(ISC)^2 CCSP– Certified Cloud Security Professional

What is CCSP?

The Certified Cloud Security Professional (CCSP) training program and CCSP certification were created for both professionals and organizations who are interested in validating their cloud security capabilities. More specifically, the CCSP training program will prove you have the knowledge and hands-on experience with cloud security architecture, design, operations and service orchestration

LearnersOne's five-day CCSP training course will help you develop the necessary knowledge and skills to face new cloud computing threats and challenges. It will also help you prepare for the CCSP certification exam offered by (ISC)^2. Students review all six of the CCSP domains and gain a wealth of current information on the (ISC)^2 Common Body of Knowledge (CBK) for the CCSP exam.

LearnersOne
Learning is a Safari

Course Breakdown

Domain 1	Cloud Architectural Concepts and Design Requirements
Domain 2	Cloud Data Security
Domain 3	Cloud Platform Infrastructure Security
Domain 4	Cloud Application Security
Domain 5	Cloud Security Operations
Domain 6	Legal and Compliance for the Cloud
Domain 7	Software Development Security

https://learnersone.com
(240) 930-4053

Table of **Contents:**

Program **Overview:**

This Certified Cloud Security Professional (CCSP) training course is the leading certification by the International Information System Security Certification Consortium, or (ISC)₂. This course will enable you to negate security threats to your cloud storage by understanding information security risks and implementing strategies to maintain data security.

Program **Features:**

- 36 hours for Live Onsite/Virtual Classes
- 6 hours of Online Self Learning content
- Lifetime access to self-paced learning
- Industry-recognized course completion certificate
- 7 real-world case studies

Delivery **Mode:**

Onsite/Online self-learning and live virtual classes

Prerequisites**:**

To obtain the CCSP certification course, you must have:

- At least five years of working experience in IT, including three years of information security and one year of cloud security experience
- Those without the required experience can take the exam to become an Associate of (ISC)₂while working toward the experience needed for full certification

Target **Audience:**

The CCSP certification course is ideal for anyone wishing to learn and explore career opportunities in IT network security and cloud computing. This course also is ideal for enterprise architects, security administrators, systems engineers, security architects, security consultants, security engineers, security managers, and system architects.

Key Learning **Outcomes:**

Upon completion of this CCSP course, you will understand:

- Fundamental cloud concepts, architecture, and design
- Cloud data security concepts such as data lifecycle and storage architectures
- The design principles of secure cloud computing
- How to plan for disaster recovery and business continuity
- The process of configuring VM tools
- How to perform risk analysis, mitigation, and management
- The theory and practice of legal risk and cloud compliance

Certification Details and **Criteria:**

- Complete 85% of the self-paced learning
- Pass the course-end assessment with a score of 70% or above

Course **Curriculum:**

Lesson 01 - Cloud Concepts, Architecture, and Design

- Domain and Learning Objectives
- Security Concepts
- Key Security Concepts, Defense in Depth, Due Care, and Due Diligence
- Security Controls and Functionalities
- Cloud Computing Concepts
- Business Drivers
- Scalability, Elasticity, Vendor Lock-in, and Vendor Lock-out
- Cloud Computing Concepts: Advantages
- Cloud Reference Architecture
- Cloud Computing Roles and Actors
- Cloud Service Categories: Infrastructure as a Service (IaaS)
- Cloud Service Categories: Platform as a Service (PaaS)
- Cloud Service Categories: Software as a Service (SaaS)
- Cloud Service Categories: Management
- Cloud Deployment Models: Public Cloud
- Cloud Deployment Models: Private Cloud
- Cloud Deployment Models: Hybrid Cloud
- Cloud Deployment Models: Community Cloud
- Models and Characteristics
- Comparison of Cloud Deployment Models
- Case Study: Hybrid Cloud
- Cloud Technology Roadmap
- Impact of Related Technologies
- Cryptography, Key Management, and Other Security Concepts
- Key Management
- IAM and Access Control
- Data Remanence
- Virtualization
- Cloud Computing Threats
- Design Principles of Secure Cloud Computing
- Cost-Benefit Analysis
- Evaluate Cloud Service Providers
- SOC
- IT Security Evaluation
- FIPS
- Scenario
- Key Takeaways

Lesson 02 - Cloud Data Security

- Domain and Learning Objectives
- Cloud Data Life Cycle
- Cloud Data Life Cycle: Create, Store, Use, and Share
- Real-World Scenario
- Cloud Data Life Cycle: Archive
- Cloud Data Life Cycle: Destroy, Key Data Functions
- Cloud Data Storage Architectures
- Cloud Data Storage Architectures: Storage Types for IaaS
- Cloud Data Storage Architectures: Storage Types for PaaS
- Cloud Data Storage Architectures: Storage Types for SaaS
- Cloud Data Storage Architectures: Threats to Storage Types
- Real-World Scenario
- Data Security Strategies
- Data Security Strategies: Encryption (Use Cases)
- Data Security Strategies: Encryption Challenges
- Data Security Strategies: Encryption in IaaS
- Data Security Strategies: Database Encryption
- Data Security Strategies: Key Management
- Data Security Strategies: Key Storage in the Cloud
- Data Security Strategies: Masking
- Data Security Strategies: Data Anonymization
- Data Security Strategies: Tokenization
- Data Security Strategies: Homomorphic Encryption and Bit Splitting Real-
- World Scenario
- Data Security Strategies: Data Loss Prevention
- Scenario
- Data Discovery and Classification Technology
- Data Discovery and Classification Technology: Data Classification
- Data Discovery and Classification Technology: Challenges with Cloud Data
- Jurisdictional Data Protections for Personally Identifiable Information (PII) Privacy
- Acts: GDPR
- Privacy Acts: Data Protection policies
- Privacy Acts: United States
- Privacy Acts: HIPAA, FISMA, and SOX
- Jurisdictional Data Protections for PII: Responsibilities of Cloud Services Data
- Rights Management
- Data Retention, Deletion, and Archiving Policies
- Data Retention
- Data Deletion
- Real-World Scenario
- Data Archiving
- Real-World Scenario
- Legal Hold

