Certified Cloud Security Professional (CCSP) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The Certified Cloud Security Professional training program provides participants with advanced knowledge and practical skills required to secure cloud architectures, protect cloud platforms, and manage enterprise-level cloud security operations. As organizations increasingly migrate critical infrastructure to AWS, Azure, and Google Cloud, the demand for professionals who can safeguard sensitive workloads, mitigate cyber threats, and ensure compliance with global security standards continues to rise. Certified Cloud Security Professional (CCSP) Training Course equips learners with robust techniques for cloud risk management, identity and access controls, data security, cloud infrastructure protection, and regulatory compliance frameworks aligned with industry best practices.

Through real-world case studies, hands-on analysis, and scenario-based learning, participants gain the ability to evaluate cloud environments, design secure architectures, and implement multi-layered cybersecurity strategies. With cloud ecosystems becoming the backbone of digital transformation, the CCSP curriculum empowers professionals to proactively address emerging security challenges, manage complex hybrid environments, and strengthen organizational resilience against cyberattacks. The course prepares learners for both certification success and real-world security leadership.

Programme Curriculum

Certified Cloud Security Professional (CCSP) Training Course

Introduction

The Certified Cloud Security Professional training program provides participants with advanced knowledge and practical skills required to secure cloud architectures, protect cloud platforms, and manage enterprise-level cloud security operations. As organizations increasingly migrate critical infrastructure to AWS, Azure, and Google Cloud, the demand for professionals who can safeguard sensitive workloads, mitigate cyber threats,

and ensure compliance with global security standards continues to rise. Certified Cloud Security Professional (CCSP) Training Course equips learners with robust techniques for cloud risk management, identity and access controls, data security, cloud infrastructure protection, and regulatory compliance frameworks aligned with industry best practices.

Through real-world case studies, hands-on analysis, and scenario-based learning, participants gain the ability to evaluate cloud environments, design secure architectures, and implement multi-layered cybersecurity strategies. With cloud ecosystems becoming the backbone of digital transformation, the CCSP curriculum empowers professionals to proactively address emerging security challenges, manage complex hybrid environments, and strengthen organizational resilience against cyberattacks. The course prepares learners for both certification success and real-world security leadership.

Course Objectives

1. Understand cloud computing concepts, architectures, and key security principles.
2. Analyze cloud risk management frameworks and assess cloud-specific vulnerabilities.
3. Apply identity and access management solutions across multi-cloud environments.
4. Implement data protection techniques including encryption, classification, and tokenization.
5. Configure secure cloud infrastructure through network segmentation and workload protection.
6. Assess and implement compliance requirements for global cloud security standards.
7. Manage cloud security operations including monitoring, logging, and threat detection.
8. Apply best practices for securing hybrid and multi-cloud deployments.
9. Evaluate cloud vendor security models and shared responsibility frameworks.
10. Conduct incident response planning and cloud forensics investigations.
11. Implement DevSecOps techniques for secure CI/CD pipeline management.
12. Strengthen governance, policies, and organizational cloud security strategies.
13. Prepare for CCSP certification through structured domain-based learning.

Organizational Benefits

- Stronger cloud security posture across hybrid and multi-cloud systems
- Enhanced readiness for compliance audits and regulatory requirements
- Reduced organizational risk through improved cloud governance
- Better monitoring and threat detection across cloud workloads
- Effective access control and protection of critical assets
- Improved resilience against cloud-based cyberattacks
- Standardized cloud security procedures across departments
- Reduced downtime and financial losses linked to security breaches
- Stronger alignment with industry frameworks and best practices
- Increased staff capability to manage advanced cloud environments

Target Audiences

- Cloud security engineers and cloud architects
- Cybersecurity analysts and security operations professionals
- IT infrastructure and system administrators
- Cloud compliance officers and risk managers
- DevOps and DevSecOps professionals
- Network security engineers and technology leads
- Digital transformation and cloud migration teams

- CTOs, IT managers, and technical decision-makers

Course Duration: 10 days

Course Modules

Module 1: Cloud Computing Concepts & Architecture

- Understand cloud service models, deployment options, and architecture layers
- Analyze cloud security responsibilities and governance requirements
- Map security roles in IaaS, PaaS, and SaaS environments
- Review industry frameworks guiding secure cloud design
- Examine risks associated with cloud transformation
- Case Study: Misconfigured cloud environment leading to exposure

Module 2: Cloud Data Security

- Implement data classification and lifecycle management
- Apply encryption, tokenization, and key management controls
- Design secure data storage and handling processes
- Protect data across multi-cloud environments
- Manage risks associated with data sharing and transfer
- Case Study: Data leakage due to weak encryption practices

