CISSP Certification Training Course Outline

Duration: 40 Hours
Level: Advanced
Delivery Mode: Online / Offline
Certification: CISSP by (ISC)²
Target Audience: Information Security Professionals, IT Managers, Security Consultants, Network Architects

---

Module 1: Security and Risk Management

- Confidentiality, Integrity, and Availability (CIA Triad)
- Security Governance Principles
- Compliance Requirements
- Legal and Regulatory Issues
- Risk Management Concepts
- Threat Modeling and Business Continuity
- Security Awareness and Education
- Professional Ethics (ISC)² Code of Ethics

Module 2: Asset Security

- Classification and Ownership of Information and Assets
- Privacy Protection
- Secure Data Handling and Retention
- Data Security Controls
- Information Lifecycle
- Data Remanence and Destruction Techniques

Module 3: Security Architecture and Engineering

- Secure Design Principles
- Security Models (Bell-LaPadula, Biba, Clark-Wilson)
- System Architecture (Trusted Computing Base, TPM, etc.)
- Cryptography Concepts and Implementation
- Physical Security Controls
- Vulnerabilities of System Components

Module 4: Communication and Network Security

- Network Architecture Design
- Secure Communication Channels
- Network Protocols and Port Security
- Secure Routing and Switching
- Wireless Security
- Firewalls, VPNs, and IDS/IPS Systems

Module 5: Identity and Access Management (IAM)

- Identification, Authentication, and Authorization
- Access Control Models (RBAC, ABAC, MAC, DAC)
- Identity as a Service (IDaaS)
- Identity Federation and Single Sign-On (SSO)
- Provisioning and Deprovisioning of Access

Module 6: Security Assessment and Testing

- Designing and Conducting Security Assessments
- Security Audits and Log Reviews
- Vulnerability Scanning and Penetration Testing
- Security Metrics and Reporting
- Testing Security Processes and Controls

Module 7: Security Operations

- Incident Response Management
- Disaster Recovery and Business Continuity Planning
- Logging and Monitoring Activities
- Patch and Change Management
- Malware Protection
- Resource Protection and Secure Operations

Module 8: Software Development Security

- Secure Software Development Lifecycle (SDLC)
- Security in DevOps and Agile Environments
- Threat Modeling in Development
- Code Quality and Security Controls
- Software Security Testing
- Secure Deployment and Maintenance

CISSP Exam Preparation and Practice

- CISSP Exam Domains Review (8 Domains)
- Practice Exams and Case Studies
- Exam Techniques and Time Management
- Post-Certification Guidance and Continuing Education