Introduction to Cybersecurity

- **CIA Triad**, Separation of Duties, Organizational Structure, Top-Down and Bottom-Up Approach
- **Information Availability**
  - Recovery Time Objective (RTO), Recovery Point Objective (RPO), Maximum Tolerable Downtime (MTD), SLA
- **Data Security: Disclosure, Alteration, and Destruction**
  - Identification, Authentication, Authorization, Accountability, and Auditing (IAAAA protocols)

Corporate Governance and Plans

- Introduction to Corporate Governance
- Strategic, Tactical, and Operational Plans
- Policies, Standards, Procedures, and Guidelines

Data Protection Mechanisms

- Data Layering, Abstraction, Data Hiding, Encryption

Data Classification Methodologies

- Confidential, Sensitive, Top Secret, Private, Public, Unclassified

Risk Management

- Asset Management, Threat and Vulnerability, Threat Agent, Exploit
- Quantitative and Qualitative Risk Assessment
- Risk Management Life Cycle: Assessment, Analysis, Mitigation, and Response
- Risk Management Framework: ISO 27001, ISO 31000, ISO 27000

Internal Controls

- Preventive, Detective, and Corrective Controls

Threat Identification Models

- STRIDE, DREAD

Disaster Recovery and Business Continuity Management

- Contingency Plans, BCP Documentation, DR Documentation, Types of Tests

Information Systems Laws and Regulations

- Criminal, Civil, and Administrative Laws (e.g., Computer Security Act, CFAA, GISRA, FISMA)
- Regulations: PCI-DSS, GDPR, HIPAA, Hi-Trust, SOX, ISO Series

Intellectual Property

- Copyright, Trademark, Patents, Trade Secrets

Data Security Controls and Ownership

- Data in Use, Data at Rest, Data in Transit
- Data Custodian, Data Processor, Data Controller, System Owners, Administrators, End Users

Data Destruction Mechanisms

- Sanitize, Degaussing, Erase, Overwrite

Security Architecture Framework and Security Models

- Zachman Framework, Sherwood Applied Business Security Architecture (SABSA), ITIL
- State Machine Models, Multilevel Lattice Models, Information Flow Models

Mobile Security

- Device Encryption, Remote Wiping, Remote Lockout
- Internal Locks (Voice, Face Recognition, Pattern, PIN, Password)
- Application Installation Control, Asset Tracking (IMEI)
- Mobile Device Management, Removable Storage (SD Card, MicroSD)

IoT and Internet Security

- Network Segmentation (Isolation), Logical Isolation (VLAN), Physical Isolation (Network Segments)
- Application Firewalls, Firmware Updates

Physical Security

- Various Threats to Physical Security

System Virtualization

- Guest OS, Virtualization Threats, Cloud Computing Models, Cloud Computing Threats

Web Security

- OWASP, OWASP Top 10, SQL Injection, XSS, CSRF

Cryptography

- Goals of Cryptography, Symmetric and Asymmetric Encryption
- Digital Signature, Hashing, Cryptographic Algorithms (DES, AES, IDEA, Twofish)

Network Security

- OSI Model, Attacks in OSI Layers, Network Types, Standards
- Network Hardware Devices, VPN Protocols

Firewall and Perimeter Security

- Types of Firewalls, DMZ, Honeypot, Honeynet

Different Types of Network Attacks

- Virus, Worms, Logic Bomb, Trojan, Backdoor, Sniffing, Zero-Day Attack, Ransomware, Rootkit, Spyware, DoS, DDoS, Botnet

Email Security

- LDAP, SASL, S/MIME

Identity and Access Management

- Three-Factor Authentication, SSO, Authorization, Federated Identity
- Access Control Models, Categories, and Types

Vulnerability Assessment and Penetration Testing

- Steps Involved, Test Types, Test Strategies, Reporting

Software Development and Testing

- Development Models, Lifecycle, Testing Types, Code Review

Security Operations and Incident Management

- Evidence Lifecycle, IDS, IPS, Backup, SIEM, Hardening Process

Threat Hunting and Attack Framework

- Cyber Kill Chain Process, MITRE ATT&CK Framework, Threat Hunting Benefits

Social Engineering Attacks

- Phishing, Spear Phishing, Whaling, Piggybacking, Watering Hole

Assessment and Knowledge Test

- Viva and Interview Preparation

SOC & SIEM

- **Introduction to SOC**
  - SOC Roles and Responsibilities, SOC Tiers (Tier 1, Tier 2, Tier 3)
  - Key SOC Tools and Technologies
- **SIEM Basics**
  - Log Collection, Normalization, Correlation, and Reporting
  - Key SIEM Components (Log Sources, Correlation Rules, Dashboards)
  - Popular SIEM Tools (Splunk, IBM QRadar, Microsoft Sentinel, ArcSight)
- **Threat Detection and Incident Response**
  - Common Cyber Threats, Threat Intelligence Integration in SIEM
  - Incident Response Process (Identify, Contain, Eradicate, Recover)
  - Hands-on: Analyzing a Simulated Security Incident in SIEM

Cloud Security Training

- **Introduction to Cloud Security**
  - Cloud Computing (IaaS, PaaS, SaaS), Shared Responsibility Model
  - Cloud Security Challenges

- **Cloud Security Best Practices**
  - Identity and Access Management (IAM), Encryption, Network Security (NSG, Firewalls, WAF)
- **Cloud Threats and Compliance**
  - Common Cloud Security Threats (Misconfigurations, Data Breaches, Privilege Escalation)
  - Compliance Frameworks (CIS Benchmark, NIST, ISO 27001, GDPR)
