

Microsoft 365 Identity and Access Management

ARC502

Design, secure, and defend modern identity systems that stop breaches at the front door. Build Zero Trust identity architectures, enforce least-privilege access, and operationalize enterprise-grade IAM programs across Microsoft 365, Entra ID, and hybrid environments.

Modules	23
Lessons	239
Phases	7
Free preview	Course Orientation (8 lessons)

The method

IAM is a governance discipline that happens to be implemented in a directory. This course runs the same loop for every access surface it governs.

1. Model the access before configuring it. Groups, roles and their nesting decide who can reach what long after anybody remembers why. Architecture first, then the objects.
2. Grant through a process that leaves a record. Access packages and entitlement management exist so a grant has a requester, an approver and an expiry rather than a memory.
3. Govern the identities with no human behind them. Service principals, workload identities and agent identities accumulate permissions and never leave the organization.
4. Review access as if the reviewer is busy. A review nobody can complete honestly gets rubber-stamped, and a rubber-stamped review is worse than none because it produces evidence of diligence.
5. Monitor for what governance misses. Stale identities, permission creep and credential health, measured rather than assumed.

The course closes by assembling the complete program: the controls, the risk register and the decision record that survives your departure.

What this course assumes

No minimum experience and no prerequisite course. The Entra object model, the governance features and the licensing that gates them are explained where they first matter.

What makes it go faster: a tenant with Entra ID P2, since most governance features are gated behind it. Not required, and the course states plainly which controls need which tier.

What this course does not cover: identity attack detection and incident response, which are separate courses, and directory administration. This is governance.

Full syllabus

Phase 1: Course Foundations

Course Orientation [FREE PREVIEW](#)

What Microsoft 365 Identity and Access Management teaches: operationalize a governed identity program where every identity, human and machine, has an owner, a lifecycle, and compliance evidence, using Entra ID Governance, entitlement management, access reviews, and PIM.

1. IAM0.1 What Identity Governance Actually Is
2. IAM0.2 The Identity Lifecycle in Your Tenant
3. IAM0.3 Access Governance Principles. Why Access Accumulates
4. IAM0.4 Non-Human Identity. The Governance Gap Nobody Sees
5. IAM0.5 The Northgate Engineering Scenario
6. IAM0.6 Lab Setup and Cost Management
7. IAM0.7 Your IAM Program Package
8. Module Summary

The Entra ID Identity Ecosystem

The foundation every subsequent module builds on.

1. IAM1.1 Identity Types as Governance Objects
2. IAM1.2 The Identity Data Model
3. IAM1.3 Data Quality as a Governance Foundation
4. IAM1.4 Group Architecture for IAM
5. IAM1.5 Administrative Units and Delegation Boundaries
6. IAM1.6 Licensing for Identity Governance
7. IAM1.7 The Governance State Assessment
8. Module Summary
9. Check My Knowledge

Phase 2: User Identities

Implementing and Managing User Identities

The operational foundation. How user identities work in Entra ID, the object model, creation process, attributes, extension mechanisms, password policies, authentication method registration, lifecycle states, external identities, and production-scale management. You can't automate what you don't...

1. IAM2.1 The User Object Model
2. IAM2.2 Creating User Identities
3. IAM2.3 Bulk User Operations
4. IAM2.4 User Attributes and Extension Attributes
5. IAM2.5 Password Policies and Self-Service Password Reset
6. IAM2.6 Authentication Method Registration
7. IAM2.7 User Lifecycle States
8. IAM2.8 External Identities and B2B Guests
9. IAM2.9 User Management at Scale
10. IAM2.10 NE User Identity Design
11. IAM2 Module Lab. User Identity Deployment
12. IAM2 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Group Architecture and Role-Based Access

Groups are the access assignment mechanism in Entra ID.

1. IAM3.1 Group Strategy as IAM Infrastructure
2. IAM3.2 Dynamic Groups for Automated Access
3. IAM3.3 Dynamic Group Design Patterns
4. IAM3.4 Role-Based Access Design in Entra ID
5. IAM3.5 Custom Role Design
6. IAM3.6 Group Governance
7. IAM3.7 Group-Based Licensing
8. IAM3.8 Group Nesting and Inheritance
9. IAM3.9 Group Access Reviews
10. IAM3.10 NE Group Architecture
11. IAM3.11 Module Lab
12. IAM3.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Phase 3: Authentication & Access

Authentication Methods and Passwordless

Authentication is how identities prove who they are.

1. IAM4.1 The Authentication Landscape
2. IAM4.2 MFA Registration and Enforcement
3. IAM4.3 FIDO2 Security Keys
4. IAM4.4 Windows Hello for Business
5. IAM4.5 Certificate-Based Authentication
6. IAM4.6 Temporary Access Pass and Microsoft Authenticator
7. IAM4.7 Authentication Strength Policies
8. IAM4.8 Method Registration Policies
9. IAM4.9 NE Authentication Architecture
10. IAM4.10 Module Lab
11. IAM4.11 Guided Walkthrough
12. Module Summary
13. Check My Knowledge

Conditional Access Architecture

Conditional Access is the access policy engine that enforces every authentication and access decision in your tenant.

