SecureOps RiskScore 360

Security Assessment Report

Generated: 2026-01-04 02:23:08 UTC

Subscription: b6df8227-8888-4209-a122-e75503b5516e

Resource Group: legacyRG

1. Executive Summary

54

Risk Level: Critical

This report consolidates governance compliance (Azure Policy), identity governance (RBAC/IAM drift), and security posture signals (Defender for Cloud) into a normalized risk score to support prioritization.

2. Score Breakdown

Component	Value	Details
Policy Risk	0	16 unique non-compliant policies
IAM Risk	0	Drift: owner (Owners: 10, Contributors: 9)
Defender Risk	0	High: 0, Medium: 0
Total RiskScore	54	Level: Critical

3. Recommended Actions

1. Remediate 16 non-compliant Azure policies in resource group 'legacyRG'. Prioritize the most frequent policies listed in the appendix.
2. Review RBAC assignments to reduce privilege sprawl. Current: 10 Owners, 9 Contributors. Ensure each Owner role is justified.

Technical Appendix

A. Data Sources

Azure Policy: Microsoft.PolicyInsights policyStates (NonCompliant) at RG scope. IAM: Microsoft.Authorization roleAssignments at subscription scope. Defender: Microsoft.Security assessments (Unhealthy only) at RG scope.

B. Top Non-Compliant Policies

Policy Definition ID	Records
/providers/microsoft.authorizatio...4c3081-a854-4457-ae30-26a93ef643f9	6
/subscriptions/b6df8227-8888-4209.../policydefinitions/audit-owner-tag	4
/providers/microsoft.authorizatio...6962a6-4747-49cd-b67b-bf8b01975c4c	4
/subscriptions/b6df8227-8888-4209...olicydefinitions/enforce-owner-tag	4
/subscriptions/b6df8227-8888-4209...licydefinitions/audit-storage-diag	3

C. IAM Evidence

Drift classification: owner. Owners: 10, Contributors: 9. Sample principals with privileged roles:

Owner Principals (sample)

Principal ID	Type
246d6963-1c7a-4d45-860f-0fa9e9e4913d	User
ce2a45e3-6cec-4d92-9ebb-b52fec12c3b0	ServicePrincipal
5e7d13ff-89ce-484f-a9a9-b5281648ff49	ServicePrincipal
a4b09772-201e-417f-8221-aa80f77035f9	User
83c3b00a-7d0b-4d59-a5dc-8d09242f5bd7	User

Contributor Principals (sample)

Principal ID	Type
ce2a45e3-6cec-4d92-9ebb-b52fec12c3b0	ServicePrincipal
63121f61-e2be-4393-9a29-2b019c6dfe2e	ServicePrincipal
a5748043-2b88-4637-bb60-51c95be66b0e	ServicePrincipal
cc8e4cbe-1e4b-4ee4-934c-441c6df44d5f	ServicePrincipal
63121f61-e2be-4393-9a29-2b019c6dfe2e	ServicePrincipal

D. Scoring Methodology

- Policy Risk = min(60, unique_noncompliant_policies × 5)
- IAM Risk = 70 (Owner drift) | 40 (Contributor drift) | 0 (none)
- Defender Risk = (High × 30) + (Medium × 15)
- Final RiskScore = min(100, Policy Risk + IAM Risk + Defender Risk)

E. Notes & Limitations

Defender assessments may be 0 if Defender for Cloud is not enabled or fully initialized. IAM drift uses threshold-based classification and can be refined with organization-specific baselines and role justification processes.