Document Generated: 05/13/2026

Learning Style: On Demand

Technology: ISC2

Difficulty: Advanced

Course Duration: 24 Weeks

Certified Cloud Security Professional Self-paced (CCSP)

About This Course:

Certified Cloud Security Professional (CCSP) training leverages the power of artificial intelligence, guiding students through a self-paced learning experience adapted to their unique needs. It covers the advanced technical skills and

knowledge for designing, managing and securing data, applications, and infrastructure in the cloud.

Course Objectives:

- Describe the cloud reference architecture.

- Indicate the design principles of secure cloud computing.

- Implement the cloud data security.

- Apply the cloud platform and infrastructure security.

- Practice the cloud application security.

- Construct the cloud security operations.

- Prepare to meet legal, risk, and compliance requirements.

Audience:

- Cloud Security Engineers

- Security Architects

- Cloud Architects

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)

Course Outline:

Domain 1.Cloud Concepts, Architecture and Design

- Cloud computing concepts and characteristics (on-demand self-service, elasticity, multi-tenancy)

- Cloud service models:

- IaaS (Infrastructure as a Service)

- PaaS (Platform as a Service)

- SaaS (Software as a Service)

- Cloud deployment models:

    - Public cloud

    - Private cloud

    - Hybrid cloud

    - Multi-cloud

- Shared Responsibility Model

- Cloud reference architectures

- Secure cloud design principles

- Business requirements and risk management

- Cloud migration strategies

Domain 2. Cloud Data Security

- Data lifecycle management

- Data classification and ownership

- Encryption methods

- Key management systems

- Tokenization and masking

- Data Loss Prevention (DLP)

- Secure data deletion

- Privacy protection

- Data discovery and governance

Domain 3. Cloud Platform & Infrastructure

- Cloud infrastructure components

- Virtualization security

- Container and serverless security

- Network security in the cloud

- Identity and Access Management (IAM)

- Secure configuration of cloud resources

- Infrastructure hardening

- Microservices security

- Zero Trust architecture

Domain 4. Cloud Application Security

- Secure software development lifecycle (SSDLC)

- DevSecOps practices

- Application vulnerabilities

- API security

- Secure coding practices

- Application testing methods

- Identity federation

- Application authentication and authorization

Domain 5. Cloud Security Operations

- Cloud monitoring and logging

- Incident response in cloud

- Disaster recovery and business continuity

https://www.quickstart.com/catalog/product/view/id/10777/s/certified-cloud-security-professional-self-paced-ccsp/

- Backup and restore strategies

- Security automation

- Patch management

- Vulnerability management

- Security orchestration

Domain 6. Legal, Risk and Compliance

- Data protection laws and regulations

- Privacy regulations (GDPR etc.)

- Risk management frameworks

- Compliance audits

- Contract and vendor management

- Service Level Agreements (SLAs)

- Cross-border data transfer regulations

- E-discovery and legal hold