1. IAM5.1 Conditional Access as the Access Policy Engine
2. IAM5.2 Policy Design Principles
3. IAM5.3 Risk-Based Policies
4. IAM5.4 CA for Guest and External Identities
5. IAM5.5 CA Templates and Common Patterns
6. IAM5.6 Session Management
7. IAM5.7 Report-Only Mode and Impact Analysis
8. IAM5.8 CA Governance
9. IAM5.9 Token Protection and Token Lifetime
10. IAM5.10 NE Conditional Access Architecture
11. IAM5.11 Module Lab
12. IAM5.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Phase 4: Apps & Workload Identities

Module 6, Application Access and OAuth Consent Governance

Application access as an identity discipline rather than an app problem: OAuth consent fundamentals, consent policy design, reviewing what has already been granted, and governing the service principals that hold permissions nobody reviews.

1. IAM6.1 Application Access as an IAM Discipline
2. IAM6.2 OAuth Consent Fundamentals
3. IAM6.3 Consent Policy Design
4. IAM6.4 Reviewing Granted Permissions
5. IAM6.5 SaaS-to-SaaS Integration Risk
6. IAM6.6 App Governance in Defender for Cloud Apps
7. IAM6.7 SCIM Provisioning to SaaS Applications
8. IAM6.8 Application Access Reviews
9. IAM6.9 Application Risk Classification
10. IAM6.10 NE Application Access Governance
11. IAM6.11 Module Lab
12. IAM6.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Module 7, Service Principal and App Registration Governance

Build a governance framework for the non-human identities that outnumber your users, hold broader permissions, and operate without any of the controls you built in Modules 1–6.

1. IAM7.1 The Non-Human Identity Problem
2. IAM7.2 App Registration vs Service Principal
3. IAM7.3 App Registration Inventory and Classification
4. IAM7.4 Credential Governance. Secrets
5. IAM7.5 Credential Governance. Certificates
6. IAM7.6 Permission Analysis and Right-Sizing
7. IAM7.7 Consent Grant Analysis
8. IAM7.8 Service Principal Lifecycle Governance
9. IAM7.9 First-Party vs Third-Party App Governance
10. IAM7.10 NE Service Principal Governance
11. IAM7.11 Module Lab
12. IAM7.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Module 8, Workload Identity and AI Agent Governance

Govern the identities that have no credentials to steal, no passwords to rotate, and no human to blame, managed identities, workload identity federation, and the AI agents that are accumulating permissions in your tenant right now.

1. IAM8.1 Managed Identity Architecture
2. IAM8.2 System-Assigned vs User-Assigned Design
3. IAM8.3 Workload Identity Federation
4. IAM8.4 Workload Identity in Conditional Access
5. IAM8.5 Workload Identity Permissions and Monitoring
6. IAM8.6 The AI Agent Identity Model
7. IAM8.7 Agent Identity Blueprints and Sponsor Accountability
8. IAM8.8 Agent Permission and Access Governance
9. IAM8.9 Agent Risk Detection and Lifecycle
10. IAM8.10 NE Workload and AI Agent Design
11. IAM8.11 Module Lab
12. IAM8.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Phase 5: Privileged Access & Delegation

Privileged Access and Delegation Architecture

How privileged access is governed and who manages the governance.

1. IAM9.1 PIM as the Privileged Access Lifecycle
2. IAM9.2 Role Assignment Governance
3. IAM9.3 PIM Policy Design by Governance Tier
4. IAM9.4 PIM for Groups and Application Roles
5. IAM9.5 Emergency Access Governance
6. IAM9.6 Privileged Access Reviews
7. IAM9.7 Delegation Architecture
8. IAM9.8 Administrative Unit Design Patterns
9. IAM9.9 Delegated Governance Operations
10. IAM9.10 NE Privileged Access and Delegation Design
11. IAM9.11 Module Lab
12. IAM9.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Phase 6: Identity Governance & Lifecycle

Identity Lifecycle Operations

How identities are provisioned, moved, and deprovisioned across your M365 environment.

1. IAM10.1 Inbound Provisioning Architecture
2. IAM10.2 Lifecycle Workflows. Joiner
3. IAM10.3 Lifecycle Workflows. Mover
4. IAM10.4 Lifecycle Workflows. Leaver
5. IAM10.5 Legal Hold, Delayed Deprovisioning, and Rehire
6. IAM10.6 Custom Workflow Extensions
7. IAM10.7 Guest Identity Lifecycle
8. IAM10.8 Provisioning Monitoring and Troubleshooting
9. IAM10.9 Tenant Configuration for Identity Governance
10. IAM10.10 Northgate Engineering Lifecycle Architecture
11. IAM10.11 Module Lab
12. IAM10.12 Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Entitlement Management

The access request engine: catalog architecture, access package design, approval workflows, and the lifecycle policies that expire access without anybody having to remember.

