Cloud Security Architecture and Design Principles Training Course

Professional Development Training Course Outline

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

Course Introduction

- In the face of relentless digital transformation, securing cloud environments has become the paramount concern for modern enterprises. Cloud Security Architecture and Design Principles Training Course is engineered to equip security professionals and architects with the strategic knowledge and tactical skills necessary to build resilient, secure, and compliant cloud infrastructures. We delve into cutting-edge architectural patterns like Zero Trust and Cybersecurity Mesh Architecture (CSMA), providing a comprehensive understanding of securing diverse models IaaS, PaaS, and SaaS across a multi-cloud/hybrid environment. Our focus is on proactive DevSecOps integration, leveraging Infrastructure as Code (IaC) for security automation, and mastering the nuances of the Shared Responsibility Model to drastically reduce the organizational attack surface and enhance overall security posture.
  The program moves beyond mere tool usage to instill a "secure-by-design" mindset, enabling participants to architect solutions that stand up to the most sophisticated threats, including advanced persistent threats and zero-day exploits. By integrating concepts such as Cloud Security Posture Management (CSPM), robust Identity and Access Management (IAM), and intelligent AI-driven threat detection, this curriculum ensures that graduates are prepared to lead their organizations toward future-proof cloud governance and continuous compliance. This is essential training for anyone responsible for designing and securing mission-critical applications and data in the highly dynamic and distributed cloud native landscape.

Programme Curriculum

Cloud Security Architecture and Design Principles Training Course

Introduction

In the face of relentless digital transformation, securing cloud environments has become the paramount concern for modern enterprises. Cloud Security Architecture and Design Principles Training Course is engineered to equip security professionals and architects with the strategic knowledge and tactical skills necessary to build resilient, secure, and compliant cloud infrastructures. We delve into cutting-edge architectural patterns like Zero Trust and Cybersecurity Mesh Architecture (CSMA), providing a comprehensive understanding of securing diverse models IaaS, PaaS, and SaaS across a multi-cloud/hybrid environment. Our focus is on proactive DevSecOps integration, leveraging Infrastructure as Code (IaC) for security automation, and mastering the nuances of the Shared Responsibility Model to drastically reduce the organizational attack surface and enhance overall security posture.

The program moves beyond mere tool usage to instill a "secure-by-design" mindset, enabling participants to architect solutions that stand up to the most sophisticated threats, including advanced persistent threats and zero-day exploits. By integrating concepts such as Cloud Security Posture Management (CSPM), robust Identity and Access Management (IAM), and intelligent AI-driven threat detection, this curriculum ensures that graduates are prepared to lead their organizations toward future-proof cloud governance and continuous compliance. This is essential training for anyone responsible for designing and securing mission-critical applications and data in the highly dynamic and distributed cloud native landscape.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Architect robust, future-proof cloud environments utilizing Zero Trust Architecture (ZTA) principles.
2. Design and implement advanced Identity and Access Management (IAM) and Federation strategies for multi-cloud parity.
3. Evaluate and apply the Shared Responsibility Model across IaaS, PaaS, and SaaS for strategic risk ownership.
4. Integrate security controls throughout the software development lifecycle using DevSecOps and Policy-as-Code (PaC) methodologies.
5. Design and enforce network security using Micro-segmentation and cloud-native firewalls in a hybrid setup.
6. Master data security frameworks, including advanced Data Encryption techniques for data at rest and in transit.
7. Implement Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) solutions for continuous security validation.
8. Formulate a Disaster Recovery (DR) and Business Continuity plan optimized for cloud resilience and high availability.
9. Develop strategies for leveraging AI and Machine Learning for proactive and automated threat detection and incident response.
10. Design a Security Operations Center (SOC) strategy for centralized logging, monitoring, and Cloud Incident Response (IR).
11. Secure Container and Serverless architectures using specialized cloud-native security tools.
12. Establish a cloud Governance, Risk, and Compliance (GRC) framework to meet major regulatory requirements
13. Apply the Cybersecurity Mesh Architecture (CSMA) concept to unify security policy across distributed assets.

