

# (ISC)<sup>2</sup> CCSP – Certified Cloud Security Professional

This CCSP training covers how to effectively secure cloud data security, data infrastructure and and applications security. This intermediate ISC2 CCSP training prepares learners to take the CCSP exam, which is the one required exam to earn the ISC2 Certified Cloud Security Professional (CCSP) certification.

[CBT Nuggets course material](#) →

## WEEK 1

### Cloud Concepts and Architecture

- Cloud Computing Roles
- Cloud Computing Characteristics
- Cloud Deployment Models
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Shared Responsibility
- Impact From Emerging Technologies

### Security Concepts and the Cloud

- Overview
- Cryptography and Key Management
- Access Control with IAM
- Data and Media Sanitization
- Network and Virtualization Security
- Common Threats in the Cloud

### Secure Cloud Computing Design Principles

- Overview
- Cloud Secure Data Lifecycle
- Data Governance
- Cloud Based DR and BC

## WEEK 2

- Cost Benefit Analysis
- Functional Requirements
- Security Considerations for Different Cloud Categories

## **Evaluating Cloud Service Providers**

Overview

Evaluating Cloud Service Providers

ISO/IEC 27017

PCI-DSS

ENISA

CSA STAR

Additional Standards

## **Cloud Data Concepts and Storage Architecture**

Overview

Cloud Data Lifecycle

Data Functions

Data Dispersion

Cloud Storage Types

Threats to Storage

## **Data Security Technologies**

Overview

The Encryption Process and the Cloud

IaaS Data Encryption Options

## **WEEK 3**

Key Management

Data Hashing

Data Obfuscation and Anonymization

Data Loss Prevention (DLP)

## **Data Discovery, Classification and IRM**

Overview

Data Discovery

Data Discovery Techniques and Issues

Data Classification

Information Rights Management (IRM)

Data Retention and Deletion

Data Archival

Logs and Auditability

Log Storage

Chain of Custody and Non-Repudiation

## **Cloud Infrastructure Components**

Overview

Intro

Physical Environment

Networking and Communications

Compute and Storage

Virtualization

Management Plane

## **WEEK 4**

## **Secure Datacenter Design**

Overview

Intro

Datacenter Services

Datacenter Security

Physical Design

Temperature and Humidity

The Importance of Airflow

Multi-Vendor Pathway Connectivity

## **Cloud Infrastructure Risk and Security**

Overview

Risk Assessments

Cloud Infrastructure Risk and Security

Cloud Specific Risks

Virtualization Risks

Countermeasure Strategies

Physical and Environmental Protection

System and Communication Protection

## **Protecting Virtualized Systems and BCDR**

Overview

Protecting Virtualized Systems

Identification, Authentication and Authorization

Audit Mechanisms

Risks Related to the Cloud and BCDR

## **WEEK 5**

Business Requirements for BCDR

BCDR Strategy and Planning

BCDR Testing

## **Secure SDLC Process and Application**

Overview

Business Requirements

Phases of the SDLC

Development Methodologies

Cloud Specific Risks

Threat Modeling

Secure Coding Techniques

## **Application Security and Software Assurance**

Overview

Intro

Common Cloud Application Vulnerabilities

Cloud Development Basics

Functional and Non-Functional Testing

Security Testing Methodologies

Quality Assurance

Abuse Case Testing

## **Cloud Application Architecture and IAM**

Overview

Supplemental Security Components

Cryptography and Applications

## **WEEK 6**

Application Virtualization and Orchestration

Federated Identity, MFA, OTP and SSO

CASB and Secrets Management

## **Implement Cloud Infrastructure**

Overview

Hardware Specific Security Configurations

Security Configurations  
Virtualization Toolset  
Controlling Access  
Securing the Network  
Operating System Security  
Stand Alone Hosts in the Cloud

### **Managing Cloud Infrastructure**

Managing It All  
Backups and Availability  
Operational Controls and Standards  
Supporting Digital Forensics  
Managing Communications  
Managing Security Operations

### **Legal, Risk and Privacy in the Cloud**

Overview  
Intro to Legal, Risk and Privacy in the Cloud  
Legal Requirements and Unique Risks in the Cloud  
Legal Frameworks and Guidelines

E-Discovery and Forensic Requirements  
Contractual vs Regulated Private Data  
Country-Specific Legislation of Data Privacy  
Privacy Standards and PIAs  
Skill Review

### **Auditing in the Cloud**

Overview  
Intro  
Audit Controls and Assurance  
Audit Reports  
Gap Analysis and Audit Planning  
ISMS and ISCS  
Policies  
Identification and Involvement of Relevant Stakeholders  
Specialized Compliance Requirements  
Impact of a Distributed IT Model

### **Risk Management and Cloud Contract Design**

Overview  
Assessing Risk Management and Data Roles  
Regulatory Transparency and Risk Treatment  
Risk Frameworks, Metrics and Environments  
Business Requirements and Vendor Management  
Contract Management  
Supply Chain Management

## **WEEK 7**