

Certified Information Systems Security Professional (CISSP®): Fourth Edition

Course Specifications

Course Length:

5 days

Course Description

Overview:

Welcome to Certified Information Systems Security Professional (CISSP)®: Fourth Edition. 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 eight 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 a framework to prepare for CISSP certification.

CISSP is the premier certification for today's information systems security professional. It remains the premier certification because the sponsoring organization, the International Information Systems Security Certification Consortium, Inc. (ISC)2®, regularly updates the test by using subject matter experts (SMEs) to make sure the material and the questions are relevant in today's security environment. By defining eight security domains that comprise a CBK, industry standards for the information systems security professional have been established. The skills and knowledge you gain in this course will help you master the eight CISSP domains and ensure your credibility and success within the information systems security field.

Course Objectives:

In this course, you will identify and reinforce the major security subjects from the eight domains of the (ISC)2 CISSP CBK.

You will:

- 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.

Target Student:

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.

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: CyberSec First Responder (CFR), MCSE, CCNP, RHCE, LCE, SSCP®, GIAC, CISA™, or CISM®.

Course Content

Lesson 1: Security and Risk Management

Topic A: Security Governance Principles

Topic B: Compliance

Topic C: Professional Ethics

Topic D: Security Documentation

Topic E: Risk Management

Topic F: Threat Modeling

Topic G: Business Continuity Plan Fundamentals

Topic H: Acquisition Strategy and Practice

Topic I: Personnel Security Policies

Topic J: Security Awareness and Training

Lesson 2: Asset Security

Topic A: Asset Classification

Topic B: Privacy Protection

Topic C: Asset Retention

Topic D: Data Security Controls

Topic E: Secure Data Handling

Lesson 3: Security Engineering

Topic A: Security in the Engineering Lifecycle

Topic B: System Component Security

Topic C: Security Models

Topic D: Controls and Countermeasures in Enterprise Security

Topic E: Information System Security Capabilities

Topic F: Design and Architecture Vulnerability Mitigation

Topic G: Vulnerability Mitigation in Embedded, Mobile, and Web-Based Systems

Topic H: Cryptography Concepts

Topic I: Cryptography Techniques

Topic J: Site and Facility Design for Physical Security

Topic K: Physical Security Implementation in Sites and Facilities

Lesson 4: Communications and Network Security

- Topic A: Network Protocol Security
- Topic B: Network Components Security
- Topic C: Communication Channel Security
- Topic D: Network Attack Mitigation

Lesson 5: Identity and Access Management

- Topic A: Physical and Logical Access Control
- Topic B: Identification, Authentication, and Authorization
- Topic C: Identity as a Service
- Topic D: Authorization Mechanisms
- Topic E: Access Control Attack Mitigation

Lesson 6: Security Assessment and Testing

- Topic A: System Security Control Testing
- Topic B: Software Security Control Testing
- Topic C: Security Process Data Collection
- Topic D: Audits

Lesson 7: Security Operations

- Topic A: Security Operations Concepts
- Topic B: Physical Security
- Topic C: Personnel Security
- Topic D: Logging and Monitoring
- Topic E: Preventative Measures
- Topic F: Resource Provisioning and Protection
- Topic G: Patch and Vulnerability Management
- Topic H: Change Management
- Topic I: Incident Response
- Topic J: Investigations
- Topic K: Disaster Recovery Planning
- Topic L: Disaster Recovery Strategies
- Topic M: Disaster Recovery Implementation

Lesson 8: Software Development Security

Topic A: Security Principles in the System Lifecycle

Topic B: Security Principles in the Software Development Lifecycle

Topic C: Database Security in Software Development

Topic D: Security Controls in the Development Environment

Topic E: Software Security Effectiveness Assessment