Identity and Access Management (IAM) 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

Identity and Access Management (IAM) for Banks Training Course is designed to strengthen identity governance, access control, privileged access management (PAM), zero trust security, regulatory compliance, and cyber risk resilience within modern financial institutions. As banks accelerate digital transformation through cloud banking, open banking, mobile platforms, artificial intelligence (AI), and API ecosystems, effective IAM has become a critical defense mechanism against data breaches, insider threats, identity fraud, unauthorized access, and cyberattacks. This course equips banking professionals with advanced knowledge of digital identity management, authentication technologies, role-based access control (RBAC), biometric security, multi-factor authentication (MFA), and identity lifecycle management.

The program focuses on building a secure, scalable, and compliant identity architecture aligned with global banking standards and emerging cybersecurity trends. Participants will explore best practices in access governance, identity analytics, automated provisioning, cloud IAM, privileged account security, and regulatory frameworks while analyzing real-world banking case studies. Through practical exercises and industry scenarios, learners will develop the capabilities required to implement effective IAM strategies that enhance operational efficiency, customer trust, cybersecurity maturity, and financial sector resilience.

Programme Curriculum

Identity and Access Management (IAM) for Banks Training Course

Introduction

Identity and Access Management (IAM) for Banks Training Course is designed to strengthen identity governance, access control, privileged access management (PAM), zero trust security, regulatory compliance, and cyber risk resilience within modern financial institutions. As banks accelerate digital transformation through cloud banking, open banking, mobile platforms, artificial intelligence (AI), and API ecosystems, effective IAM

has become a critical defense mechanism against data breaches, insider threats, identity fraud, unauthorized access, and cyberattacks. This course equips banking professionals with advanced knowledge of digital identity management, authentication technologies, role-based access control (RBAC), biometric security, multi-factor authentication (MFA), and identity lifecycle management.

The program focuses on building a secure, scalable, and compliant identity architecture aligned with global banking standards and emerging cybersecurity trends. Participants will explore best practices in access governance, identity analytics, automated provisioning, cloud IAM, privileged account security, and regulatory frameworks while analyzing real-world banking case studies. Through practical exercises and industry scenarios, learners will develop the capabilities required to implement effective IAM strategies that enhance operational efficiency, customer trust, cybersecurity maturity, and financial sector resilience.

Course Duration

5 days

Course Objectives

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

1. Understand the strategic importance of Identity and Access Management (IAM) in modern banking cybersecurity.
2. Develop effective identity governance frameworks aligned with banking regulations and risk management practices.
3. Implement Zero Trust Architecture (ZTA) principles for secure banking environments.
4. Design and manage Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models.
5. Strengthen authentication security through Multi-Factor Authentication (MFA) and adaptive authentication.
6. Manage Privileged Access Management (PAM) to protect critical banking systems.
7. Apply identity lifecycle management from onboarding to access termination.
8. Improve compliance with GDPR, ISO 27001, PCI DSS, NIST, and financial regulations.
9. Understand modern cloud identity security and hybrid IAM architectures.
10. Reduce risks associated with insider threats and identity-based attacks.
11. Apply automation through Identity Governance and Administration (IGA) solutions.
12. Enhance fraud prevention using identity analytics and behavioral monitoring.
13. Develop a future-ready IAM strategy supporting digital banking transformation.

Target Audience

1. Chief Information Security Officers (CISOs) and cybersecurity executives.
2. Bank IT managers and infrastructure leaders.
3. Identity and Access Management professionals.
4. Cybersecurity analysts and security engineers.
5. Risk management and compliance officers.
6. Digital banking and transformation teams.
7. Internal auditors and governance professionals.
8. System administrators and application security teams.

Course Modules

Module 1: Fundamentals of Identity and Access Management in Banking

- Introduction to IAM concepts, principles, and banking applications.
- Importance of digital identity in financial services.
- Identity lifecycle management processes.
- IAM architecture components and frameworks.
- Emerging trends in banking identity security.
- **Case Study:** A global bank implements an IAM transformation program after multiple unauthorized access incidents, improving security visibility and regulatory compliance.

Module 2: Identity Governance and Administration (IGA)

- Designing effective identity governance frameworks.
- User provisioning and de-provisioning automation.
- Access certification and entitlement reviews.
- Segregation of duties (SoD) controls.
- Governance dashboards and identity analytics.
- **Case Study:** A commercial bank automates employee access reviews using IGA tools, reducing compliance risks during regulatory audits.

Module 3: Authentication Technologies and Access Security

- Multi-Factor Authentication (MFA) implementation.
- Passwordless authentication strategies.
- Biometrics and behavioral authentication.
- Single Sign-On (SSO) solutions.
- Adaptive and risk-based authentication.
- **Case Study:** A digital bank introduces biometric authentication to improve customer security while reducing account takeover fraud.

Module 4: Privileged Access Management (PAM)

- Protecting privileged accounts and administrators.
- PAM architecture and implementation strategies.
- Privileged session monitoring.
- Just-in-Time (JIT) access management.
- Preventing insider threats through privileged controls.
- **Case Study:** A financial institution deploys PAM controls after detecting excessive administrator privileges across critical systems.

Module 5: Zero Trust Identity Security Framework

- Principles of Zero Trust security.
- Identity as the new security perimeter.
- Continuous authentication and authorization.
- Least privilege access models.
- Micro-segmentation and identity-based controls.
- **Case Study:** A multinational bank adopts Zero Trust IAM to secure remote employees and cloud-based banking applications.

Module 6: Cloud IAM and Digital Banking Security

- Cloud identity management strategies.
- Hybrid and multi-cloud IAM challenges.
- API identity security.
- Securing mobile banking identities.
- Cloud access governance.
- **Case Study:** A bank migrating workloads to the cloud implements cloud IAM controls to protect customer financial data.

Module 7: IAM Risk Management, Compliance and Audit

- IAM regulatory requirements in banking.
- ISO 27001 and NIST IAM controls.
- PCI DSS identity requirements.
- IAM auditing methodologies.
- Cyber risk reporting and monitoring.
- **Case Study:** A regulated bank improves audit readiness by aligning IAM processes with international cybersecurity standards.

Module 8: Future Trends in Banking IAM

- Artificial Intelligence (AI) in identity security.
- Machine learning for identity threat detection.
- Decentralized digital identity.
- Identity analytics and fraud prevention.
- Future IAM operating models.
- **Case Study:** A fintech organization uses AI-driven identity analytics to detect suspicious access behavior and prevent fraud.

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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