

# CCSP - Certified Cloud Security Professional

## Course Description & Overview

Managing and utilizing cloud computing introduces new security challenges that cannot be addressed with traditional information security approaches. Secure clouds cannot exist without the right cloud security expertise. As a result, organizations are seeking competent, experienced professionals who know how to secure cloud computing environments and services. The CCSP credential helps employers ensure they have the right expertise by providing a new benchmark for knowledge, skills, and experience that is viewed as the most reliable indicator of overall competency in cloud security.

SecureNinja's 5-day Certified Cloud Security Professional (CCSP) training and certification boot camp 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.

### CCSP CBK

Our 5-day program covers the six (6) domains of CCSP

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

### Course Completion

After completing this workshop, participants will be able to:

- Describe the building blocks necessary to develop cloud-based systems, including concepts concerning customer, provider, partner, measured services, scalability, virtualization, storage, and networking. Students will also be able to understand the cloud reference architecture based on activities defined by industry-standard documents.
- Identify the types of controls necessary to administer various levels of confidentiality, integrity, and availability, concerning securing data in the cloud. You will gain knowledge on topics of data discovery and classification techniques, digital rights management, privacy of data, data retention, deletion, and archiving, data event logging, chain of custody and non-repudiation, and the strategic use of security information and event management.
- Identify the virtual and physical components of the cloud infrastructure concerning risk management analysis, including tools and techniques necessary for maintaining secure cloud infrastructure. In addition to risk analysis, you will gain an understanding of how to prepare and maintain business continuity and disaster recovery plans, including techniques and concepts for identifying critical systems

and lost data recovery.

- Demonstrate an understanding of the Software Development Life Cycle, you will gain an understanding in cloud software assurance and validation, utilizing secure software, and the controls necessary for developing secure cloud environments with regard to program interfaces, cloud application architecture, and how to ensure data and application integrity, confidentiality, and availability through identity and access management solutions.
- Demonstrate an ability to develop, plan, implement, run, and manage the physical and logical cloud infrastructure through an understanding of the necessary controls and resources, best practices in monitoring and auditing, and the importance of risk assessment in both the physical and logical cloud infrastructures.
- Identify privacy issues and audit processes utilized within a cloud environment, including, auditing controls, assurance issues, and the specific reporting attributes. Topics covered include, ethical behavior and required compliance within regulatory frameworks, which includes investigative techniques for crime analysis and evidence gathering methods.

## CCSP Benefits

### How CCSP Certification Helps the Professional

- Demonstrate not just cloud knowledge but competence gained through hands-on experience in addressing the unique information security demands intrinsic to cloud environments
- Enhance your credibility and marketability for the most desirable cloud security opportunities; bolster your standing and provide a career differentiator
- Affirm your commitment to understanding and applying security best practices to cloud environments – today and in the future
- As a member of (ISC)<sup>2</sup>, gain access to valuable career resources, such as networking and ideas exchange with peers

### How CCSP Certification Helps Organizations

- Secure and optimize the organization's use of cloud computing infrastructure and services with qualified professionals who have demonstrated their cloud security competence
- Ensure the organization is applying the proper cloud security controls not only internally but also with third parties by reinforcing risk and legal requirements through cloud contract and SLAs with cloud service providers
- Know that with the two leading stewards of information and cloud security knowledge – (ISC)<sup>2</sup> and CSA – responsible for CCSP, organizations can be confident it reflects the most current required best practices and competency
- Increase organizational integrity in the eyes of clients and other stakeholders
- Ensure work teams stay current on evolving cloud technologies, threats, and mitigation strategies by meeting the continuing professional education requirements

## Course Outline

### 1. Architectural Concepts and Designs Requirements

- a. Understanding cloud computing concepts
- b. Describing cloud reference architecture
- c. Security concepts relevant to cloud computing
- d. Design principles of secure cloud computing
- e. Identifying trusted cloud services
- f. Design and apply data security strategies

## **2. Cloud Data Security**

- a. Understanding cloud data lifecycle
- b. Designing and implementing cloud data storage architectures
- c. Designing and applying data security strategies
- d. Understanding and implementing data discovery and classification technologies
- e. Designing and implementing relevant jurisdictional data protections for personally identifiable information

## **3. Cloud Platform and Infrastructure Security**

- a. Comprehending cloud infrastructure components
- b. Analyzing risks associated to cloud infrastructure
- c. Designing and planning security controls
- d. Planning disaster recovery and business continuity management

## **4. Cloud Application Security**

- a. Recognizing the need for training and awareness in application security
- b. Understanding cloud software assurance and validation
- c. Using verified secure software
- d. Comprehending the Software Development Life-Cycle (SDLC) process
- e. Applying the Secure Software Development Life-Cycle

## **5. Operations**

- a. Supporting the planning process for the data center design

- b. Implementing and building physical infrastructure for cloud environment
- c. Running physical infrastructure for cloud environment
- d. Managing physical infrastructure for cloud environment
- e. Building logical infrastructure for cloud environment

## **6. Legal and Compliance**

- a. Legal requirements and unique risks within the cloud environment
- b. Privacy issues, including jurisdictional variation
- c. The audit process, methodologies, and required adaptations for a cloud environment
- d. Implications of cloud to enterprise risk management
- e. Outsourcing and cloud contract design

## **Who Should Attend**

CCSP is most appropriate for those whose day-to-day responsibilities involve procuring, securing, and managing cloud environments or purchased cloud services.

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

## **Prerequisites**

To attain CCSP, applicants must have a minimum of five years of cumulative, paid, full-time working experience in information technology, of which three years must be in information security and one year in one of the six CBK domains:

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

## **Required Exam**

ISC2 CCSP Exam

- Format: 125 multiple-choice questions.
- Duration: 3 hours.
- Passing Score: 700 out of 1000 points.

### **Course Length**

- 5 Days
- 40 hours

### **Follow-on Courses**

CISSP