

Identity Governance in Action

Access Certification & Entitlement Remediation

NOCTURNE SYSTEMS | NS-IAM-002 | Microsoft Entra ID | October 2026

PROJECT TYPE: Controlled hands-on identity-governance lab. Business policy, employee transfer scenario, and owner approval are simulated; Entra group-membership changes and audit records are real lab actions.

1. Executive Summary

This project demonstrates a manual access-certification workflow in the Wayne Enterprise Systems Microsoft Entra ID test tenant. Existing identity groups were reviewed, a controlled policy-inconsistent group membership was introduced, and a simulated resource-owner decision authorized removing that membership. The test account was removed and its absence confirmed in the group membership view. Microsoft Entra audit logs recorded successful addition and removal operations.

Scope limitation: WayneHelpDesk is a placeholder enterprise application without a working application backend. This project validates security-group entitlement governance—not successful or denied access to a functioning helpdesk application.

2. Objectives and Environment

Objective	Evidence/approach
Discover existing IAM groups	Review group members, owners, purpose, and application assignments
Assess least privilege	Compare membership with fictional WES-APP-001 policy
Certify and remediate	Record simulated reviewer decision; remove test membership
Validate the change	Recheck group members and inspect Entra audit log events

Tools: Microsoft Entra admin center (browser), Entra ID cloud security groups, enterprise application assignment view, audit logs, and manual certification worksheet. Microsoft 365 Business Premium was the active subscription. No Entra P2-native access review campaign or SailPoint implementation was used.

3. Initial Access Discovery

Group	Observed facts	Outcome
SG-ROLE-IAM-Administrators	1–2 members; owner and documented purpose; no Entra administrator role or enterprise app assignment identified	Effective access not established; investigate further
SG-DEP-HumanResources	1–2 members; HR-aligned; owner assigned; resource assignment not identified	Pending entitlement mapping and owner certification
SG-APP-WayneHelpDesk-Users	3–5 members initially; group owner; assigned to placeholder enterprise application	Selected for controlled certification exercise

The WayneHelpDesk enterprise application was configured with “Assignment required” set to No, and no enterprise application owner was assigned. These are review observations, not proof of exploitability. An assignment existed, but app-role enforcement and live access could not be validated.

4. Access Policy and Certification Logic

Simulated policy WES-APP-001: WayneHelpDesk group membership is intended for employees with IT support, IAM operations, or security incident support responsibilities. Other departments require a documented, owner-approved exception. Access should be reviewed periodically and removed when it no longer has a justified business purpose.

Analyst decision rule: employee job title alone is insufficient to approve or revoke access. Assess the actual entitlement, current job duties, exception history, supporting evidence, and reviewer approval. “Revoke” is supported when a lack of justification is established under policy and a responsible reviewer authorizes the action.

Individual member review — preliminary recommendations

Alias / role	Initially recorded need	Evidence-based outcome
A / Security Engineer	Reported confirmed	Investigate the actual role and required access
B / Security Analyst	Reported confirmed	Investigate; revocation based on title alone unjustified
C / Chief Information Officer	Reported confirmed	Investigate reporting needs and role scope
D / IAM Administrator	Reported confirmed	Provisional retain; verify owner approval and scope

These preliminary recommendations are analyst assessments, not completed owner-approved certifications.

5. Controlled Access Violation

A fictional non-support test employee (“Employee E”) was deliberately added to SG-APP-WayneHelpDesk-Users in the isolated test tenant. The exercise assumed no current helpdesk-related job duty and no approved exception. Baseline and post-addition membership evidence were captured.

SCREENSHOT 1: Baseline group membership

4 group members found						
☐	Name ↑	Type	Email	User type	Object Id	Device Id
☐	 Barbara Gordon	User	barbara.gordon@WayneEnterprise921.onmicrosoft.com	Member	d64a5625-d8b1-47bc-a03a-22700cc8cc1f	
☐	 Dick Grayson	User	dick.grayson@WayneEnterprise921.onmicrosoft.com	Member	cae5d681-110a-495f-bb59-6e5b94f8beb8	
☐	 Lucius Fox	User	lucius.fox@WayneEnterprise921.onmicrosoft.com	Member	a8c5cb45-1898-4944-a459-c7f594097b6d	
☐	 Tim Drake	User	tim.drake@WayneEnterprise921.onmicrosoft.com	Member	a305245c-f652-4dcf-b3b2-3750635bb462	

