Certified Cloud Security Professional (CCSP) Preparation Course

Duration: 5 Days

Language: en

Course Code: PI1 - 145

Objective

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

- Master the six domains of the CCSP Common Body of Knowledge (CBK).
- Understand cloud computing concepts, architectures, and security requirements.
- Apply best practices in cloud data protection, identity management, and risk governance.
- Assess compliance with international standards such as ISO 27017, ISO 27018, and GDPR.
- Implement cloud security controls across major providers (AWS, Azure, GCP).
- Prepare confidently for the CCSP certification exam with practical tools and mock assessments.

Audience

This course is ideal for:

- Information Security Professionals aiming for advanced cloud security certification.
- Cloud Architects and Engineers managing multi-cloud infrastructures.
- Security Consultants and Auditors specialising in cloud compliance and governance.
- IT Risk Managers and CISOs responsible for securing enterprise cloud assets.
- Professionals preparing for CCSP or CISSP certifications.

Training Methodology

The course uses a blend of interactive lectures, case studies, and hands-on labs based on real-world cloud configurations. Participants will engage in domain-specific exercises and exam simulations to strengthen understanding and readiness.

Summary

This advanced and comprehensive course is designed to prepare IT and cybersecurity professionals for the **(ISC)² Certified Cloud Security Professional (CCSP)** certification. The

programme combines theoretical knowledge with hands-on cloud security practices to help participants master the six domains of the CCSP Common Body of Knowledge (CBK).

Participants will develop a deep understanding of cloud architecture, data security, compliance frameworks, risk management, and operations within multi-cloud environments. Through a blend of conceptual learning and practical exercises, learners will be able to apply security principles across AWS, Azure, and GCP infrastructures.

By the end of this course, participants will possess the technical and strategic expertise to secure cloud environments, manage risks, and lead cloud security initiatives within their organisations — while being fully prepared to pass the CCSP certification exam on their first attempt.

Course Content & Outline

Section 1: Cloud Concepts, Architecture, and Design

- Overview of cloud computing models (IaaS, PaaS, SaaS).
- Cloud reference architectures and service models.
- Key components of secure cloud architecture.
- Shared responsibility model and its implications for security.
- Assessing cloud service provider (CSP) risks and capabilities.

Section 2: Cloud Data Security

- Data lifecycle management in the cloud.
- Encryption, key management, and tokenisation strategies.
- Data classification, retention, and disposal policies.
- Implementing secure data storage and backups.
- Ensuring compliance with privacy regulations (GDPR, HIPAA, ISO 27701).

Section 3: Cloud Platform and Infrastructure Security

- Securing compute, storage, and networking layers.
- Virtualisation and container security principles.
- Cloud hardening techniques for AWS, Azure, and GCP.
- Managing vulnerabilities and configuration baselines.
- Security considerations in hybrid and multi-cloud environments.

Section 4: Cloud Application Security

- Secure software development in the cloud (DevSecOps).

- Application threat modelling and secure API design.
- Identity federation, SSO, and access control mechanisms.
- Monitoring, logging, and runtime protection for cloud-native apps.
- Evaluating cloud application risks and third-party integrations.

Section 5: Cloud Security Operations

- Security operations management in the cloud (SOC, SIEM, and SOAR).
- Continuous monitoring and incident response in cloud environments.
- Business continuity and disaster recovery strategies.
- Patch management and automated compliance validation.
- Investigating and mitigating cloud breaches and misconfigurations.

Section 6: Legal, Risk, and Compliance in Cloud Environments

- Cloud compliance frameworks: ISO 27017, ISO 27018, NIST 800-53, CSA CCM.
- Legal and regulatory considerations in data sovereignty.
- Risk management methodologies and contractual requirements.
- Vendor management and third-party assurance processes.
- Preparing for audits and certification readiness assessments.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Assessment Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

IT & Computer Application, Technology

Tags

Cloud Data Security, CISSP certifications, Cloud Security Professional

Related Articles

How Cloud Computing Can Improve Your Accounting Information System

Discover how cloud computing is reshaping the accounting landscape, providing enhanced accessibility, cost-efficiency, and data security. Uncover five key benefits and address potential risks to optimise your financial management.