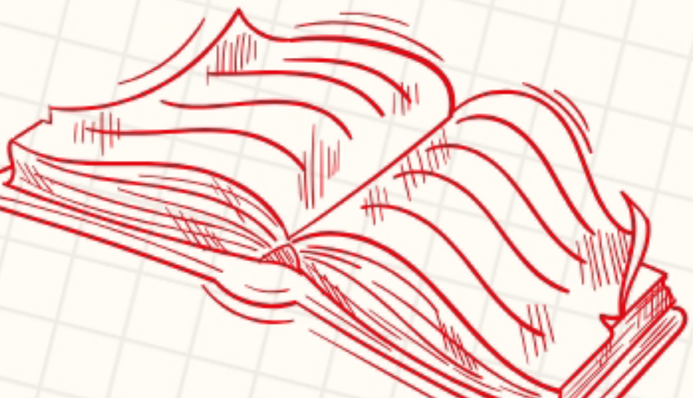
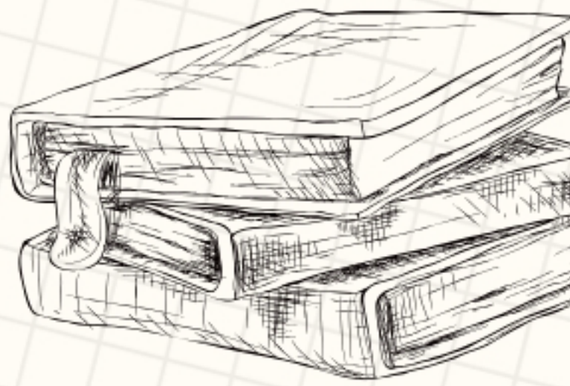
INFOSECTRAIN

MIND MAP

CISSP DOMAIN 7

SECURITY OPERATIONS





INFOSECTRAIN

7.1: UNDERSTANDING AND COMPLYING WITH INVESTIGATIONS

CISSP DOMAIN 7

- **Evidence Collection and Handling** — Properly gather, store, and preserve evidence while maintaining its integrity
- **Reporting and Documentation** — Record investigation findings and maintain thorough documentation
- **Investigative Techniques** — Use systematic approaches to gather and analyze evidence
- **Digital Forensic Tools, Tactics, and Procedures** — Use specialized tools and procedures to analyze digital data
- **Artifacts** — Identify and analyze digital artifacts (files, logs, etc.)

INFOSECTRAIN

7.2: CONDUCT LOGGING AND MONITORING ACTIVITIES

CISSP DOMAIN 7

- **Intrusion Detection and Prevention (IDS/IPS)** — Detect and prevent network intrusions
- **Security Information and Event Management (SIEM)** — Centralized logging and threat detection
- **Continuous Monitoring** — Ongoing assessment of security status
- **Egress Monitoring** — Monitoring outbound network traffic
- **Log Management** — Collect and store log data
- **Threat Intelligence** — Gather and analyze threat data
- **User and Entity Behavior Analytics (UEBA)** — Analyze user and entity behavior patterns

INFOSECTRAIN

7.3: PERFORM CONFIGURATION MANAGEMENT (CM)

CISSP DOMAIN 7

- **Identify Configuration Items** — List all configuration components
- **Baseline Establishment** — Define standard configuration settings
- **Change Management** — Control changes to configurations
- **Configuration Status Accounting** — Track and document configurations
- **Configuration Verification and Audit** — Ensure compliance with configurations
- **Automated Tool Utilization** — Use software for CM tasks

INFOSECTRAIN

7.4: APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

CISSP DOMAIN 7

- **Need-to-Know/Least Privilege**
  - **Need-to-Know** — Access only to information necessary for a role
  - **Least Privilege** — Minimum level of access required for job functions
- **Separation of Duties (SoD)** — Divide responsibilities among different individuals
- **Privileged Account Management** — Control and monitor privileged accounts
- **Job Rotation** — Reduce risk and prevent collusion
- **Service Level Agreements (SLAs)**
  - **Purpose** — Define performance and security expectations
  - **Components** — Uptime guarantees, response times, and security measures

INFOSECTRAIN

7.5: APPLY RESOURCE PROTECTION

CISSP DOMAIN 7

- **Media Management**
  - Inventory tracking
  - Labeling and classification
  - Secure storage
  - Controlled access
- **Media Protection Techniques**
  - **Physical Security**
    - Secure storage locations (e.g., locked cabinets)
    - Environmental controls (e.g., temperature, humidity)
  - **Logical Security**
    - Encryption of data on media
    - Access controls (e.g., user authentication)
  - **Handling Procedures**
    - Secure transportation
    - Sanitization and destruction
    - Regular audits and monitoring

INFOSECTRAIN

7.6: CONDUCT INCIDENT MANAGEMENT

CISSP DOMAIN 7

- **Detection** — Identify incidents via logs and alerts
- **Response** — Immediate actions to contain incident
- **Mitigation** — Address root cause, prevent recurrence
- **Reporting** — Document incident, response, lessons learned
- **Recovery** — Restore systems and data functionality
- **Remediation** — Fix vulnerabilities causing incident
- **Lessons Learned** — Implement security improvements post-incident