- Auditability, Traceability, and Accountability of Data Events
- SIEM
- Chain of Custody
- Nonrepudiation
- Real-World Scenario
- Key Takeaways

Lesson 03 - Cloud Platform and Infrastructure Security

- Domain and Learning objectives
- Cloud Infrastructure Components
- Network and Communications
- Management Plane and Virtualization
- Factors That Impact Datacenter Design
- Physical Design: Buy or Build
- Physical Design: Data Center Design Standards
- Physical Design: Uptime Institute
- Physical Design: Tiers
- Physical Design: Features of Tiers
- Real-World Scenario
- Environmental Design Considerations
- Connectivity
- Hypervisor and Resource Allocation
- Risks Associated with Cloud Infrastructure
- Policy, General, and Virtualization Risks
- Cloud-Specific, Legal, and Non-Cloud Specific Risks
- Cloud Attack Vectors and Compensating Controls
- Business Scenario
- Design and Plan Security Controls
- Real-World Scenario
- Plan Disaster Recovery and Business Continuity
- DReal-World Scenario
- RBCDR Planning Factors and Disruptive Events
- Characteristics of Cloud Infrastructure
- BCDR Strategies and Returning to Normal
- Real-World Scenario
- BCDR Creation
- BCDR Creation: Test
- Business Requirements
- BCDR Creation: Report and Revise
- Testing Types, Uptime, Availability, Activity, and Case Study
- Security Training and Awareness
- Real-World Scenario
- Key Takeaways

Lesson 04 - Cloud Application Security

- Domain and Learning objectives
- Advocate Training and Awareness for Application Security
- Real-World Scenario
- Common Pitfalls
- Encryption Dependency Awareness
- Business Scenario
- Understanding Software Development Lifecycle Process
- Real-World Scenario
- Vulnerabilities and Risks
- Threat Modeling
- Real-World Scenario
- Encryption
- Sandboxing and Application Virtualization
- Federated Identity Management
- SAML Authentication
- Identity and Access Management
- Multi-Factor Authentication
- Real-World Scenario
- Cloud Access Security Broker
- Application Security Testing
- Software Supply Chain Management
- Real-World Scenario
- Key Takeaways

Lesson 05 - Cloud Security Operations

- Domain and Learning objectives
- Secure Configuration of Hardware: Servers
- Secure Configuration of Hardware: Storage Controllers (Part 1)
- Real-World Scenario
- Secure Configuration of Hardware: Storage Controllers (Part 2)
- Secure Configuration of Hardware: Virtual Switches
- Configuration of VM Tools
- Configuration of VM Tools: Running a Physical Infrastructure (Part 1)
- Configuration of VM Tools: Running a Physical Infrastructure (Part 2)
- Configuration of VM Tools: Running a Physical Infrastructure (Part 3)
- Configuration of VM Tools: Running a Physical Infrastructure (Part 4)
- Real-World Scenario
- Securing Network Configuration (Part 1)
- Real-World Scenario
- Clustered Hosts
- Dynamic Optimization and Clustered Storage
- Maintenance Mode and Patch Management
- Performance Monitoring
- Real-World Scenario
- Network Security Controls: Layered Security and Honeypots
- Network Security Controls: SIEM
- Log Management
- Orchestration
- Availability of Guest OS
- Operations Management (Part 1)
- Real-World Scenario
- Operations Management (Part 2)
- Risk-Management Process: Framing Risk and Risk Assessment
- Quantitative Risk Analysis
- Scenario
- Risk Response and Risk Monitoring
- Collection and Preservation of Digital Evidence
- Communication with Relevant Parties
- Real-World Scenario
- Security Operations Center
- Key Takeaways

Lesson 06 - Legal Risk and Compliance

- Domain and Learning objectives
- Case Study
- Legislative Concepts
- Intellectual Property Laws
- Case Study
- Scenario
- Acts and Agreements
- Case Study
- NERC
- Privacy Shield and Generally Accepted Privacy Principles (GAPP)
- Jurisdictional Difference in Data Privacy
- Terminologies and eDiscovery
- Forensic Requirements and PII
- Gap Analysis, SOC Reports, and Chain of Custody Vendor
- Management
- Cloud Computing Policies and Risk Attitude
- SLA
- Quality of Service
- Risk Mitigation
- Risk Management Metrics and ISO 28000:2007
- Real-World Scenario
- Key Takeaways

About **Us**:

Trusted by hundreds of satisfied students and organizations, we are a top-notch educator providing the most complete training complete training programs to help you stay informed, engaged and a step ahead.