Certified Information Security Systems Professional (CISSP)

Course Overview

In this course, students will expand upon their knowledge by addressing the essential elements of the 8 domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals.

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.

Course Objectives

- 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.

Suggested Prerequisites

- CompTIA Network+ Certification
- CompTIA Security+ Certification

Course Outline

1 - Security and 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 Classification
- Privacy Protection
- Asset Retention
- Data Security Controls
- Secure Data Handling

3 - Security Engineering

- Security in the Engineering Lifecycle
- System Component Security
- 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 - Information Security Management Goals

- Organizational Security
- The Application of Security Concepts

5 - Information Security Classification and Program Development

- Information Classification
- Security Program Development

6 - Risk Management and Ethics

- Risk Management
- Ethics

7 - Software Development Security

- Software Configuration Management
- Software Controls
- Database System Security

8 - Cryptography

- Ciphers and Cryptography
- Symmetric-Key Cryptography
- Asymmetric-Key Cryptography
- Hashing and Message Digests
- Email, Internet, and Wireless Security
- Cryptographic Weaknesses

9 - Physical Security

- Physical Access Control
- Physical Access Monitoring
- Physical Security Methods
- Facilities Security