(ISC)² established the Certified Cloud Security Professional (CCSP) credential to offer a way for cloud security professionals to display mastery of the necessary knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks. This professional competency is compared to a globally recognized CCSP Common Body of Knowledge (CBK) to ensure relevancy across all disciplines in the field of cloud security.

Successful candidates will be competent in the following 6 domains:

- Cloud Concepts, Architecture and Design (17%)
- Cloud Data Security (19%)
- Cloud Platform & Infrastructure Security (17%)
- Cloud Application Security (17%)
- Cloud Security Operations (17%)
- Legal, Risk and Compliance (13%)

CCSP exam candidates must have a minimum of 5 years cumulative paid work experience in information technology, of which 3 years must be in information security and 1 year in 1 or more of the 6 domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for 1 year of experience in 1 or more of the 6 domains of the CCSP CBK. Earning (ISC)²'s CISSP credential can be substituted for the entire CCSP experience requirement.

This course is a live highly accelerated 3-day, 4 hour per day exam cram to help candidates who are within a few weeks of taking the exam to gain a high degree of confidence that they will be successful on their first attempt. The course is taught by Michael J. Shannon, a senior technical instructor at Skillsoft.

These are the topics covered over the 3-day live course:

Topic 1: Cloud System Architecture Design

- Cloud Computing Definitions
- Cloud Computing Participants
- Cloud Computing Characteristics
- Cloud Computing Infrastructure
- Cloud Computing Activities
- Cloud Computing Service Capabilities
- Cloud Deployment Categories and Models
- Cloud Shared Responsibility
- Impact of Related Technologies
- Business Requirements
- Contract and Vendor Management and Assessment
- Supply Chain Management

Topic 2: Secure Cloud Computing

- Information Management Controls
- Cryptography and Cloud Computing
- Asset Access Control
- Asset Removal and Storage Media Sanitization

- Cloud Network Security
- Jump Boxes
- Cloud Packet Capturing
- Cloud Firewalls
- Security in the Virtualized Environment
- Infrastructure and Data Threats
- Platform-specific Security
- Cloud Secure Data Life Cycle
- Cloud Service Continuity
- Cloud Functional Security
- Cloud Service Certification Assessment

Topic 3: Data Security Technologies

- Data Asset Security and Associated Technologies
- Storage Types
- Data Owner vs. Data Custodian
- Storage Type Threat
- Encryption of Data Assets
- Key Management
- Hashing
- Data Masking
- Data Tokenization
- Data Loss Prevention

Topic 4: Implementing Data Discovery and Classification

- Information Rights Management
- Data Discovery
- Data Discovery Challenges
- Data Classification
- Public Key Infrastructure
- PowerShell Certificate Generation
- Cloud Certificate Generation
- VPNs and the Cloud
- Configuring a Cloud VPN
- Custom Cloud Storage Encryption Keys

Topic 5: Data Retention and Events

- Data Retention Policies
- Data Deletion
- Data Archiving
- Legal Hold
- eDiscovery

- Event Sources and Attributes
- Data Events
- SIEM

Topic 6: Cloud Infrastructure Architecture

- Physical Architecture
- Network and Communications Service
- Deploy a Cloud Virtual Network
- Compute Service
- Deploy a Cloud Virtual Machine
- Storage Service
- Deploy Cloud Storage
- Cloud Management GUI Tools
- Cloud Management Using Command Line Tools
- Logical Design

Topic 7: Data Center Security

- Cloud Computing Risk
- Risk Frameworks
- Threat and Attack
- Security Controls
- Cloud Storage Security
- Cloud Network Protection
- Virtual Machine Management
- Authentication and Authorization
- Auditing
- Types of Audit Reports
- Virtual Machine High Availability
- Failover Testing
- Cloud Virtual Machine Grouping
- Cloud Application Load Balancing

Topic 8: Application Development and Security

- Training and Awareness
- Cloud Security and the SDLC
- Data Privacy Standards
- Web Applications and OWASP
- Containerized Applications
- Cloud Web Application Security
- Cloud Web Applications
- Cloud Web Application Scaling
- Web Application SSL/TLS

- Cloud APIs and Third-Party Software
- Cloud Functions
- Security Testing Methodologies
- Web Application Deployment Slots
- Threat Modeling and QoS

Topic 9: Identity and Access Management

- Identity and Access Management
- Identity Providers
- Microsoft Azure User Accounts
- Amazon Web Services User Accounts
- Single Sign-on
- Microsoft Azure AD Connect
- Amazon Web Services User Policies
- Multi-factor Authentication
- Enable Cloud MFA
- Cloud MFA User Sign-in

Topic 10: Cloud Infrastructure Management

- Hardware Specific Security
- Virtualization Template Deployment
- Guest Operating System Virtualization Toolsets
- Network Configuration
- Network Security Management
- Host Management
- Operating System Hardening
- Availability of Guest Operating System
- RDP Remote Access
- SSH Remote Access
- Performance Monitoring
- Performance Metric Alerts
- On-Premises File Server to Cloud Backup
- Virtual Machine Backup

Topic 11: Operational Controls and Standards

- Change Management
- Continuity Management
- Information Security and Vulnerability Management
- Configuration Management
- Service Level Agreements
- Digital Forensics and the Cloud
- Digital Forensics Hardware

- Digital Forensics Software
- Chain of Custody
- Examination and Analysis