

## Certified Information Systems Security Professional (CISSP)®

### Course Specifications

Course length: 5.0 day(s)

### Course Description

Welcome to Certified Information Systems Security Professional (CISSP)®. With your completion of the prerequisites and necessary years of experience, you are firmly grounded in the knowledge requirements of today's security professional. This course will expand upon your knowledge by addressing the essential elements of the 10 domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals. The course offers a job-related approach to the security process, while providing the basic skills required to prepare for CISSP certification.

**Course Objective:** You will control access to data and information systems using common access control best practices. You will discover how networks are designed for security, and the components, protocols, and services that allow telecommunications to occur in a secure manner. Next, you will learn about the principles of security management and how to manage risk as part of a comprehensive information security management program. You will explore applications and systems development security controls. Then, you will learn how to perform cryptography and how to secure system architecture. You will examine operations security and the appropriate controls and best practices to use to keep operations secure. You will learn how to perform business continuity planning and apply physical security to protect organizational assets and resources. Finally, you will explore law, investigations, and ethics with respect to information systems security and computer forensics.

**Target Student:** Students pursuing CISSP training want to establish themselves as credible computer security professionals through a study of all 10 CISSP Common Body of Knowledge domains. Validating this knowledge is the goal of certification; therefore, students attending this training should also meet the requirements needed to sit for the CISSP certification exam. These include four years of direct professional work experience in one or more fields related to 10 CBK security domains, or a college degree and three years of experience. Check with (ISC)2 for the most up-to-date requirements. New certifications have emerged and will continue to emerge from (ISC)2, which may cause changes to base requirements.

**Prerequisites:** Students should have certifications in A+, Network+, or Security+, or possess equivalent professional experience. Students may have one or more of the following certifications or equivalent experience: MCSE, SCNP, CCNP, RHCE, LCE, CNE, SSCP, SANS, or GIAC.

**Delivery Method:** Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

### Hardware Requirements

- A CD-ROM drive.
- A mouse or other pointing device.
- A 1024 x 768 resolution monitor.
- A projection system to display the instructor's computer screen.

## Performance-Based Objectives

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

- Control access to information systems.
- Network systems and telecommunications.
- Define security management.
- Create applications security.
- Perform cryptography.
- Secure system architecture.
- Execute operations security.
- Perform business continuity planning.
- Apply physical security.
- Apply law, investigations, and ethics.

## Course Content

### Lesson 1: Controlling Access to Information Systems

Topic 1A: Control Data Access

Topic 1B: Control System Access

Topic 1C: Determine an Access Control Administration Method

Topic 1D: Perform a Penetration Test

### Lesson 2: Networking Systems and Telecommunications

Topic 2A: Design Data Networks

Topic 2B: Provide Remote Access to a Data Network

Topic 2C: Secure a Data Network

Topic 2D: Manage a Data Network

### Lesson 3: Defining Security Management

Topic 3A: Determine Security Management Goals

Topic 3B: Classify Information

Topic 3C: Develop a Security Program

Topic 3D: Manage Risk

### Lesson 4: Creating Applications Security

Topic 4A: Perform Software Configuration Management

Topic 4B: Implement Software Controls

Topic 4C: Secure Database Systems

### Lesson 5: Performing Cryptography

Topic 5A: Apply a Basic Cipher

Topic 5B: Select a Symmetric Key Cryptography Method

Topic 5C: Select an Asymmetric Key Cryptography Method

Topic 5D: Determine Email Security

Topic 5E: Determine Internet Security

**Lesson 6: Securing System Architecture**

- Topic 6A: Evaluate Security Models
- Topic 6B: Choose a Security Mode
- Topic 6C: Provide System Assurance

**Lesson 7: Executing Operations Security**

- Topic 7A: Control Operations Security
- Topic 7B: Audit and Monitor Systems
- Topic 7C: Handle Threats and Violations

**Lesson 8: Performing Business Continuity Planning**

- Topic 8A: Sustain Business Processes
- Topic 8B: Perform Business Impact Analysis
- Topic 8C: Define Disaster Recovery Strategies
- Topic 8D: Test the Disaster Recovery Plan

**Lesson 9: Applying Physical Security**

- Topic 9A: Control Physical Access
- Topic 9B: Monitor Physical Access
- Topic 9C: Establish Physical Security Methods
- Topic 9D: Design Secure Facilities

**Lesson 10: Applying Law, Investigations, and Ethics**

- Topic 10A: Interpret Computer Crime Laws and Regulations
- Topic 10B: Apply the Evidence Life Cycle
- Topic 10C: Perform an Investigation
- Topic 10D: Identify Codes of Conduct

**Appendix A: CISSP Certification Exam Objectives**

**Appendix B: SSCP Certification Exam Objectives**