



course : Cloud Security Professional (CSP)

City :	Paris	Hotel :	Le Meurice
Start Date :	2025-12-22	End Date :	2025-12-26
Duration :	1 Week	Price :	5950 \$



Course Overview

With the rapid adoption of cloud computing, organizations face new security challenges in protecting sensitive data, applications, and infrastructure. The Cloud Security Professional (CSP) training course equips participants with the knowledge and skills required to secure cloud environments effectively. This course covers cloud security principles, risk management, compliance frameworks, and best practices for designing, implementing, and managing secure cloud solutions. Participants will gain hands-on experience with security tools, techniques, and strategies to mitigate threats, manage vulnerabilities, and ensure data privacy and regulatory compliance.

Course Objectives

By the end of this course, participants will be able to:

- Understand core cloud security concepts, models, and deployment types.
- Identify and mitigate security risks in cloud environments.
- Apply best practices for cloud identity and access management (IAM).
- Implement encryption, data protection, and network security measures.
- Develop compliance strategies aligned with global cloud security standards.
- Monitor, detect, and respond to cloud security incidents effectively.
- Design and implement secure cloud architectures for business continuity.

Target Audience

This course is suitable for professionals responsible for cloud environments, including:

- Cloud security engineers and architects
- IT security managers and officers
- Network administrators and systems engineers
- Risk and compliance professionals
- Anyone preparing for cloud security certifications or responsible for securing cloud-based services

Methodology



The course combines interactive learning methods to ensure comprehension and practical application, including:

Instructor-led lectures and demonstrations

Hands-on labs and practical exercises

Case studies of real-world cloud security scenarios

Group discussions and problem-solving workshops

Participants will gain both theoretical knowledge and practical skills to implement cloud security measures that protect organizational assets and comply with industry standards.

Course Outline

Day One: Introduction to Cloud Security

Overview of cloud computing and deployment models (IaaS, PaaS, SaaS)

Cloud security challenges and threat landscape

Shared responsibility model in cloud environments

Key cloud security terminology and concepts

Day Two: Identity, Access, and Authentication

Cloud identity and access management (IAM) principles

Authentication methods, multi-factor authentication (MFA)

Role-based access control (RBAC) and policy management

Hands-on exercises: configuring IAM in cloud platforms

Day Three: Data Security and Encryption

Data classification and sensitivity in the cloud

Encryption at rest and in transit

Secure key management practices

Backup, recovery, and data integrity strategies

Hands-on exercises: implementing data protection in cloud services

Day Four: Network Security and Threat Management

Network segmentation and cloud firewall configuration

Intrusion detection and prevention in cloud environments

Monitoring, logging, and alerting for cloud security events

Incident response planning and best practices

Hands-on exercise: detecting and responding to cloud security incidents

Day Five: Cloud Security Governance and Compliance

Regulatory frameworks and standards (ISO 27017, NIST, GDPR)

Cloud security policies and procedures

Risk assessment and continuous monitoring



Final project: designing a secure cloud architecture
Course wrap-up, Q&A, and personal action plan

Certificates

On successful completion of this training course, HighPoint Certificate will be awarded to the delegates.
Continuing Professional Education credits (CPE): In accordance with the standards of the National Registry of CPE Sponsors, one CPE credit is granted per 50 minutes of attendance.