ACME AWS risk review — Q1 2026

Prepared 2026-04-02 12:14 UTC · 6 AWS accounts · 11 regions · 1,204 AWS resources in scope

TOTAL FINDINGS Q1	CRITICAL REMEDIATED	MEAN TTR (CRIT)	EXCEPTIONS ACTIVE
213	11	3.8d	6
-19%	+4	-1.2d	+1

Headline

AWS risk fell materially in Q1. Total findings dropped 19% quarter over quarter, with the biggest gains from closing the long-running bucket-policy audit in the data OU. Mean time to remediate a critical finding fell to 3.8 days, well inside the 7-day SLO. Two themes dominate what's left: drift in IAM policies after the payments launch, and a cluster of Performance Insights misconfigurations in RDS.

Findings by account

ACCOUNT	OPEN	CRITICAL / HIGH
acme-root (mgmt)	2	0 / 0
acme-prod-use1	14	1 / 3
acme-stage-use1	9	0 / 4
acme-data-usw2	8	0 / 1
acme-sandbox	6	0 / 0
acme-legacy-ops	3	1 / 0

Top three open critical items

1. Public READ on bronze bucket

Bucket acme-data-bronze-usw2 grants s3:GetObject to Principal: * on the /static/ prefix. Owner: data-eng. Target closure: April 20. Remediation: restrict prefix to the CloudFront OAI or switch to a dedicated public assets bucket.

2. Rotated IAM root access key on legacy-ops

Access key AKIA…XWPZ last used 4 days ago. Remediation started; new workload identity with IRSA is deployed. Expected closure April 22 after traffic is confirmed shifted.

3. stage Aurora accepts 0.0.0.0/0 on 5432

Security group sg-0a33… on acme-stage-aurora. Blocked externally by WAF but still a defense-in-depth issue. Owner: platform. Closure April 25.

Exceptions

Six exceptions are active. All have owners and expiry dates. The oldest expires in 8 days (port-scanner-allowlist on audit-usw2) — data-sec has acknowledged and will decide on renewal by April 23.

Recommendations for Q2

1. Turn on Performance Insights on the remaining two RDS clusters; cost is under $10/mo each.
2. Move the acme-legacy-ops account onto Identity Center; eliminate long-lived access keys.
3. Introduce an SCP that denies s3:PutBucketPublicAccessBlock outside the sandbox OU.