

SecureOps RiskScore 360

Security Assessment Report

Generated: 2026-01-04 10:00:46 UTC
Subscription: b6df8227-8888-4209-a122-e75503b5516e
Resource Group: aoss-dev-rg-secops

1. Executive Summary

51

Risk Level: Critical

This report consolidates governance compliance (Azure Policy), identity governance (RBAC/IAM), Defender for Cloud posture, and selected exposure controls (network & encryption) into a normalized risk score to support remediation prioritization.

Top Risk Drivers:

- IAM: 35 points (critical)
- POLICY: 32 points (high)
- ENCRYPTION: 2 points (low)

2. Score Breakdown

Component	Value	Evidence (Real Inputs)
Policy	32	17 unique non-compliant policies
IAM	35	Drift: owner Owners: 10 Contributors: 9 Readers: 2
Defender	0	Unhealthy: High=0, Medium=0, Low=0
Network	0	Open risky ports: 0 Public IPs: 0 Missing NSG: 0
Encryption	2	Unencrypted storage: 0 Weak TLS: 0
Total (Normalized)	51	Raw: 69 / 135 Level: Critical

3. Recommended Actions (Prioritized)

1. Remediate 17 non-compliant Azure policies in RG 'aoss-dev-rg-secops'. Start with the highest-frequency policies listed in the appendix.
2. Reduce privileged sprawl: review RBAC assignments. Current counts -> Owners=10, Contributors=9. Keep Owner role for break-glass/admin accounts only.

Technical Appendix - Evidence & Methodology

A. Data Sources & Scope

Azure Policy: Microsoft.PolicyInsights policyStates (NonCompliant) at resource-group scope.
IAM/RBAC: Microsoft.Authorization roleAssignments at subscription scope. Defender for Cloud: Microsoft.Security assessments (Unhealthy only) at RG scope. Network: NSG rules, NIC protection, public IP exposure. Encryption: storage account encryption, TLS, and HTTPS enforcement.

B. Top Non-Compliant Policies (by records)

Policy Definition ID	Records
/providers/microsoft.authorization/policy...ions/e56962a6-4747-49cd-b67b-bf8b01975c4c	14
/providers/microsoft.authorization/policy...ions/404c3081-a854-4457-ae30-26a93ef643f9	10
/subscriptions/b6df8227-8888-4209-a122-e7...ization/policydefinitions/audit-owner-tag	9
/subscriptions/b6df8227-8888-4209-a122-e7...ation/policydefinitions/enforce-owner-tag	6
/providers/microsoft.authorization/policy...ions/1604f626-4d8d-4124-8bb8-b1e5f95562de	5
/subscriptions/b6df8227-8888-4209-a122-e7...tion/policydefinitions/audit-storage-diag	5
/providers/microsoft.authorization/policy...ions/6edd7eda-6dd8-40f7-810d-67160c639cd9	5
/providers/microsoft.authorization/policy...ions/fd9903f1-38c2-4d36-8e44-5c1c20c561e8	5
/providers/microsoft.authorization/policy...ions/8c6a50c6-9ffd-4ae7-986f-5fa6111f9a54	5
/providers/microsoft.authorization/policy...ions/db4f9b05-5ffd-4b34-b714-3c710dbb3fd6	5

C. IAM Evidence (samples)

Drift: owner. Owners=10, Contributors=9, Readers=2. Samples below.

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
966dc3e7-210a-4117-a638-75f2c27ddf53	User
ce6795c4-0294-4088-8fe2-2538ea58beb2	User
f27c8a13-a0b7-4414-a8cb-1f2966bfd42b	User

Contributor principals (sample)

Principal ID	Type
ce2a45e3-6cec-4d92-9ebb-b52fec12c3b0	ServicePrincipal
63121f61-e2be-4393-9a29-2b019c6dfe2e	ServicePrincipal

a5748043-2b88-4637-bb60-51c95be66b0e
cc8e4cbe-1e4b-4ee4-934c-441c6df44d5f
246d6963-1c7a-4d45-860f-0fa9e9e4913d
25f17dd1-197e-48ee-8a20-b3f5fedf8f17
83c3b00a-7d0b-4d59-a5dc-8d09242f5bd7

ServicePrincipal
ServicePrincipal
User
User
User

D. Scoring Methodology (Normalized)

- Each component produces a bounded sub-score: Policy(0-40), IAM(0-35), Defender(0-35), Network(0-15), Encryption(0-10).
- Raw total = sum(component scores). Max possible = 135.
- Final RiskScore = $\min(100, \text{round}((\text{RawTotal} / 135) \times 100))$.
- Risk Level thresholds: Low<10, Low-Medium<25, Medium<40, Medium-High<60, High<75, Critical \geq 75 (or critical component + score \geq 50).

E. Notes & Limitations

Defender counts may be 0 if Defender for Cloud is not enabled or not fully initialized. IAM drift is computed using threshold-based heuristics and should be tuned to organizational baselines. Network/encryption checks depend on RBAC permissions and available resources in the RG.