SCREENSHOT 2: Simulated excessive membership

5 group members found						
☐ Name ↑	Type	Email	User type	Object id	Device id	
☐  Barbara Gordon	User	barbara.gordon@WayneEnterprise921.onmicrosoft.com	Member	d64a5625-d8b1-47bc-a03a-22700cc8cc1f		
☐  Dick Grayson	User	dick.grayson@WayneEnterprise921.onmicrosoft.com	Member	cae5d681-110a-495f-bb59-6e5b94f8beb8		
☒  Leslie Thompkins	User	leslie.thompkins@WayneEnterprise921.onmicrosoft.com	Member	27b03946-41a5-4435-9393-95d57c6d0003		
☐  Lucius Fox	User	lucius.fox@WayneEnterprise921.onmicrosoft.com	Member	a8c5cb45-1898-4944-a459-c7f594097b6d		
☐  Tim Drake	User	tim.drake@WayneEnterprise921.onmicrosoft.com	Member	a305245c-f652-4dcf-b3b2-3750635bb462		

6. Certification Decision and Remediation

Record field	Training-lab entry
Finding ID	IGA-004
Identity	Employee E (fictional test account)
Entitlement	Membership in SG-APP-WayneHelpDesk-Users
Policy reference	WES-APP-001 (simulated lab policy)
Analyst recommendation	Revoke: no job-based justification or documented exception in scenario
Decision authority	Simulated WayneHelpDesk resource owner
Owner decision	Simulated approval to revoke
Action performed	Removed Employee E from group

The analyst recommendation and simulated resource-owner approval were recorded separately. Actual remediation consisted only of removal of a test account from an Entra security group; no working application-side permission was modified.

SCREENSHOT 3: Post-remediation group membership

4 group members found						
☐ Name ↑	Type	Email	User type	Object id	Device id	
☐  Barbara Gordon	User	barbara.gordon@WayneEnterprise921.onmicrosoft.com	Member	d64a5625-d8b1-47bc-a03a-22700cc8cc1f		
☐  Dick Grayson	User	dick.grayson@WayneEnterprise921.onmicrosoft.com	Member	cae5d681-110a-495f-bb59-6e5b94f8beb8		
☐  Lucius Fox	User	lucius.fox@WayneEnterprise921.onmicrosoft.com	Member	a8c5cb45-1898-4944-a459-c7f594097b6d		
☐  Tim Drake	User	tim.drake@WayneEnterprise921.onmicrosoft.com	Member	a305245c-f652-4dcf-b3b2-3750635bb462		

7. Audit Evidence and Validation

The Entra audit-log screenshot shows a successful “Add member to group” event at 6:43:35 AM and a successful “Remove member from group” event at 6:45:18 AM on October 15, 2026 (as displayed in the portal). The events are approximately 103 seconds apart. The user separately checked the group membership page and confirmed the test identity was no longer listed.

Evidence note: the provided audit-list screenshot shows event types, success statuses, and timestamps, but not detailed target identifiers. To fully establish event-to-identity linkage, retain the event-detail view privately showing matching target user and group.

SCREENSHOT 4: Microsoft Entra group-management audit log

Date ↓	Service	Category	Activity	Status
10/15/26, 6:45:18 AM	Core Directory	GroupManagement	Remove member from g...	Success
10/15/26, 6:43:35 AM	Core Directory	GroupManagement	Add member to group	Success

8. Results and Security Interpretation

Control / result	Verified outcome
Membership policy simulation	Policy-inconsistent access was intentionally introduced for training
Analyst review and certification	Decision documented with simulated owner approval
Group remediation	Test membership removed; test user absent afterward
Audit telemetry	Successful add/remove operations visible in Entra audit log
Actual WayneHelpDesk access control	Not evaluated: placeholder application has no backend

Main lesson: access certification is evidence-based. It requires a known entitlement, business justification, accountable decision-maker, documented remediation, and verification. A group name or job title alone is not proof of effective access or a policy violation.

9. Portfolio Privacy and Publication Notes

All screenshots intended for publication must exclude tenant identifiers, object IDs, user principal names, personal email addresses, authentication artifacts, and unnecessary local information. Use irreversible opaque redaction. Explain clearly that identities, company policy, and reviewer sign-off were simulated while group-management operations and audit observations occurred in a personal lab tenant.

Suggested portfolio caption: “Manual Entra ID access-certification exercise demonstrating entitlement discovery, policy-based review, simulated owner approval, test-group membership removal, and audit-log validation.”

10. Follow-up Improvements

Potential next iteration: identify a real test resource enforcing group assignment; document an application owner; validate whether unassigned sign-in is possible; perform an owner-reviewed access matrix for every member; and export a sanitized certification evidence package. These improvements were not completed as part of this lab.