Target Audience

1. Cloud Security Architects
2. Security Engineers/Analysts
3. Enterprise Architects
4. DevSecOps Engineers
5. Chief Information Security Officers (CISOs) and Security Leaders
6. IT/Cloud Infrastructure Managers
7. Security-Focused Software Developers
8. Compliance and Risk Management Professionals

Course Modules

Module 1: Foundational Cloud Security and Architectural Principles

- Review of the core cloud service models and deployment models.
- In-depth analysis of the Shared Responsibility Model for each service type.
- Key security design principles.
- Understanding cloud-native tools and third-party security solutions.
- Identifying and mitigating the Top Cloud Threats
- Case Study: Analysis of a major cloud data breach caused by a simple misconfigured S3 bucket, demonstrating a failure in understanding the Shared Responsibility Model.

Module 2: Zero Trust Architecture (ZTA) in the Cloud

- Core pillars of ZTA.
- Designing and implementing a "Never Trust, Always Verify" policy across cloud environments.
- Transitioning from perimeter-based security to identity-based controls.
- Leveraging Conditional Access Policies and device posture for continuous verification.
- The role of SASE in ZTA implementation.
- Case Study: Implementing Google?ÇÖs BeyondCorp model to secure workforce access without traditional VPNs across a hybrid cloud setup.

Module 3: Cloud Identity and Access Management (IAM) Design

- Designing hierarchical resource structures for policy enforcement.
- Implementing Role-Based Access Control and Attribute-Based Access Control
- Strategies for Identity Federation and Single Sign-On.
- Securing Privileged Access Management and "Break Glass" procedures.
- Managing Customer Identity and Access Management solutions.
- Case Study: Consolidating multiple on-premises Active Directory instances into a centralized cloud IAM to eliminate identity sprawl.

Module 4: Cloud Network Security and Micro-segmentation

- Designing secure Virtual Private Clouds and subnet architectures.
- Implementing Hub-and-Spoke models and centralized security inspection points.
- Techniques for Micro-segmentation using security groups, network ACLs, and firewall rules.
- Securing ingress and egress traffic.
- Advanced DDoS protection and traffic filtering using cloud-native services.

- Case Study: Designing a secure network architecture for a finance application, enforcing strict micro-segmentation to prevent lateral movement following a breach in a public-facing tier.

Module 5: Data Security and Encryption Strategies

- Data classification, discovery, and tagging methodologies in a cloud context.
- Designing an end-to-end Data Encryption strategy
- Key Management Architecture.
- Implementing data loss prevention across cloud storage and applications.
- Securing data lakes, object storage, and managed database services.
- Case Study: Migrating a highly regulated healthcare database to the cloud, focusing on the correct implementation of Customer-Managed Encryption Keys to meet strict patient privacy requirements.

Module 6: Governance, Risk, and Compliance in the Cloud

- Establishing a Cloud Governance framework and a centralized security policy.
- Conducting cloud-specific Risk Assessments and mitigation planning.
- Mapping cloud controls to regulatory requirements
- Using cloud-native tools for continuous compliance validation.
- Implementing security guardrails using Organization Policy services.
- Case Study: An organization?ÇÖs journey to achieve PCI DSS compliance in the cloud, detailing the architectural controls required for the cardholder data environment.

Module 7: DevSecOps and Security Automation

- Integrating security tools into the CI/CD pipeline
- Using Infrastructure as Code tools for secure provisioning.
- Implementing Policy-as-Code with tools like OPA/Rego to enforce guardrails pre-deployment.
- Automated remediation of misconfigurations and security vulnerabilities.
- Designing immutable infrastructure and secure golden images/containers.
- Case Study: Implementing a DevSecOps pipeline where automated security scans and a PaC engine block a deployment if an unencrypted storage bucket is found in the IaC template.

