Certified Information Security Systems Professional (CISSP)

Duration	Delivery Methods
5 Days	VILT, Private Group

The CISSP certification preparatory course teaches students how to design, build and maintain a secure business IT architecture using globally approved security standards. Students learn about the eight domains of knowledge, as determined by (ISC)2, that form a critical part of the CISSP® exam. The course covers each knowledge domain in depth and explains how they relate to each other and other critical areas of information security.

(ISC)^2 was founded in 1989 as the International Information System Security Certification Consortium, Inc., an international, nonprofit membership association for information security leaders. That same year, (ISC)^2 published the first Common Body of Knowledge (CBK) to document best practices, skills, and techniques for security professionals. Today the CISSP certification is internationally recognized and respected as the premier cybersecurity professional credential.

CISSP certification is a unique IT certification because it requires a demonstrated fundamental understanding of the eight domains of cybersecurity and documented proof of experience in the information security and architecture field. This training course helps students acquire a broad range of cybersecurity skills, from developing security policies to managing risk to understanding technical security controls.

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.

It is also highly recommended that students complete the CompTIA Network+ CompTIA and Security+ certifications or possess equivalent professional experience upon beginning CISSP training. Students will also benefit from having one or more of the following security-related or technology-related certifications or equivalent industry experience: MCSE, MCTS, MCITP, SCNP, CCNP, RHCE, LCE, CNE, SSCP®, GIAC, CISA™, or CISM®.

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.

Agenda

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

Prerequisites

It is highly recommended that students have certifications in Network+ or Security+, or possess equivalent professional experience upon entering CISSP training. It will be beneficial if students have one or more of the following security-related or technology-related certifications or equivalent industry experience: MCSE, MCTS, MCITP, SCNP, CCNP, RHCE, LCE, CNE, SSCP®, GIAC, CISA™, or CISM®.

Prerequisite Courses Recommended

- CompTIA Network+