

Who Should Attend:

This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals, who are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current computer security careers or to migrate to a related career. Through the study of all eight CISSP Common Body of Knowledge (CBK) domains, students will validate their knowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certification exam. Additional CISSP certification requirements include a minimum of five years of direct professional work experience in two or more fields related to the eight CBK security domains, or a college degree and four years of experience.

Lesson 1: Security Fundamentals

- The Information Security Cycle
- Information Security Controls
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

Lesson 2: Identifying Security Threats and Vulnerabilities

- Social Engineering
- Malware
- Software-Based Threats
- Network-Based Threats
- Wireless Threats and Vulnerabilities
- Physical Threats and Vulnerabilities

Lesson 3: Managing Data, Application, and Host Security

- Manage Data Security
- Manage Application Security
- Manage Device and Host Security
- Manage Mobile Security

Lesson 4: Implementing Network Security

- Configure Security Parameters on Network Devices and Technologies
- Network Design Elements and Components
- Implement Networking Protocols and Services

- Apply Secure Network Administration Principles
- Secure Wireless Traffic

Lesson 5: Implementing Access Control, Authentication, and Account Management

- Access Control and Authentication Services
- Implement Account Management Security Controls

Lesson 6: Managing Certificates

- Install a CA Hierarchy
- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Back Up and Restore Certificates and Private Keys
- Revoke Certificates

Lesson 7: Implementing Compliance and Operational Security

- Physical Security
- Legal Compliance
- Security Awareness and Training
- Integrate Systems and Data with Third Parties
-

Lesson 8: Risk Management

- Risk Analysis
- Implement Vulnerability Assessment Tools and Techniques
- Scan for Vulnerabilities
- Mitigation and Deterrent Techniques
-

Lesson 9: Troubleshooting and Managing Security Incidents

- Respond to Security Incidents
- Recover from a Security Incident

Lesson 10: Business Continuity and Disaster Recovery Planning

- Business Continuity
- Plan for Disaster Recovery
- Execute DRPs and Procedures