1. IAM11.1 Entitlement Management as the Access Request Engine
2. IAM11.2 Catalog Architecture
3. IAM11.3 Access Package Design
4. IAM11.4 Approval Workflows
5. IAM11.5 Auto-Assignment Policies
6. IAM11.6 Incompatible Access Packages
7. Time-Bound Access and Recertification
8. External Access via Entitlement Management
9. Non-Human Identities in Entitlement Management
10. NE Entitlement Management Design
11. Module Lab
12. Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Access Reviews and Certification

Why access reviews fail, and the design that stops them rubber-stamping: scope and targeting, choosing reviewers and cadence, automation and recommendations, and acting on the outcome.

1. IAM12.1 Why Access Reviews Fail
2. IAM12.2 Access Review Design. Scope and Targeting
3. IAM12.3 Access Review Design. Reviewers and Cadence
4. IAM12.4 Review Automation and AI Recommendations
5. IAM12.5 Guest and External Access Reviews
6. IAM12.6 PIM Access Reviews
7. IAM12.7 Application Access Reviews
8. IAM12.8 Access Review Remediation
9. IAM12.9 Building a Review Program
10. IAM12.10 NE Access Review Program
11. Module Lab
12. Guided Walkthrough
13. Module Summary
14. Check My Knowledge

IAM Monitoring, Detection, and Compliance

Identity monitoring as an IAM function rather than a SOC one: stale identities, permission creep, credential health, and the evidence a compliance conversation actually needs.

1. IAM13.1 Identity Monitoring as an IAM Function
2. IAM13.2 Stale Identity Detection
3. IAM13.3 Permission Creep Detection
4. IAM13.4 Credential Health Monitoring
5. IAM13.5 KQL Queries for IAM Operations
6. IAM13.6 IAM Dashboards and Reporting
7. IAM13.7 Compliance Framework Mapping
8. IAM13.8 Automated Evidence Collection
9. IAM13.9 IAM Maturity Roadmap
10. IAM13.10 NE Monitoring and Compliance
11. Module Lab
12. Guided Walkthrough
13. Module Summary
14. Check My Knowledge

Phase 7: Capstone

The Complete IAM Program

Assembling the program: coherence across every control built so far, the risk register, the architecture decision portfolio, and the deliverable that survives your departure.

1. IAM14.1 IAM Program Assembly
2. IAM14.2 Program Coherence Review
3. IAM14.3 Risk Register Finalization
4. IAM14.4 ADR Portfolio Review
5. IAM14.5 CISO Challenge Simulation
6. IAM14.6 IT Director Challenge Simulation
7. IAM14.7 Audit Challenge Simulation
8. IAM14.8 Operational Cadence Finalization
9. IAM14.9 Executive Summary
10. IAM14.10 Program Maintenance Plan
11. IAM14.11 The Learner's Own Environment
12. IAM14.12 Course Completion and Next Steps
13. IAM14.13 Guided Walkthrough
14. Module Summary
15. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The commands and queries behind every IAM domain in the course, with what each answer decides and what it leaves open.

1. The Identity Data Model
2. User Identity Operations
3. Groups and Role-Based Access
4. Authentication Methods
5. Conditional Access
6. Application Access and Consent
7. Service Principal Governance
8. Workload and Agent Identity
9. Privileged Access and Delegation
10. Lifecycle Operations
11. Entitlement Management
12. Access Reviews
13. Monitoring and Compliance
14. Cadences, Thresholds and Graph Reference

Cookbooks

Ordered procedures for the identity work that recurs: onboarding at scale, offboarding properly, tightening consent, and cleaning up what accumulated.

1. Offboarding Somebody Properly
2. Tightening Consent Without Breaking Work
3. Fixing the Attribute Data
4. Cleaning Up the Guests
5. Rolling Out PIM
6. Building a Review Program That Works
7. Responding to a Compromised Identity

Lab Setup

Building a tenant with a population messy enough to behave like a real directory, where you can break governance safely.

1. The Tenant and What It Carries
2. Building a Directory That Misbehaves
3. Applying Governance and Watching It Miss
4. Breaking It on Purpose
5. Verify, Delays, and What the Lab Cannot Teach

Walkthroughs

Identity work reasoned end to end, including the cases where the number everybody quoted was wrong and the ones that end in doing nothing.

1. The Coverage Number That Was Wrong
2. The Reviews That Certified Nothing
3. The Group That Was Missing Nine People
4. The Access Request That Should Be Refused
5. The Cleanup That Would Have Broken Payroll
6. The Compromise That Was Not One

Playbooks

What to do when something fires or somebody asks: a compromised account, a stalled pipeline, an urgent access request, a departure, an audit.

1. A Risky Sign-In Fires
2. The Provisioning Pipeline Has Stopped
3. Somebody Needs Access Now
4. An Urgent Departure
5. An Auditor Wants Evidence
6. A Change Locked People Out
7. A Supplier Has Been Breached

Playground

Every practice surface available for this course, what each one gives you, and where the gaps are.

References & Further Reading

Microsoft documentation, security frameworks, compliance standards, threat intelligence, and vendor references used throughout the IAM course.

Course Completion

Course Exam

Microsoft 365 Identity and Access Management end-of-course exam: a three-phase simulation testing whether you can apply the method to a situation the course did not walk through.

1. Course Completion. Microsoft 365 Identity and Access Management

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/identity-access-management/