ENTERPRISE SECURITY ENGINEERING:
AUDIT RESULTS LEDGER (ARL)

Framework Baseline: ACPHF IAL v2.1
Audit Document Class: Standard Telemetry & Gate Verification Report

[SECTION 1: AUDIT EXECUTION METADATA]

Audit Tracking ID:	ARL-2026-0810-WORKLOAD-01
Execution Timestamp (UTC):	2026-08-10 19:55:27 UTC
Evaluating Auditor / AI Agent:	Steven Gary Tuschman / ACPHF-Agent-Core
Target Application (Client) ID:	d7e8f9a0-b1c2-d3e4-f5g6-h7i8j9k0l1m2
Target Tenant (Directory) ID:	8a1b2c3d-4e5f-6g7h-8i9j-0k1l2m3n4o5p
Target Asset Scope:	kv-acphf-prod-eus-01
Evaluated Subject Claim (sub):	repo:Compcode1/machine-identity-1:ref:refs/heads/main
Overall Compliance Outcome:	**[PASS]**

[SECTION 2: SYSTEM VALIDATOR & GATE AUDIT MATRIX]

[AUDIT GATE 1] Coordinate Check

Telemetry Target:	Inbound Tenant ID & Application (Client) ID mapping
Evaluated Log Source:	Entra ID Non-Interactive Sign-In Logs
Gate Verification Status:	**[PASS]**
Diagnostic Summary:	> Directory coordinates and Application ID match active tenant objects. No unmapped AppID routing errors detected.

[AUDIT GATE 2] Character Check

Telemetry Target:	Subject Claim string casing & OIDC trust handshake
Evaluated Log Source:	Sign-In Status & Error Codes (AADSTS70021 / AADSTS70022 / 500121)
Gate Verification Status:	**[PASS]**
Diagnostic Summary:	> Federated credential subject claim matches repository path character-for-character. OIDC handshake completed with Status: Success.

[AUDIT GATE 3] Clock Check

Telemetry Target:	Token volatility lifetime & re-authentication cadence (60-minute ceiling)
Evaluated Log Source:	Sign-In Timestamp Spacing & Session Lifecycles
Gate Verification Status:	**[PASS]**
Diagnostic Summary:	> Runner successfully initiates a fresh OIDC handshake upon execution. No script crashes or expired token faults observed during execution loops.

[AUDIT GATE 4] Plane Check

Telemetry Target:	Control-Plane vs. Data-Plane RBAC authorization ("Silent 403" audit)
Evaluated Log Source:	Log Analytics Workspace (AuditEvent / KeyVaultRequests)
Gate Verification Status:	**[PASS]**
Diagnostic Summary:	> Machine identity successfully authenticated and executed data-plane operations against target vault with 0 HTTP 403 Forbidden drops.

[SECTION 3: DATA-PLANE TRACING & AI INTENT DIRECTIVE LOG]

Audit Circumstance: Correlating OIDC federated token issuance with Key Vault data-plane access to detect unauthorized reads or clock skew outside execution windows.

AI Prompt Directive Executed:

> *"Inspect active Log Analytics workspace. Join ServicePrincipalSignInLogs for App ID d7e8f9a0... with Key Vault data-plane access logs (AuditEvent) for target vault kv-acphf-prod-eus-01 within a 5-minute time window. Group by 60-minute buckets to highlight any clock skew or HTTP 403 access denials."*

Dynamic Query Result Summary:

> Query executed against active schema; confirmed 100% correlation between token issuance and data-plane operations. Zero orphan events.

[SECTION 4: DEFECT LOG & REMEDIATION ACTION PLAN]

Evaluated Gate	Defect Detected	Root Cause Analysis	Corrective Action Required
Gate 1 (Coordinates)	None	[N/A]	[N/A]
Gate 2 (Characters)	None	[N/A]	[N/A]
Gate 3 (Clock)	None	[N/A]	[N/A]
Gate 4 (Plane)	None	[N/A]	[N/A]

Final Sign-Off:	Steven Gary Tuschman
Audit State Locked:	[YES]
Next Scheduled Review Date:	2026-11-10