INFOSECTRAIN

7.7: OPERATE AND MAINTAIN DETECTIVE AND PREVENTIVE MEASURES

CISSP DOMAIN 7

- **Firewalls**
  - Control traffic via security policies
  - Types
    - Next-gen
    - web application
    - Network
- **Intrusion Detection/Prevention Systems (IDS/IPS)** — Monitor and prevent unauthorized access
- **Whitelisting/blacklisting**
  - **Whitelisting** — Allow authorized applications/users
  - **Blacklisting** — Block malicious applications/users
- **Third-party provided security services** — Managed Detection and Response (MDR)
- **Sandboxing** — Isolated environment to analyze suspicious code/files
- **Honeypots/honeynets** — Decoy systems to lure and capture attackers
- **Anti-malware** — Protect against malicious software
- **Machine learning and Artificial Intelligence tools** — Anomaly detection and threat hunting

INFOSECTRAIN

7.8: IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

CISSP DOMAIN 7

- **Identify and Classify Vulnerabilities**
  - **Vulnerability Scanning** — Detect vulnerabilities
  - **Risk Assessment** — Prioritize based on risk
- **Patch Management Process**
  - **Patch Identification** — Vendor patches
  - **Patch Testing** — Test before deployment
  - **Patch Deployment** — Apply patches
  - **Patch Verification** — Ensure correct application
- **Vulnerability Management Process**
  - **Discovery** — Monitor continuously
  - **Analysis** — Assess impact
  - **Remediation** — Apply fixes
  - **Verification** — Confirm resolution
- **Tools and Technologies**
  - **Patch Management Tools** — Automate deployment
  - **Vulnerability Management Tools** — Automate scanning
  - **Configuration Management** — Maintain secure configurations

INFOSECTRAIN

7.9: UNDERSTAND AND PARTICIPATE IN CHANGE MANAGEMENT PROCESSES

CISSP DOMAIN 7

- **Purpose of Change Management**
  - Manage and control changes
  - Reduce the impact of changes
  - Maintain business continuity
- **Change Management Process**
  - **Request for Change (RFC)** — Submit and track change requests
  - **Impact Assessment** — Evaluate the potential effects of changes
  - **Approval Process** — Gain authorization for proposed changes
  - **Implementation** — Execute approved changes
  - **Testing and Validation** — Ensure the change works as intended
  - **Documentation** — Record all changes for future reference
- **Types of Changes**
  - **Standard Changes** — Pre-approved, low-risk changes
  - **Emergency Changes** — Unplanned, urgent changes
  - **Major Changes** — High-impact, complex changes

INFOSECTRAIN

7.10: IMPLEMENT RECOVERY STRATEGIES

CISSP DOMAIN 7

- **Backup Storage Strategies**
  - **Types** — Full, incremental, differential
  - **Locations** — On-site, off-site, cloud
  - **Frequency** — Regular scheduling
- **Recovery Site Strategies**
  - **Hot Sites** — Fully operational, minimal downtime
  - **Warm Sites** — Partially equipped, moderate setup time
  - **Cold Sites** — Basic infrastructure, significant setup time
- **Multiple Processing Sites**
  - **Primary and Secondary Sites** — Ensure business continuity
  - **Load Balancing** — Distribute workload across multiple sites
  - **Geographical Separation** — Reduce risk from localized disasters
- **System Resilience, HA, QoS, and Fault Tolerance**
  - **System Resilience** — Ability to recover from failures
  - **High Availability (HA)** — Minimizing downtime through redundancy
  - **Quality of Service (QoS)** — Ensuring performance standards
  - **Fault Tolerance** — Continuous operation despite failures

INFOSECTRAIN

7.11: IMPLEMENT DISASTER RECOVERY (DR) PROCESSES

CISSP DOMAIN 7

- **Response** — Follow DR plan to initiate recovery procedures
- **Personnel** — Assign roles and responsibilities
- **Communications** — Establishing clear communication channels
- **Assessment** — Evaluate damage and scope of recovery
- **Restoration** — Restore systems and data
- **Training and awareness** — Train personnel on DR procedures
- **Lessons learned** — Review and improve DR process

INFOSECTRAIN

7.12: PARTICIPATE IN BUSINESS CONTINUITY (BC) PLANNING AND EXERCISES

CISSP DOMAIN 7

- **Understand Business Continuity (BC)**
  - **Definition** — Continuous operations during/after a disaster
  - **Importance** — Minimize disruption and loss
- **Conduct Business Impact Analysis (BIA)**
  - Identify critical functions
  - Prioritize recovery efforts
- **Develop Business Continuity Plan (BCP)**
  - Recovery strategies
  - Document procedures
  - Define roles
- **Implement Recovery Strategies**
  - Backup solutions
  - Alternative sites
  - Redundant systems
- **Conduct Training and Awareness**
  - Regular training
  - Awareness programs
- **Perform Testing and Exercises**
  - Tabletop exercises
  - Functional tests
  - Full-scale drills
- **Review and Update the BCP**
  - Regular updates
  - Incorporate changes
- **Integrate with Incident Response Plan**
  - Align plans
  - Streamline processes

FOUND THIS USEFUL?

Get More Insights Through Our FREE

Courses

Workshops

eBooks

Checklists

Mock Tests

INFOSECTRAIN