



Certified Cloud Security Professional 'Bootcamp' in Addis Ababa

The objective of this course is to help cybersecurity teams and IT professionals build strong cloud security skills to design, manage, and protect cloud environments across modern platforms. The course provides hands-on learning in cloud security architecture, data protection, identity management, compliance, threat mitigation, and operational security measures.

5 FULL DAYS | <DATE - TBD> | TRAINING FACILITIES AT <LOCATION>

- The course is aligned with global Cloud Security frameworks and CCSP-based learning objectives.
- Focus on real-world cloud risks, configuration vulnerabilities, threat modeling, compliance, IAM, and incident response.
- Hands-on practice with cloud environments covering IaaS, PaaS, SaaS, multi-cloud, and hybrid security scenarios.
- Includes practical exercises on encryption, key management, DevSecOps, IAM controls, and secure configuration assessment.
- Participants will gain confidence to design secure cloud architectures, implement protection controls, and respond to cloud incidents.
- Ideal for professionals planning to enhance Cloud Security skills or prepare for global CCSP certification.
- **Course prerequisites:** Basic understanding of cybersecurity & cloud fundamentals; familiarity with networking, virtualization & encryption concepts; recommended 2+ years of IT/Security experience.

TARGET AUDIENCE

- Cloud Security Professionals
- Cybersecurity Analysts
- SOC Teams / Blue Team / Security Engineers
- Network & System Administrators
- Cloud Architects & Cloud Engineers
- IT Security Managers
- Anyone preparing for CCSP Certification

THE INSTRUCTOR

Delivered by senior instructors with 10+ years of experience in cybersecurity and ICT systems, with strong hands-on and professional training expertise. Practical, scenario-based learning and hands-on labs are emphasized.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.



MODULE 01

CLOUD CONCEPTS, ARCHITECTURE, AND DESIGN

Understand the foundational principles of cloud computing. Explore service models (IaaS, PaaS, SaaS), deployment models (public, private, hybrid), and shared responsibility frameworks. Learn about virtualization, containerization, and emerging technologies influencing cloud architecture.

MODULE 02

CLOUD GOVERNANCE AND RISK MANAGEMENT

Study governance frameworks and organizational roles in cloud adoption. Learn risk management methodologies, security policy development, and compliance integration within cloud strategies. Understand SLA negotiation and continuous monitoring requirements.

MODULE 03

CLOUD DATA SECURITY

Explore cloud data lifecycle management, data classification, and protection mechanisms. Learn about encryption technologies, tokenization, key management systems (KMS), and strategies for securing data at rest, in transit, and in use.

MODULE 04

CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

Understand how to secure virtualized environments and cloud infrastructure components. Learn about workload isolation, virtualization security, and hypervisor vulnerabilities. Study network segmentation, perimeter controls, and baseline configuration management.

MODULE 05

CLOUD APPLICATION SECURITY

Examine secure software development practices within the cloud. Learn secure DevOps (DevSecOps), code repositories, API security, and application containerization. Understand the importance of software supply chain security and CI/CD pipeline integrity.

MODULE 06

CLOUD SECURITY OPERATIONS

Explore operational security concepts in cloud environments, including threat detection, logging, auditing, and continuous monitoring. Learn incident response procedures, forensic analysis techniques, and cloud-native SOC integration principles.

MODULE 07

CLOUD IDENTITY AND ACCESS MANAGEMENT (IAM)

Study identity federation, single sign-on (SSO), multi-factor authentication (MFA), and privilege management. Understand IAM implementation in AWS, Azure, and Google Cloud. Learn the principles of least privilege, just-in-time access, and access review cycles.

MODULE 08

CLOUD SECURITY ARCHITECTURE AND DESIGN

Develop the ability to architect secure cloud environments. Learn security patterns, zero-trust design, and secure multi-tenancy. Explore security configuration baselines, reference architectures, and defense-in-depth strategies for complex deployments.

MODULE 09

CLOUD LEGAL, RISK, AND COMPLIANCE

Understand legal and regulatory obligations in cloud computing. Study data privacy laws (GDPR, HIPAA, CCPA), cross-border data transfer challenges, and compliance auditing. Learn about e-discovery, cloud evidence management, and contractual risk mitigation.

MODULE 10

CLOUD INFRASTRUCTURE AND VIRTUALIZATION TECHNOLOGIES

Explore cloud infrastructure components in depth - compute, storage, and networking. Understand orchestration tools, container security (Docker, Kubernetes), and virtual machine management. Learn about securing APIs and management planes.

MODULE 11

BUSINESS CONTINUITY AND DISASTER RECOVERY IN THE CLOUD

Learn to design and maintain resilient cloud architectures. Study backup strategies, replication, failover mechanisms, and recovery point/time objectives (RPO/RTO). Understand continuity planning within multi-cloud and hybrid models.

MODULE 12

CLOUD THREATS, ATTACKS, AND VULNERABILITIES

Examine cloud-specific attack vectors and vulnerabilities. Understand account hijacking, API abuse, insecure interfaces, and misconfiguration exploits. Learn detection and mitigation strategies against these threats.

MODULE 13

CLOUD FORENSICS AND INCIDENT RESPONSE

Study forensic acquisition, evidence preservation, and investigation challenges in virtualized and multi-tenant environments. Learn coordinated response strategies, reporting procedures, and containment methodologies.

MODULE 14

CLOUD SECURITY AUTOMATION AND ORCHESTRATION

Understand automation concepts in cloud security operations. Study Infrastructure as Code (IaC), Security as Code, automated policy enforcement, and orchestration tools used for compliance and monitoring.

MODULE 15

CLOUD VENDOR MANAGEMENT AND AUDITING

Learn how to assess third-party cloud providers. Study vendor risk management, compliance audits, and contractual controls. Understand shared audit responsibilities and continuous compliance frameworks (ISO 27017, SOC 2, CSA STAR).

MODULE 16

SECURE CLOUD MIGRATION AND INTEGRATION

Explore the security implications of cloud migration strategies. Learn migration planning, data transfer security, and hybrid cloud integration. Understand challenges in securing interconnectivity between on-premises and cloud environments.



MODULE 17

CLOUD SECURITY METRICS AND MONITORING

Study performance metrics, key performance indicators (KPIs), and continuous monitoring techniques. Learn to interpret security event data, detect anomalies, and measure cloud security effectiveness.

MODULE 18

CLOUD GOVERNANCE FRAMEWORKS AND BEST PRACTICES

Understand industry frameworks and standards such as CSA CCM, NIST SP 800-53, ISO 27001, and CIS Benchmarks. Learn to align governance structures with organizational risk appetite and compliance goals.

MODULE 19

EMERGING CLOUD TECHNOLOGIES

Explore emerging technologies including serverless computing, edge computing, and artificial intelligence in cloud environments. Analyze new risks, trends, and the evolving landscape of cloud security innovation.

MODULE 20

CLOUD SECURITY PROGRAM MANAGEMENT

Integrate all prior concepts into an enterprise-wide cloud security strategy. Learn program development, maturity assessment, reporting, and continuous improvement processes for long-term organizational success.