Certified Information Systems Security Professional

CISSP

Course Title: CISSP

Duration: 5 days, 40 Hrs

Class Format Options:
Instructor-Led Training/
Classroom

Who Should Attend:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect
- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Director of Security
- Network Architect

Course Overview

Led by an (ISC)² authorized instructor, this training seminar provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP CBK:

- Security and Risk Management
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Asset Security
- Security Engineering
- Security Operations
- Software Development Security

Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam and features:

- Official (ISC)² courseware
- Student handbook
- Taught by an authorized (ISC)² instructor
- Collaboration with classmates
- Real-world learning activities and scenarios

Upon Completion

Students will have knowledge to:

* Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure business environment
* Ensure professionals stay current on emerging threats, technologies, regulations, standards, and practices through the continuing professional education requirements
* Increase confidence that candidates are qualified and committed to information security
* Ensure employees use a universal language, circumventing ambiguity with industry-accepted terms and practices
* Increase organizations credibility when working with clients and vendors

Course Content

- Security and Risk Management
- Asset Security
- Security Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security