Identity and Access Management Operations Training Course

16 – 20 May 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Identity and Access Management Operations Training Course

Ref: 1658_222507 **Date:** 16 – 20 May 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Identity and Access Management Operations Training Course is a one-week foundation-to-practitioner course for IAM analysts, security administrators and audit teams, who leave with an IAM Control Design and Operations Pack. It connects identity proofing, account lifecycle, authentication, federation, authorization, privileged access, governance and monitoring through documented controls and operational evidence. Participants design a traceable identity operating model. Agile Leaders Training Center develops practical identity and access management operations capability.

Who Should Attend

- Identity teams responsible for account lifecycle and access services
- Security administration teams responsible for authentication and authorization
- Governance teams responsible for access policy and certification
- Audit and risk teams responsible for control assurance
- Application teams responsible for federation and role integration
- Privileged-access teams responsible for sensitive accounts and sessions

The course assumes participants support enterprise systems or security controls, and it leaves out vendor-specific administration, software development and certification exam preparation.

Departments and Industries

The course supports organisations that manage workforce, contractor and privileged access across digital services.

- Cybersecurity, identity governance and technology risk
- Information technology and application operations
- Financial services, insurance and professional services
- Healthcare, education and public services
- Energy, manufacturing, retail and logistics

Learning Objectives

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

- Build an identity lifecycle and ownership model
- Apply identity-proofing and authentication assurance decisions
- Compare RBAC, ABAC and policy-based authorization
- Use SSO, MFA and federation design patterns
- Evaluate privileged access and identity-governance controls
- Diagnose access incidents and control-evidence gaps

Course Agenda

Day 1: Identity Lifecycle and Governance

- NIST SP 800-63-4 Digital Identity Model
- Identity Source and Attribute Authority Map
- Joiner Mover Leaver Lifecycle Workflow
- Account Ownership and RACI Matrix
- Identity Policy and Exception Register

Day 2: Authentication and Federation

- Identity Assurance and Authentication Assurance Decision
- MFA Authenticator Selection and Recovery Plan
- SSO Trust Boundary and Session Map
- OpenID Connect Provider and Relying-Party Flow
- Federation Assertion and Claims Design

Day 3: Authorization and Privileged Access

- RBAC Role Engineering and Entitlement Catalogue
- ABAC Attribute and Policy Decision Matrix
- Access Request Approval and Provisioning Workflow
- Segregation-of-Duties Conflict Ruleset
- PAM Vault Session and Emergency-Access Controls

Day 4: Identity Governance and Operations

- Access Review and Certification Campaign Design
- Orphan Dormant and Shared Account Detection
- Directory Synchronisation and Reconciliation Control
- IAM Logging Monitoring and Alert Matrix
- Identity Incident and Revocation Runbook

AGILE LEADERS
Training Center

Day 5: IAM Control Practice and Capstone

- Exercise: Trace a Joiner Mover Leaver Failure
- Exercise: Diagnose Authentication and Federation Errors
- Exercise: Resolve Role and Segregation Conflicts
- Exercise: Review Privileged Access Evidence
- Capstone: IAM Control Design and Operations Pack

Practical Exercises

Suggested activities use identity records, access requests, logs and control evidence.

- Suggested activity: map identity sources, owners and lifecycle transitions
- Suggested activity: design SSO, MFA and federation trust controls
- Suggested activity: build role, entitlement and segregation rules
- Suggested activity: investigate an access incident and complete review evidence

FAQs

Who should take identity and access management training, and what does it assume?

It suits IAM analysts, security administrators, application teams, auditors and identity-governance staff who already support enterprise systems or security controls.

How does identity and access management training differ from general cybersecurity training?

IAM training concentrates on digital identities, authentication, authorization, account lifecycle, federation, privileged access and governance; general cybersecurity training covers a broader range of threats, technologies and controls.

What is the difference between RBAC and ABAC in IAM?

RBAC assigns permissions through defined roles, while ABAC evaluates attributes about subjects, resources, actions and context against policy rules; organisations may combine both approaches.

How do SSO and identity federation work together?

SSO reduces repeated authentication across services, while federation conveys trusted identity and authentication information between separate security domains using protocols and assertions.

Why are access reviews important in identity governance?

Access reviews provide accountable evidence that entitlements remain appropriate, identify excessive or orphaned access and trigger remediation through named owners and tracked decisions.

Conclusion

Participants take back an IAM Control Design and Operations Pack containing lifecycle, authentication, federation, authorization, PAM, review and incident artefacts. The pack connects policy decisions to technical flows, ownership and evidence. It helps identity teams provision access consistently, detect exceptions, govern privilege and support audit assurance.