Cloud Security for Banks Training Course

Professional Development Training Course Outline

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

Course Introduction

In today’s rapidly evolving digital banking ecosystem, Cloud Security for Banks has become a mission-critical priority driven by digital transformation, cloud adoption, fintech integration, and regulatory compliance. Financial institutions are increasingly leveraging public cloud, private cloud, and hybrid cloud infrastructures to enhance scalability, operational efficiency, and customer experience. However, this shift introduces complex cybersecurity risks, data privacy challenges, and regulatory obligations, requiring banks to implement robust cloud security frameworks, zero trust architecture, and advanced threat protection strategies.

Cloud Security for Banks Training Course equips banking professionals with cutting-edge knowledge on cloud risk management, secure cloud architecture, identity and access management (IAM), data protection, encryption strategies, and compliance standards such as GDPR, PCI DSS, and ISO 27001. Participants will gain practical insights into cloud threat intelligence, DevSecOps, API security, and incident response in cloud environments, ensuring resilience against evolving cyber threats while maintaining regulatory alignment and operational continuity.

Programme Curriculum

Cloud Security for Banks Training Course

Introduction
In today’s rapidly evolving digital banking ecosystem, Cloud Security for Banks has become a mission-critical priority driven by digital transformation, cloud adoption, fintech integration, and regulatory compliance. Financial institutions are increasingly leveraging public cloud, private cloud, and hybrid cloud infrastructures to enhance scalability, operational efficiency, and customer experience. However, this shift introduces complex cybersecurity risks, data privacy challenges, and regulatory obligations, requiring banks to implement robust cloud security frameworks, zero trust architecture, and advanced threat protection strategies.

Cloud Security for Banks Training Course equips banking professionals with cutting-edge knowledge on cloud risk management, secure cloud architecture, identity and access management (IAM), data protection, encryption strategies, and compliance standards such as GDPR, PCI DSS, and ISO 27001. Participants will gain practical insights into cloud threat intelligence, DevSecOps, API security, and incident response in cloud environments, ensuring resilience against evolving cyber threats while maintaining regulatory alignment and operational continuity.

Course Duration

5 days

Course Objectives

1. Understand cloud computing models and banking applications
2. Identify cloud security risks, vulnerabilities, and threat vectors
3. Implement Zero Trust Security Architecture in banking cloud systems
4. Strengthen Identity and Access Management (IAM) frameworks
5. Apply data encryption, tokenization, and secure data lifecycle management
6. Ensure compliance with GDPR, PCI DSS, ISO 27001, and Basel guidelines
7. Develop secure cloud migration strategies for core banking systems
8. Enhance API security and open banking protection mechanisms
9. Integrate DevSecOps practices into cloud-based banking applications
10. Monitor and respond to cloud-based cyber threats and breaches
11. Implement cloud governance, risk, and compliance (GRC) frameworks
12. Strengthen business continuity and disaster recovery in cloud environments
13. Utilize AI-driven threat detection and cloud security analytics

Target Audience

1. Chief Information Security Officers (CISOs)
2. IT Security Managers and Analysts
3. Cloud Architects and Engineers
4. Risk and Compliance Officers
5. Core Banking System Administrators
6. Digital Banking and FinTech Professionals
7. Internal Auditors and IT Auditors
8. Cybersecurity Consultants and Advisors

Course Modules

Module 1: Cloud Computing Fundamentals in Banking

- Cloud service models-IaaS, PaaS, SaaS
- Public vs Private and Hybrid cloud
- Cloud adoption trends in banking
- Benefits and risks of cloud transformation
- Case Study: Migration of a regional bank to hybrid cloud

Module 2: Cloud Security Frameworks & Standards

- Shared responsibility model
- NIST, ISO 27001, CSA frameworks

- Regulatory compliance in banking cloud
- Cloud security governance models
- Case Study: Compliance failure and regulatory penalties

Module 3: Identity & Access Management (IAM)

- Role-based and attribute-based access control
- Multi-factor authentication (MFA)
- Privileged access management (PAM)
- Identity federation and SSO
- Case Study: Unauthorized access breach in cloud banking

Module 4: Data Security & Encryption

- Data classification and protection
- Encryption at rest and in transit
- Tokenization and masking techniques
- Key management systems (KMS)
- Case Study: Data leakage incident in a cloud database

Module 5: Network Security in Cloud

- Virtual private clouds (VPCs)
- Firewalls, IDS/IPS systems
- Secure network architecture
- DDoS protection strategies
- Case Study: DDoS attack on online banking platform

Module 6: Application & API Security

- Secure software development lifecycle (SDLC)
- API security in open banking
- DevSecOps integration
- Vulnerability scanning and patching
- Case Study: API breach in fintech integration

Module 7: Cloud Risk Management & Compliance

- Risk identification and assessment
- Third-party/vendor risk management
- Regulatory reporting and audits
- Governance, Risk & Compliance (GRC) tools
- Case Study: Vendor risk causing compliance breach

Module 8: Incident Response & Business Continuity

- Cloud incident detection and response
- Security monitoring and SIEM tools
- Disaster recovery planning (DRP)
- Business continuity planning (BCP)
- Case Study: Cloud outage impacting banking operations

Training Methodology

- 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

Start Date	End Date	Location	Price
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