

## **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 & Risk Management**

- Topic A: Security Governance Principles
- Topic B: Compliance
- Topic C: Professional Ethics
- Topic D: Security Documentation
- Topic E: Risk Management
- Topic F: Threat Modeling
- Topic G: Business Continuity Plan Fundamentals
- Topic H: Acquisition Strategy and Practice
- Topic I: Personnel Security Policies
- Topic J: Security Awareness and Training

## **Lesson 2: Asset Security**

- Topic A: Asset Classification
- Topic B: Privacy Protection
- Topic C: Asset Retention
- Topic D: Data Security Controls
- Topic E: Secure Data Handling

## **Lesson 3: Security Engineering**

- Topic A: Security in the Engineering Lifecycle
- Topic B: System Component Security
- Topic C: Security Models
- Topic D: Controls and Countermeasures in Enterprise Security
- Topic E: Information System Security Capabilities
- Topic F: Design and Architecture Vulnerability Mitigation
- Topic G: Vulnerability Mitigation in Embedded, Mobile, and Web-Based Systems

- Topic H: Cryptography Concepts
- Topic I: Cryptography Techniques
- Topic J: Site and Facility Design for Physical Security
- Topic K: Physical Security Implementation in Sites and Facilities

#### **Lesson 4: Communications & Network Security**

- Topic A: Network Protocol Security
- Topic B: Network Components Security
- Topic C: Communication Channel Security
- Topic D: Network Attack Mitigation

#### **Lesson 5: Identity and Access Management**

- Topic A: Physical and Logical Access Control
- Topic B: Identification, Authentication, and Authorization
- Topic C: Identity as a Service
- Topic D: Authorization Mechanisms
- Topic E: Access Control Attack Mitigation

#### **Lesson 6: Security Assessment and Testing**

- Topic A: System Security Control Testing
- Topic B: Software Security Control Testing
- Topic C: Security Process Data Collection
- Topic D: Audits

#### **Lesson 7: Security Operations**

- Topic A: Security Operations Concepts
- Topic B: Physical Security
- Topic C: Personnel Security
- Topic D: Logging and Monitoring
- Topic E: Preventative Measures
- Topic F: Resource Provisioning and Protection
- Topic G: Patch and Vulnerability Management
- Topic H: Change Management
- Topic I: Incident Response
- Topic J: Investigations
- Topic K: Disaster Recovery Planning
- Topic L: Disaster Recovery Strategies
- Topic M: Disaster Recovery Implementation

#### **Lesson 8: Software Development Security**

- Topic A: Security Principles in the System Lifecycle
- Topic B: Security Principles in the Software Development Lifecycle
- Topic C: Database Security in Software Development
- Topic D: Security Controls in the Development Environment
- Topic E: Software Security Effectiveness Assessment