Cloud-Native Risk Controls and Compliance Training Course

Professional Development Training Course Outline

Category	Risk Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The accelerating shift to Cloud-Native Architectures leveraging technologies like Kubernetes, containers, and microservices on platforms such as AWS, Azure, and GCP has revolutionized application development and deployment speed. However, this agility introduces complex, dynamic security and compliance challenges that traditional, perimeter-focused strategies cannot address. A core tenet of modern enterprise security is embedding risk controls directly into the automated CI/CD pipeline, a philosophy known as DevSecOps. This essential training course is designed to bridge the gap between rapid cloud-native innovation and stringent regulatory requirements. Cloud-Native Risk Controls and Compliance Training Course moves beyond the foundational Shared Responsibility Model to focus on implementing automated compliance-as-code (CaC) and continuous monitoring solutions to proactively manage misconfigurations, secure the software supply chain, and maintain Cloud Security Posture Management (CSPM) across multi-cloud environments. The goal is to cultivate a security culture that is both resilient and compliant by design.

The course delivers a practical, hands-on methodology to master the Governance, Risk, and Compliance (GRC) landscape in the age of hyperscale cloud computing. Participants will learn how to design and deploy robust, automated security guardrails to protect sensitive data and critical workloads in dynamic, ephemeral cloud environments. By mastering tools for real-time threat detection, vulnerability management, and aligning cloud controls with major frameworks, professionals will gain the expertise to transform compliance from a reactive bottleneck into a competitive enabler. This training equips technical and governance teams with the knowledge to establish a unified and effective Cloud Center of Excellence (CCoE), ultimately reducing cyber risk and ensuring data sovereignty in a rapidly evolving digital landscape.

Programme Curriculum

Cloud-Native Risk Controls and Compliance Training Course

Introduction

The accelerating shift to Cloud-Native Architectures leveraging technologies like Kubernetes, containers, and microservices on platforms such as AWS, Azure, and GCP has revolutionized application development and deployment speed. However, this agility introduces complex, dynamic security and compliance challenges that traditional, perimeter-focused strategies cannot address. A core tenet of modern enterprise security is embedding risk controls directly into the automated CI/CD pipeline, a philosophy known as DevSecOps. This essential training course is designed to bridge the gap between rapid cloud-native innovation and stringent regulatory requirements. Cloud-Native Risk Controls and Compliance Training Course moves beyond the foundational Shared Responsibility Model to focus on implementing automated compliance-as-code (CaC) and continuous monitoring solutions to proactively manage misconfigurations, secure the software supply chain, and maintain Cloud Security Posture Management (CSPM) across multi-cloud environments. The goal is to cultivate a security culture that is both resilient and compliant by design.

The course delivers a practical, hands-on methodology to master the Governance, Risk, and Compliance (GRC) landscape in the age of hyperscale cloud computing. Participants will learn how to design and deploy robust, automated security guardrails to protect sensitive data and critical workloads in dynamic, ephemeral cloud environments. By mastering tools for real-time threat detection, vulnerability management, and aligning cloud controls with major frameworks, professionals will gain the expertise to transform compliance from a reactive bottleneck into a competitive enabler. This training equips technical and governance teams with the knowledge to establish a unified and effective Cloud Center of Excellence (CCoE), ultimately reducing cyber risk and ensuring data sovereignty in a rapidly evolving digital landscape.

Course Duration

5 days

Course Objectives

1. Master the Shared Responsibility Model and implement Zero Trust Architecture (ZTA) principles in cloud-native settings.
2. Design and enforce Security Policies-as-Code (PaC) using tools like OPA/Rego and cloud-native services.
3. Implement robust Infrastructure-as-Code (IaC) security scanning and controls using Terraform and CloudFormation.
4. Establish DevSecOps automation by integrating security and compliance tools into the CI/CD pipeline.
5. Perform effective Container and Kubernetes Security hardening, including image scanning and runtime protection.
6. Configure and utilize Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) tools for continuous compliance.
7. Design and audit Cloud Identity and Access Management (IAM) with a focus on least privilege and secrets management.
8. Navigate and map cloud controls to major Compliance Frameworks
9. Develop strategies for Data Sovereignty and implementing Data Loss Prevention (DLP) in multi-cloud environments.
10. Implement Automated Remediation workflows to proactively address security drift and compliance violations.
11. Secure Serverless and Microservices architectures against common threats and misconfigurations.
12. Conduct Cloud Risk Assessments focused on emerging threats, including securing GenAI infrastructure.

