# (ISC)² Certified Cloud Security Professional (CCSP) Exam Preparation

**Modality: Virtual Classroom**

**Duration: 5 Days**

## About this course:

ISC $^2$ certified Cloud Security Professional Exam (CCSSP) preparation course is an instructor lead, five day course. The courseware covers all the aspects of the cloud security certification exams; it includes strategies of securing data and system. Recording and detecting attacks and working alongside security agencies. It also covers the legalities and privacy protection in case of collaboration with the law enforcement agencies.

## Course Objectives:

- Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing
- Differentiate between various as-a-service delivery models and frameworks that are incorporated into the cloud computing reference architecture
- Explain strategies for protecting data at rest and data in motion
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies, and working with authorities during legal investigations
- Contrast between forensic analysis in corporate data center and cloud computing environments

## Prerequisites:

- Five years of cumulative, full-time working experience in IT (three of which must be in information security, and one of which must be in one of the six CCSP CBK domains)

## Exam Information:

- This course includes a voucher to take the CCSP exam at any Pearson VUE Test Center location

You Will Learn How To

- Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing
- Differentiate between various as-a-service delivery models and frameworks that are incorporated into the cloud computing reference architecture
- Explain strategies for protecting data at rest and data in motion
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies and working with authorities during legal investigations

- Contrast between forensic analysis in corporate data center and cloud computing environments

## Course Outline:

### Architectural Concepts and Designs Requirements

- Reviewing cloud computing concepts
- Describing cloud reference architecture
- Security concepts relevant to cloud computing
- Design principles of secure cloud computing
- Identifying trusted cloud services

### Cloud Data Security

- Understanding cloud data lifecycle
- Designing and implementing cloud data storage architectures
- Designing and applying data security strategies
- Understanding and implementing data discovery and classification technologies
- Designing and implementing relevant jurisdictional data protections for personally identifiable information

### Cloud Platform and Infrastructure Security

- Comprehending cloud infrastructure components
- Analyzing risks associated to cloud infrastructure
- Designing and planning security controls
- Planning disaster recovery and business continuity management

### Cloud Application Security

- Recognizing the need for training and awareness in application security
- Understanding cloud software assurance and validation
- Using verified secure software
- Comprehending the Software Development Life-Cycle (SDLC) process
- Applying the Secure Software Development Life-Cycle

### Operations

- Supporting the planning process for the data center design
- Implementing and building physical infrastructure for cloud environment
- Running physical infrastructure for cloud environment
- Managing physical infrastructure for cloud environment
- Building logical infrastructure for cloud environment

### Legal and Compliance

- Legal requirements and unique risks within the cloud environment

- Privacy issues, including jurisdictional variation
- The audit process, methodologies, and required adaptions for a cloud environment
- Implications of cloud to enterprise risk management
- Outsourcing and cloud contract design