Certified Cloud Security Professional (CCSP) Course Outline

About CCSP

(ISC)² developed the Certified Cloud Security Professional (CCSP) credential to ensure that cloud security professionals have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks. A CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge.

The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of cloud security. Successful candidates are competent in the following six domains:

- Cloud Concepts, Architecture and Design
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Cloud Security Operations
- Legal, Risk and Compliance

Experience Requirements

Candidates must have a minimum of five years cumulative paid work experience in information technology, of which three years must be in information security and one year in one or more of the six domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for one year of experience in one or more of the six domains of the CCSP CBK. Earning (ISC)²'s CISSP credential can be substituted for the entire CCSP experience requirement.

A candidate that doesn't have the required experience to become a CCSP may become an Associate of (ISC)² by successfully passing the CCSP examination. The Associate of (ISC)² will then have six years to earn the five years required experience. You can learn more about CCSP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CCSP/experience-requirements.

Accreditation

CCSP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CCSP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CCSP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals focusing on cloud technologies.

CCSP Examination Information

Length of exam	4 hours
Number of items	150
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Chinese, German, Korean, Japanese, Spanish
Testing center	Pearson VUE Testing Center

CCSP Examination Weights

Domains	Weight
1. Cloud Concepts,	17%
2. Cloud Data Security	20%
3. Cloud Platform and	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and	13%
Total:	100%

CCSP Course Resources Domain Wise:

Domain 1:

Cloud Concepts, Architecture, and Design:

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

Domain 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
- Plan and implement data retention, deletion, and archiving policies
- Design and implement auditability, traceability, and accountability of data events

Domain 3:

Cloud Platform and Infrastructure Security:

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

Domain 4:

Cloud Application Security

- Advocate training and awareness for application security
- Describe the secure software development lifecycle process
- Apply the secure software development lifecycle
- Apply cloud software assurance and validation
- Use verified secure software
- Comprehend the specifics of cloud application architecture
- Design appropriate identity and access management solutions

Domain 5:

Cloud Security Operations

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

Domain 6:

Legal, Risk, and Compliance

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