CERTIFIED INFORMATION SYSTEM SECURITY PROFFESSONAL (CISSP)

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 domains, students will validate their knowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certification exam.

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.

Course Objectives

Upon successful completion of this course, students will be able to:

- Analyze components of the Security and Risk Management domain.
- Analyze components of the Asset Security domain.
- Analyze components of the Security Engineering domain.
- Analyze components of the Communications and Network Security domain.
- Analyze components of the Identity and Access Management domain.
- Analyze components of the Security Assessment and Testing domain.
- Analyze components of the Security Operations domain.
- Analyze components of the Software Development Security domain.

Course Outline

1 - SECURITY & RISK MANAGEMENT

- Security Governance Principles
- Compliance
- Professional Ethics
- Security Documentation
- Risk Management
- Threat Modeling

- Business Continuity Plan Fundamentals
- Acquisition Strategy and Practice
- Personnel Security Policies
- Security Awareness and Training

2 - ASSET SECURITY

- Asset Security
- Privacy Protection
- Asset Retention
- Data Security Controls
- Secure Data Handling

3 - SECURITY ENGINEERING

- Security in the Engineering Lifecycle
- System Component Security
- Models Controls and Countermeasures in Enterprise Security
- Information System Security Capabilities
- Design and Architecture Vulnerability Mitigation
- Vulnerability Mitigation in Embedded, Mobile, and Web-Based Systems
- Cryptography Concepts
- Cryptography Techniques
- Site and Facility Design for Physical Security
- Physical Security Implementation in Sites and Facilities

4 - COMMUNICATIONS AND NETWORK SECURITY

- Network Protocol Security
- Network Components Security
- Communication Channel Security
- Network Attack Mitigation

5 - IDENTITY AND ACCESS MANAGEMENT (IAM)

- Physical and Logical Access Control
- Identification, Authentication, and Authorization
- Identity as a Service

- Authorization Mechanisms
- Access Control
- Attack Mitigation

6 - SECURITY ASSESSMENT AND TESTING

- System Security Control
- Test Software Security
- Control Testing Security
- Process Data Collection
- Audits

7 - SECURITY OPERATIONS

- Security Operations Concepts
- Physical Security
- Personnel Security
- Logging and Monitoring
- Preventative Measures
- Resource Provisioning and Protection
- Patch and Vulnerability Management
- Change Management
- Incident Response Investigations
- Disaster Recovery Planning
- Disaster Recovery Strategies
- Disaster Recovery Implementation

8 - SOFTWARE DEVELOPMENT SECURITY

- Security Principles in the System Lifecycle
- Security Principles in the Software Development Lifecycle
- Database Security in Software Development
- Security Controls in the Development Environment
- Software Security Effectiveness Assessment