowledge-Based Systems

- Knowledge Management Systems (KMS)
- Expert Systems and Artificial Intelligence
- Decision Support Systems (DSS)
- Machine Learning in Knowledge Systems

- Knowledge Representation Techniques
- Security in Knowledge-Based Systems
- Ethical Issues in Knowledge-Based Systems

CHAPTER 21

1. Malware

- Types of Malware (Viruses, Worms, Trojans, etc.)
- Malware Propagation Methods
- Malware Behavior and Analysis
- Detection and Removal of Malware
- Malware Impact on Systems and Networks

2. Malware Prevention

- Antivirus and Antimalware Software
- Behavior-Based Detection Techniques
- Endpoint Protection Systems
- Sandboxing and Virtualization
- Regular Patching and Updates
- User Awareness and Training

3. Application Attacks

- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Buffer Overflow Attacks
- Directory Traversal Attacks
- Session Hijacking
- Denial of Service (DoS) Attacks

4. Injection Vulnerabilities

- SQL Injection
- Command Injection
- LDAP Injection
- XML Injection
- Code Injection

5. Exploiting Authorization Vulnerabilities

- Broken Access Control
- Privilege Escalation
- Insecure Direct Object References (IDOR)
- Inadequate Authentication

- Misconfigured Authorization Settings

6. Exploiting Web Application Vulnerabilities

- Cross-Site Scripting (XSS)
- SQL Injection
- Cross-Site Request Forgery (CSRF)
- Remote File Inclusion (RFI)
- Security Misconfigurations
- Insufficient Logging and Monitoring

7. Application Security Controls

- Input Validation and Output Encoding
- Authentication and Authorization Controls
- Session Management Controls
- Data Encryption and Integrity
- Web Application Firewalls (WAF)
- Secure Software Development Lifecycle (SDLC)

8. Secure Coding Practices

- Input Validation and Sanitization
- Principle of Least Privilege
- Error Handling and Logging
- Avoiding Hardcoded Credentials
- Use of Secure Communication Protocols
- Secure Session Management
- Code Review and Static Analysis