13. Build a Continuous Compliance program through advanced logging, monitoring, and real-time threat detection.

Target Audience

1. Cloud Security Engineers
2. DevSecOps Practitioners
3. Governance, Risk, and Compliance (GRC) Professionals
4. Cloud Architects
5. Security and IT Auditors
6. CISO/VP of Security Leaders
7. SREs (Site Reliability Engineers)
8. Internal Audit and Legal Teams

Course Modules

Module 1: Cloud-Native GRC Fundamentals and the Shared Fate Model

- Understanding the cloud-native GRC shift from traditional audit to continuous compliance.
- Deconstructing the Shared Responsibility Model and transitioning to Shared Fate.
- Mapping standard controls to ephemeral cloud resources.
- Introduction to Cloud Control Matrix (CCM) and Consensus Assessment Initiative Questionnaire (CAIQ).
- Case Study: Analyzing a major cloud breach caused by a fundamental IAM misconfiguration under the Shared Responsibility Model.

Module 2: Identity, Access, and the Zero Trust Perimeter

- Implementing Zero Trust Architecture (ZTA) across all cloud access points.
- Designing robust Cloud IAM policies, roles, and conditional access
- Securing sensitive data using dedicated solutions like Vault or cloud provider services.
- Multi-Factor Authentication, FIDO, and leveraging machine identity.
- Case Study: Auditing a microservices application for adherence to the Principle of Least Privilege and remediating service-to-service credential exposure.

Module 3: Security-as-Code and DevSecOps Automation

- Integrating security checks from the commit stage using pre-commit hooks.
- Scanning and enforcing compliance policies within Terraform and CloudFormation templates.
- Writing and deploying governance rules using Open Policy Agent (OPA) and Rego.
- Securing the CI/CD pipeline itself to prevent supply chain attacks
- Case Study: Automating the prevention of public S3 bucket creation by embedding an OPA policy check into a GitHub Actions CI/CD pipeline.

Module 4: Container and Kubernetes Security Controls

- Image scanning, trusted registries, and mitigating vulnerabilities.
- Securing the control plane, data plane, and API server
- Enforcing security policies at deployment time using Admission Controllers
- Monitoring and protecting running containers against unexpected behavior
- Case Study: Implementing a cluster-wide Network Policy to isolate sensitive workloads in a production Kubernetes cluster to meet PCI DSS segmentation requirements.

Module 5: Cloud Security Posture Management (CSPM) and Continuous Monitoring

- Using native and third-party CSPM tools to gain comprehensive visibility across multi-cloud.
- Detecting and remediating unauthorized changes and cloud misconfigurations in real-time.
- Security Information and Event Management.
- Setting up workflows to automatically fix non-compliant resources
- Case Study: Utilizing a CSPM tool dashboard to identify and auto-remediate a critical finding: unencrypted database volumes across a multi-region deployment.

Module 6: Data Protection, Encryption, and Sovereignty

- Identifying, classifying, and tagging sensitive data across cloud services.
- Implementing and managing encryption at rest and in transit using KMS and External Key Management
- Data Loss Prevention.
- Regulatory Compliance
- Case Study: Designing a solution for a financial firm to meet EU data sovereignty laws by restricting data processing and storage to specific geographical regions using cloud resource policies.

Module 7: Serverless, Microservices, and API Security

- Securing Function-as-a-Service components and minimizing the attack surface.
- API Gateway Security.
- Leveraging a service mesh for mTLS encryption and fine-grained authorization between microservices.
- Deploying Web Application Firewalls and Content Delivery Network security controls.
- Case Study: Securing a vulnerable Lambda function by implementing resource-based IAM policies and integrating a Serverless Application Repository (SAR) for vulnerability scanning.

Module 8: Incident Response, Audit, and Future Trends

- Preparing cloud environments for effective incident response and data collection.
- Generating automated, continuous evidence for audit requests
- Addressing the risks and compliance controls for securing Large Language Models and AI infrastructure.
- Anticipating future regulations like the Cyber Resilience Act and evolving cloud standards.
- Case Study: Simulating an incident response exercise for a ransomware attack on a cloud-native database, focusing on automated recovery and forensic log preservation.

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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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