Module 3: Cloud Platform & Infrastructure Security

- Secure virtual networks and cloud workload architectures
- Configure segmentation, firewalls, and security groups
- Implement hardened virtual machines and secure baselines
- Assess cloud network attack surfaces
- Use automated tools for infrastructure scanning
- Case Study: Compromised workload in a public cloud VPC

Module 4: Identity & Access Management in Cloud

- Design strong IAM policies and zero-trust controls
- Implement multifactor authentication and privileged access controls
- Manage identity federation across cloud platforms
- Reduce risks through least-privilege and continuous verification
- Monitor identity-related threats and anomalies
- Case Study: IAM misconfiguration leading to unauthorized access

Module 5: Cloud Application Security

- Apply secure coding and application hardening practices
- Evaluate APIs, containers, and microservices for vulnerabilities
- Integrate security testing into CI/CD pipelines
- Review secure software development methodologies
- Apply runtime protection for cloud applications
- Case Study: API vulnerability exploited in a cloud-native application

Module 6: Cloud Security Operations

- Monitor cloud events, logs, and security alerts
- Apply SIEM and SOC tools for cloud-focused monitoring
- Detect cloud-specific attack vectors
- Manage configuration changes and continuous compliance
- Perform operational risk assessments
- Case Study: Threat hunting and remediation in a cloud SOC

Module 7: Cloud Risk Management & Assessment

- Identify cloud-specific risks and mitigation strategies
- Conduct cloud security assessments and gap analysis
- Apply risk scoring methods for prioritization
- Build organizational risk registers for cloud systems
- Leverage automated risk assessment tools
- Case Study: Cloud risk audit revealing governance weaknesses

Module 8: Cloud Compliance & Legal Requirements

- Interpret global cloud compliance frameworks and standards
- Assess data protection regulations in cloud adoption
- Map shared responsibility for compliance obligations
- Implement compliance monitoring dashboards
- Document compliance controls for auditors
- Case Study: Cloud compliance breach resulting in penalties

Module 9: Cloud Virtualization Security

- Understand hypervisor vulnerabilities and isolation techniques
- Secure container environments and orchestration platforms
- Manage risks in shared technology layers
- Implement workload segmentation and runtime controls
- Monitor virtualization events and abnormal activity
- Case Study: Hypervisor escape attack simulation

Module 10: Cloud Network Security

- Evaluate cloud-native network security features
- Configure network controls for segmentation and secure routing
- Protect cloud perimeters using advanced filtering techniques
- Implement DDoS protection and traffic monitoring
- Detect unauthorized network behaviors
- Case Study: Network breach through unsecured cloud gateway

Module 11: Cloud Encryption & Key Management

- Design encryption strategies aligned with regulatory requirements
- Manage cloud key management systems and HSM integrations
- Protect keys across cloud environments
- Apply lifecycle management to keys and certificates
- Monitor unauthorized access attempts to encryption assets
- Case Study: Compromised key store impacting cloud data security

Module 12: DevSecOps & Automation

- Embed security controls into CI/CD pipelines
- Automate configuration, patching, and deployment checks
- Use IaC (Infrastructure as Code) securely
- Prevent configuration drift and policy violations
- Deploy automated scanning tools during builds
- Case Study: DevSecOps transformation in a financial cloud project

Module 13: Cloud Forensics & Incident Response

- Build incident response plans for cloud breaches
- Conduct log analysis and forensic data acquisition
- Coordinate cloud provider involvement in investigations
- Respond to identity, data, and infrastructure attacks
- Document findings and lessons learned
- Case Study: Forensic investigation following a multi-cloud compromise

Module 14: Cloud Governance & Policy Development

- Develop cloud security policies and governance frameworks
- Establish oversight structures for cloud initiatives
- Integrate governance with enterprise risk management
- Align governance with compliance and business objectives
- Define roles for cloud security ownership
- Case Study: Governance overhaul after audit deficiencies

Module 15: Designing a Secure Cloud Strategy

- Build enterprise cloud security architecture roadmaps
- Integrate multi-cloud strategies with business goals
- Identify long-term investments in cloud security tools
- Evaluate vendor maturity and security posture
- Ensure sustainable security across cloud expansion
- Case Study: Enterprise-wide secure cloud adoption strategy

Training Methodology

- Instructor-led presentations on cloud security domains
- Hands-on exercises using real cloud security scenarios
- Case study analysis to reinforce practical understanding
- Peer learning discussions and group problem-solving
- Step-by-step practice for CCSP exam preparation
- Tools, templates, and checklists for workplace application

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com