Certified Cloud Security Professional (CCSP)

Price	Duration	Delivery Methods
$4,549.00	5 Days	VILT, Private Group

The goal of the course is to prepare professionals for the challenging CCSP exam by covering the objectives of the exam based on the six domains as defined in the (ISC)2 CCSP common body of knowledge.

Who Should Attend

The CCSP is ideal for IT and information security leaders responsible for applying best practices to cloud security architecture, design, operations and service orchestration.

Course Objectives

Upon completing this course, the participants will gain valuable knowledge and skills including the ability to:

- Successfully pass the CCSP exam.
- Understand the fundamentals of the cloud computing architecture framework.
- Understand security challenges associated with different types of cloud services.
- Identify and evaluate security risks for their organization's cloud environments.
- Select and implement appropriate controls to ensure secure implementation of cloud services.
- Thoroughly understand the 6 essential core domains of the CCSP common body of knowledge: 1. Architectural Concepts & Design Requirements 2. Cloud Data Security 3. Cloud Platform & Infrastructure Security 4. Cloud Application Security 5. Operations 6. Legal & Compliance

Agenda

1 - ARCHITECTURAL CONCEPTS AND DESIGN REQUIREMENTS

- Cloud Computing Concepts
- Cloud Reference Architecture
- Cloud Computing Security Concepts
- Design Principles of Secure Cloud Computing
- Trusted Cloud Services

2 - CLOUD DATA SECURITY

- CSA (Cloud Security Alliance) Cloud Data Lifecycle
- Cloud Data Storage Architectures
- Data Security Strategies
- Data Discovery and Classification Technologies
- Protecting Privacy and PII (Personally Identifiable Information)
- Data Rights Management
- Data Retention, Deletion, and Archiving Policies
- Auditability, Traceability, and Accountability of Data Events

3 - CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

- Cloud Infrastructure Components
- Cloud Infrastructure Risks
- Designing and Planning Security Controls
- Disaster Recovery and Business Continuity Management

4 - CLOUD APPLICATION SECURITY

- The Need for Security Awareness and Training in application Security
- Cloud Software Assurance and Validation
- Verified Secure Software
- SDLC (Software Development Life Cycle) Process
- Secure SDLC
- Specifics of Cloud Application Architecture
- Secure IAM (Identity and Access Management) Solutions

5 - OPERATIONS

- Planning Process for the Data Center Design
- Installation and Configuration of Physical Infrastructure for Cloud Environment
- Running Physical Infrastructure for Cloud Environment
- Managing Physical Infrastructure for Cloud Environment
- Installation and Configuration of Logical Infrastructure for Cloud Environment
- Running Logical Infrastructure for Cloud Environment
- Managing Logical Infrastructure for Cloud Environment
- Compliance with Regulations and Controls
- Risk Assessment for Logical and Physical Infrastructure
- Collection, Acquisition, and Preservation of Digital Evidence
- Managing Communication with Stakeholders

6 - LEGAL AND COMPLIANCE

- Legal Requirements and Unique Risks within the Cloud Environment
- Relevant Privacy and PII Laws and Regulations
- Audit Process, Methodologies, and Required Adaptions for a Cloud Environment

- Implications of Cloud to Enterprise Risk Management
- Outsourcing and Cloud Contract Design
- Vendor Management