

## Certified Information Systems Security Professional (CISSP)

### Overview

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 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.

This course may earn a Credly Badge.

### Prerequisite Comments

It is highly recommended that students have obtained CompTIA® Network+® or Security+® certifications, or possess equivalent professional experience upon entering CISSP training.

### Target Audience

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 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.

[Register Online](#)

### Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run"   OLL = "Online LIVE" ILT = "Instructor-Led-Training"						
07/18/22	G2R	4:00PM - 12:00AM	Athens	OLL	Call	
08/22/22	G2R	6:00PM - 2:00AM	Athens	OLL	Call	
09/19/22	G2R	4:00PM - 12:00AM	Athens	OLL	Call	
10/10/22	G2R	4:00PM - 12:00AM	Athens	OLL	Call	
11/14/22	G2R	6:00PM - 2:00AM	Athens	OLL	Call	
12/12/22	G2R	4:00PM - 12:00AM	Athens	OLL	Call	

## 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 Architecture and Engineering domain.

Analyze components of the Communication 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.

## Course Outline

---

### 1 - Security and Risk Management

Topic A: Security Concepts

Topic B: Security Governance Principles

Topic C: Compliance

Topic D: Professional Ethics

Topic E: Security Documentation

Topic F: Risk Management

Topic G: Threat Modeling

Topic H: Risk Response

Topic I: Business Continuity Plan Fundamentals

Topic J: Acquisition Strategy and Practice

Topic K: Personnel Security Policies

Topic L: Security Awareness and Training

### 2 - Asset Security

Topic A: Asset Classification

Topic B: Secure Data Handling

Topic C: Resource Provisioning and Protection

Topic D: Manage Data Lifecycle

Topic E: Asset Retention

Topic F: Data Security Control

### 3 - Security Architecture and 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 Emerging Technologies  
Topic H: Cryptography Concepts  
Topic I: Cryptography Techniques  
Topic J: Cryptanalytic Attacks  
Topic K: Site and Facility Design for Physical Security  
Topic L: Physical Security Implementation in Sites and Facilities

### 4 - Communication and Network Security

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

### 5 - Identity and Access Management

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

### 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

### 7 - Security Operations

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

## 8 - Software Development Security

Topic A: Security Principles in the System Lifecycle

Topic B: Security Principles in the Software Development Lifecycle

Topic C: Security Controls in the Development Environment

Topic D: Database Security in Software Development

Topic E: Software Security Effectiveness Assessment

---