# CCSP: Certified Cloud Security Professional

Course Code: CCSP
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

## OVERVIEW

**Attackers never rest,** and along with all the traditional threats targeting internal networks and systems, **an entirely new variety specifically targeting the cloud has emerged**.

As more organisations adopt cloud-based systems, new complexities and challenges surface and the risks increase. Organisations need cloud security professionals with the requisite knowledge, skills and abilities to be able to audit, assess and secure cloud infrastructures.

To address this need, (ISC)² and the Cloud Security Alliance (CSA) have developed the Certified Cloud Security Professional (CCSP) certification. This credential reflects in-depth knowledge derived from hands-on information security and cloud computing experience. It validates practical know-how for professionals whose responsibilities involve cloud security architecture, design, operations and service orchestration.

In this 5-day course you will Gain a thorough understanding of the information security risks and mitigation strategies critical to data security in the cloud in this (ISC)² Certified Cloud Security Professional (CCSP) Exam Preparation course. This course covers the six domains of the Official (ISC)² CCSP Common Body of Knowledge (CBK®) and prepares you to take the CCSP exam to become a Certified Cloud Security Professional.

## SKILLS COVERED

- Identify and explain the Cloud Computing concepts and definitions based on the ISO/IEC 17788 and NIST standards.
- Identify and explain the Cloud Security Alliance's Notorious Nine, Treacherous Twelve and Egregious Eleven.
- Understand, and be able to differentiate between, the various service delivery models, frameworks and hypervisor threats that are incorporated into the cloud computing reference architecture.
- Demonstrate the application of appropriate security strategies and be able to recommend appropriate controls for protecting data at rest, data in use and data in motion.
- Discuss strategies for data ownership, data sovereignty, data classification and implementing appropriate measures for assurance for ensuring privacy, compliance with regulatory agencies and working with authorities during legal investigations.
- Understand the challenges for data centre design, forensic analysis and cloud environment deployments and recommend appropriate risk mitigation strategies.
- Understand and apply Business Continuity Planning and Disaster Recovery procedures for disaster situations.
- Design appropriate identity and access management solutions.
- Comprehend and apply appropriate processes and frameworks including the Software Development Life-Cycle (SDLC) process and secure operations.

**WHO SHOULD ATTEND?**

The course is designed for:

- Enterprise architects
- Security administrators
- Systems engineers
- Security architects
- Security consultants
- Security engineers
- Security managers
- Systems architects

**PREREQUISITES**

The course assumes you have an at least reasonable level of varied IT experience.

Candidates who wish to sit the exam must have at least five years of cumulative, paid full-time working experience in Information Technology. Three of these must be in information security, and one of which must be in one of the six CCSP domains.

Candidates who are already (ISC)2 members in good standing and who possess a Certified Information Systems Security Professional (CISSP) certificate may substitute all of the CCSP experience requirements on this basis.

CCSP candidates who have passed the Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK) may count this certification towards one year of experience in one of the six domains.

**MODULES**

**Module 1: Cloud Concepts, Architecture and Design**

- Understand cloud computing concepts
- Describe cloud reference architecture
- Understand security concepts relevant to cloud computing
- Understand security design principles of cloud computing
- Evaluate cloud service providers

**Module 2: Cloud Data Security**

- Describe cloud data concepts
- Design and implement cloud data storage architectures
- Design and apply data security technologies and strategies
- Implement data discovery
- Implement data classification
- Design and implement Information Rights Management
- Design and implement of data retention, deletion and archiving policies
- Design and implement auditability, traceability and accountability of data events

**Module 3: Cloud Platform and Infrastructure Security**

- Comprehend cloud infrastructure components
- Design a secure data centre
- Analyse risks associated with cloud infrastructure
- Design and plan security controls
- Plan disaster recovery and business continuity

**Module 4: Cloud Application Security**

- Advocate training and awareness for application security
- Describe the secure software development life cycle process
- Apply the secure software development life cycle

- Apply cloud software assurance and validation
- Use verified secure software
- Comprehend the specifics of cloud application architecture
- Design appropriate Identity and Access Management solutions

**Module 5: Cloud Security Operations**

- Implement and build physical and logical infrastructure for cloud environments
- Operate physical and logical infrastructure for cloud environments
- Manage physical and logical infrastructure for cloud environments
- Implement operational controls and standards
- Support digital forensics
- Manage communication with relevant parties
- Manage security operations

**Module 6: Legal and Compliance**

- Articulate legal requirements and unique risks within the cloud environment
- Understand privacy issues
- Understand audit process, methodologies, and required adaptations
- Understand implications of cloud to enterprise risk management
- Understand outsourcing and cloud contract design

**Module 7: Exam**

- CCSP Official Practice Questions
- CCSP Workbook Review

**END OF PAGE**