Online Certified Information Systems Security Professional (CISSP) Course

150 Hours / 6 Months

Course Description

Our Certified Information Systems Security Professional (CISSP) training is an engaging, fully online course that provides in-depth instruction in key areas related to information/cyber security.

The Certified Information Systems Security Professional (CISSP) course is designed to ensure that someone handling computer security for a company or client has mastered a standardized body of knowledge. Certified Information Systems Security Professional (CISSP) has developed as the key certification for security professionals in government and industry. Corporations are seeking certified, experienced information security professionals to safeguard their information and assets. The CISSP® is considered the global standard that proves an individual's proficiency in several security disciplines. Security professionals consider the Certified Information Systems Security Professional (CISSP) to be the most desired certification to achieve.

Prerequisites

This is an advanced level course. Students should have a base knowledge or certification in SSCP. If students wish to take the course without the foundational topics of SSCP, the student is expected to supplement course materials with outside resources.

For certification through (ISC)2, an individual must have a minimum of five-years of paid, full-time work experience in two of the eight domains of CISSP. A one-year experience waiver can be used in place of a four-year college degree or equivalent through an (ISC)2 approved list.

Once a person passes the (ISC)2 vendor exam, an endorsement is also required. This endorsement form must be signed by two (ISC)2 professional who are active members and can verify your professional experience.

Hardware Requirements

- This course can be taken on either a PC or Mac device.
- Mac users are encouraged to have access to a Windows environment on their device.

Software Requirements

- PC: Windows 7 or later.
- Mac: OS X Snow Leopard 10.6 or later.
- Browser: The latest version of Google Chrome or Mozilla Firefox are preferred. Microsoft Edge and Safari are also compatible.
- Adobe Flash Player. Click here to download the Flash Player.
- Adobe Acrobat Reader. Click here to download the Acrobat Reader.
- Email capabilities and access to a personal email account.
- Software must be installed and fully operational before the course begins.

Course Outline

The Online CISSP Course is broken down into eight practical modules that directly correspond to the CISSP study guide.

MODULE	TOPICS COVERED	
1: Security and Risk Management	• Security Governance • Security Policies • Confidentiality • Business Continuity	• Legal and Regulatory • Professional Ethic • Risk Management
2: Asset Security	• Information Classification • Handling Requirements • Ownership	• Data Security Controls • Protect Privacy • Retention
3: Security Engineering	• Security Models • Security Designs • Engineering Processes • Vulnerabilities	• Cryptography • Embedded Devices • Site Design and Security
4: Communication and Network Security	• Network Architecture Design • Network Components	• Communication Channels • Network Attacks
5: Identity and Access Management	• Physical and Logical Assets Control • Identification and Authentication • Third-Party Identity Services	• Identity as a Service • Provisioning Lifecycle • Authorization Mechanisms
6: Security Assessment and Testing	• Assessment and Test Strategies • Test Outputs • Security Control Testing	• Security Process Data • Security Architectures
7: Security Operations	• Foundational Security Operations Concepts • Logging, Monitoring and Investigating Activities • Provisioning of Resources • Management Processes	• Physical Security • Preventative Measures • Business Continuity
8: Software Development Security	• Security in the Software Development Lifecycle • Development Environment Security Controls • Software Security Effectiveness	• Software Security Impact