

## CCSP Certification Training Course



**Certified Cloud  
Security  
Professional**

## **Overview**

Certified Cloud Security Professional (CCSP) is one of the industry's premier cloud security certifications offered for individuals and enterprise teams to manage cloud assets in a secure way. This 5-day Certified Cloud Security Professional (CCSP) certification is governed by the not-for-profit International Information Systems Security Certification Consortium (ISC)2. Check out the dates below and enrol today for the CCSP certification course.

In this continually evolving and highly competitive world of cloud, one faces unique security challenges on an almost day-to-day basis regarding unaccustomed threats to sensitive data or a less equipped internal team. The CCSP is a globally renowned certification that validates the certification holder's advanced skills and abilities to design, manage, and protect data, applications in a cloud environment while adhering to the established practices, policies, and procedures.

CCSP certification course at Certifications Master aims to provide an in-depth understanding of cloud computing concepts, cloud reference architecture, cloud computing security concepts. The participants learn to safeguard the critical data assets in a cloud environment and exhibit their competency in implementing cloud security architecture.

## **CCSP Training**

The Certified Cloud Security Professional Certification course from ISC2 is one of the most sought-after cloud-based certification courses worldwide. There is a massive transformation across industry sectors to move to cloud infrastructure to deliver around-the-clock services to customers globally. There are already several cloud-based platforms that are quite popular, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and many more. Knowing to work on these platforms is pretty much straight forward, but to secure your assets in the cloud is a different ball game altogether.

In this regard, ISC2 Certified Cloud Security Professional Certification training helps individuals and enterprise teams to learn advanced technical skills to design, manage, and secure data by creating relevant applications and infrastructure for the cloud. Participants taking part in this CCSP training will get a copy of the course material that is wholly aligned with cloud security topics from the ISC2 Common Body of Knowledge and will receive a course completion certificate from an ISC2 Official Training Provider.

## **Learning Objectives**

**Participants who take part in the Certified Cloud Security Professional (CCSP) training will learn about:**

- A holistic understanding of cloud security aspects in an organization
- Designing, managing, and securing data on cloud platforms
- Necessary skills required to become a CCSP certified professional
- Gain a thorough understanding of all the 6 domains prescribed in the ISC2 CCSP Common Body of Knowledge (CBK)
- Various as-a-service delivery models that include PaaS, SaaS, IaaS, and others to the cloud architecture
- Best practices of cloud security architecture, its design, operations, and overall service orchestration

## **Skills Measured/CCSP Examination Weights**

- Architectural Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

### **Domain 1:**

#### **Architectural Concepts and Design Requirements**

- Understanding basic cloud computing concepts
- Describing cloud reference architecture
- Understanding security concepts relevant to cloud computing
- Understanding the design principles of secure cloud computing
- Identifying trusted cloud services

## **Domain 2:** **Cloud Data Security**

- Understanding the entire 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 protection for personally identifiable information
- Designing and implementing data rights management
- Planning and implementing data retention, deletion, and archiving policies
- Designing and implementing auditability, traceability and accountability of data events .

## **Domain 3:** **Cloud Platform and Infrastructure Security**

- Understanding cloud infrastructure components
- Analysing overall risks associated to cloud infrastructure
- Designing and planning security controls
- Planning disaster recovery and business continuity management

## **Domain 4: Cloud Application Security**

- Recognizing the need for training and awareness for application security
- Understanding the cloud software assurance and validation
- Using verified secure software
- Understanding the SDLC process
- Applying the secure software development lifecycle
- Understanding the specifics of cloud application architecture
- Designing an appropriate identity and access management solutions

## **Domain 5: Operations**

- Supporting the planning of the data centre design
- Implementing and building infrastructure for the cloud environment
- Running and managing a logical infrastructure for a cloud environment
- Ensuring compliance with the latest regulations and controls
- Conducting a risk assessment to logical and physical infrastructure
- Understanding the collection, acquisition, and preservation of digital evidence
- Managing communication with relevant parties

## **Domain 6: Legal and Compliance**

- Understanding the legal requirements and unique risks within the cloud environment
- Understanding the privacy issues, including jurisdictional variation
- Understanding the audit process, methodologies, and required adaption for a cloud environment
- Understanding the implications of cloud to an enterprise through risk management
- Understanding about outsourcing and cloud contract design
- Executing vendor management