

SEC549 Cloud Security Architecture Training

30 May – 3 June 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

SEC549 Cloud Security Architecture Training

Ref: 2224_262697 **Date:** 30 May – 3 June 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

The SEC549 Cloud Security Architecture Training is a one-week technical course designed for enterprise security architects, cloud engineers, and technical leads seeking to design resilient defense architectures across distributed multi-cloud platforms. Organizations often struggle to secure multi-cloud environments due to inconsistent identity perimeters, fragmented network transit designs, and complex regulatory data requirements across cloud service providers. This course addresses these hurdles by examining structured threat modeling, federated identity frameworks, micro-segmented network transit patterns, and compliance-aligned security controls. The SEC549 Cloud Security Architecture Training is delivered by Agile Leaders Training Center.

Who Should Attend

- Cloud security architects responsible for engineering multi-cloud defense frameworks.
- Enterprise infrastructure engineers responsible for designing secure network transit topologies.
- Identity and access management specialists responsible for configuring federated cross-cloud authentication.
- Information security managers responsible for aligning cloud architecture with regulatory compliance mandates.
- Cybersecurity operations leads responsible for integrating centralized telemetry and incident visibility.

The course assumes participants already manage enterprise cloud infrastructure or security operations at work, leaving out foundational system administration and introductory cloud provisioning.

Departments and Industries

The course delivers practical architectural methodologies for specialists across diverse operating environments.

- Cloud Infrastructure and Security Architecture in Financial Services
- Information Security and Network Operations in Telecommunications
- Cybersecurity Engineering and Systems Integration in Energy and Utilities
- IT Governance, Risk, and Compliance in Healthcare Technology
- Enterprise Architecture and Infrastructure Defense in Retail and Supply Chain

Learning Objectives

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

- Apply STRIDE and PASTA threat modeling methodologies to distributed multi-cloud workloads.
- Build cross-cloud identity architectures utilizing OpenID Connect and conditional access controls.
- Design micro-segmented virtual transit networks utilizing central firewall inspection points.
- Prioritize regulatory data protection baselines aligned with NCA CCC-2:2024 controls and SDAIA PDPL requirements.
- Evaluate multi-cloud logging topologies to centralize telemetry into Microsoft Sentinel.
- Build an enterprise security architecture review document for complex cloud deployments.

AGILE LEADERS
Training Center

Course Agenda

Day 1: Threat Modeling and Cloud Security Foundations

- STRIDE, LINDDUN, and PASTA Threat Modeling for Cloud Workloads
- Cloud Security Architecture Reviews for Multi-Tenant Environments
- Infrastructure-as-Code Security Validation using Terraform Scanning
- Shared Responsibility Mapping across Hyperscaler Workloads
- Resource Tagging and Data Classification Schema Design

Day 2: Cross-Cloud Identity and Access Perimeter

- Cross-Cloud Identity Federation with OpenID Connect and Service Principals
- Conditional Access Policy Design and Zero Trust Enforcement
- Customer Identity and Access Management with Microsoft External ID
- AWS Cognito User Pool Architecture and Token Validation
- Break-Glass Account Procedures and Privileged Credential Management

Day 3: Network Architecture and Micro-Segmentation

- Hub-and-Spoke Transit Network Topologies across Multi-Cloud Environments
- Centralized Virtual Appliance Inspection with Palo Alto Firewalls
- Azure Virtual WAN and Transit Gateway Routing Architectures
- VPC Gateways and Private Interface Endpoint Security Micro-Segmentation
- NCA CCC-2:2024 Network Control Architecture for Cloud Tenants

Day 4: Data Protection, Logging, and Compliance Controls

- Cross-Cloud Key Management Service Topologies and Envelope Encryption
- Centralized Telemetry Aggregation using Microsoft Sentinel
- CST Cloud Computing Services Provisioning Regulations Version 4 Registration Tiers
- SDAIA Personal Data Protection Law Cross-Border Data Transfer Controls
- Cloud Security Monitoring Architecture under NCA ECC Control 4-1-3-2

Day 5: Security Architecture Practice and Capstone

- Exercise: Cross-Cloud Identity Federation and Conditional Access Design
- Exercise: Multi-Cloud Transit Network Micro-Segmentation Architecture
- Exercise: Compliance-Aligned Data Protection and Sentinel Ingestion Review
- CloudWars Defensive Architecture Evaluation Scenarios
- Capstone Exercise: Multi-Cloud Enterprise Security Architecture Blueprint

Practical Exercises

The course includes practical architectural design sessions structured around realistic deployment scenarios.

- **Cross-Cloud Identity Blueprint:** Configure OpenID Connect federation and conditional access rules across environments as a suggested activity.
- **Secure Transit Hub Design:** Construct a hub-and-spoke network transit diagram featuring centralized inspection appliances as a suggested activity.
- **Regulatory Compliance Audit:** Evaluate cloud workload data handling against national cloud cybersecurity standards as a suggested activity.
- **Defensive Architecture Capstone:** Produce an enterprise multi-cloud security architecture blueprint mitigating complex infrastructure threats as a suggested activity.

FAQs

Who suits the SEC549 Cloud Security Architecture Training and what does it assume?

The course suits cybersecurity professionals, enterprise architects, and senior engineers responsible for cloud workload protection. Participants should have practical experience administering cloud services or enterprise networks before enrolling, as the course leaves out introductory system administration and basic cloud concepts.

How does SEC549 Cloud Security Architecture Training differ from foundational cloud security courses?

This course focuses on advanced multi-cloud architectural design, cross-cloud identity federation, transit network micro-segmentation, and regulatory alignment, rather than single-provider administration or basic security hygiene checklists.

Which cloud platforms are evaluated during the SEC549 Cloud Security Architecture Training?

The course addresses security architecture patterns across major cloud service providers including Amazon Web Services, Microsoft Azure, and Google Cloud Platform, highlighting cross-platform federation and interoperability.

How does the SEC549 Cloud Security Architecture Training address local compliance mandates?

The course aligns multi-cloud architecture decisions with the NCA Cloud Cybersecurity Controls CCC-2:2024 and SDAIA Personal Data Protection Law requirements for tenant workloads and data hosting.

Conclusion

Participants complete the course with an enterprise cloud security architecture blueprint and a formal threat modeling review framework. This structured documentation provides standardized architectural patterns that streamline security reviews, strengthen cross-cloud defense, and enforce governance boundaries. Organizations achieve resilient multi-cloud environments capable of withstanding advanced threats while meeting stringent tenant compliance standards.