Module 8: Serverless and Container Security

- Understanding the expanded Shared Responsibility Model for PaaS and Serverless.
- Securing container orchestration platforms and their control planes.
- Implementing container image scanning, trusted registries, and runtime protection.
- Securing serverless functions and their execution roles.
- Best practices for secure secret management and environment variable handling.
- Case Study: Securing a microservices-based application running on a Kubernetes cluster, focusing on implementing a robust Container Network Policy and vulnerability management process.

Module 9: Cloud Security Posture Management and Visibility

- Implementing Cloud Security Posture Management for continuous misconfiguration detection.
- Utilizing Cloud Workload Protection Platforms for runtime visibility and hardening.
- Automating security validation and continuous assurance processes.
- Designing a centralized, aggregated view of the security posture across multi-cloud.
- Selecting and integrating unified security platforms

- Case Study: Using a CSPM tool to identify and automatically remediate critical policy violations across 100+ production accounts.

Module 10: Security Operations and Centralized Logging

- Designing a logging and monitoring architecture for security purposes.
- Integrating cloud-native logs into a central SIEM/SOAR platform.
- Implementing effective security alerts, anomaly detection, and correlation rules.
- Automating incident triage and response using Security Orchestration, Automation, and Response.
- Leveraging AI-driven threat detection to analyze massive data volumes.
- Case Study: Designing a Cloud-Focused SOC capability for a global enterprise, detailing the log aggregation architecture and the automation of a suspicious login alert

Module 11: Cloud Incident Response and Forensics

- Creating a cloud-specific Incident Response Playbook and communication plan.
- Identifying key data sources for cloud forensics and evidence preservation.
- Architecting "Immutable" logging trails for non-repudiation in an IR scenario.
- Technical steps for isolation, containment, and eradication of cloud-based threats.
- Post-incident activities: lessons learned, reporting, and architectural feedback loops.
- Case Study: Responding to a crypto-mining attack that leveraged compromised service accounts, detailing the steps for containment, identity credential rotation, and forensic data capture.

Module 12: Business Continuity and Disaster Recovery

- Designing highly resilient architectures using availability zones and multiple regions.
- Implementing automated failover mechanisms and continuous health checks.
- The 3-2-1 Backup Rule and securing backup/snapshot access and immutability.
- Disaster Recovery testing strategies and establishing Recovery Time/Point Objectives
- Securing the BCDR plane from ransomware and malicious access.
- Case Study: Architecting a high-availability, multi-region application using active-active deployment to ensure a near-zero RTO/RPO following a regional cloud outage.

Module 13: Vendor Management and Multi-Cloud Strategy

- Establishing a Multi-Cloud/Hybrid security reference architecture for consistency.
- Conducting due diligence and risk assessment for Cloud Service Providers and third-party SaaS vendors.
- Addressing vendor lock-in and security integration challenges across disparate platforms.
- Utilizing the Cybersecurity Mesh Architecture to unify security policies across clouds.
- Evaluating vendor security certifications and compliance reports
- Case Study: A global retail company adopting a multi-cloud strategy, focusing on the design pattern used to achieve unified IAM and centralized logging across both providers.

Module 14: Threat Modeling and Secure Design Review

- Introduction to structured threat modeling methodologies
- Practicing Threat Modeling for new cloud application designs and microservices.
- Conducting formal Secure Architecture Review workshops and documentation.
- Identifying and avoiding common security architectural Anti-Patterns.
- Integrating threat modeling as a mandatory step in the pre-production gate.

- Case Study: Threat modeling a new API gateway service that processes sensitive user data, identifying and mitigating elevation of privilege and spoofing threats before deployment.

Module 15: Advanced Topics and Future Trends

- Securing modern APIs and implementing robust API Security controls.
- Security implications and architecture of Quantum Computing and Post-Quantum Cryptography.
- The use of Confidential Computing for protecting data in use.
- Emerging trends: FinOps and security alignment, and AI/ML Security frameworks.
- Career pathways and professional certifications for the Cloud Security Architect.
- Case Study: Evaluating the security benefits and architectural design of using a confidential computing service to protect highly sensitive intellectual property during in-memory processing.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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