WELL-ARCHITECTED · DIAGNOSTIC DELIVERABLE

AWS Well-Architected Review · Final Report — SAMPLE

6-pillar review · HRI / MRI / LRI classification

Client	Empresa Anônima S.A.
Engagement ID	#ANV-WA-2604-0428
Period	Q2 2026 · April 06 – May 04, 2026
Issued by	Anuvia · Mila Vernazza, Principal Consultant
Classification	SAMPLE · Confidential · Not for distribution

This document is a sample preview of an Anuvia diagnostic deliverable. All figures, customer names, and findings are illustrative and anonymized. No real-client data is contained within.

anuvia.com.br · contato@anuvia.com.br

SCORECARD

6-Pillar Scorecard

Scores are calibrated on a 0–10 scale derived from the AWS Well-Architected Tool (85 questions across 6 pillars) and verified by direct evidence review. Aggregate posture: **6.0 / 10** — "Solid foundation, security & sustainability gap".

Risk inventory

Severity	Count	Definition
HRI · High Risk	7	Could plausibly cause outage, data loss, or compliance breach within 90 days.
MRI · Medium Risk	14	Material posture gap; should be remediated in current quarter.
LRI · Low Risk	23	Polish / hygiene items; bundle into normal backlog.

PILLAR · 02 / 06

Security — 5 / 10

Strongest gap. AWS-native foundations are partially deployed (GuardDuty in 3/4 accounts, Security Hub disabled, Config rules sparse) and the IAM blast radius is wider than warranted by the team's role model.

Findings

#	Finding	Severity	Effort
SEC-01	Root-account MFA missing on payer account	HRI	S
SEC-02	GuardDuty disabled in 1 of 4 accounts (acct-dev)	HRI	S
SEC-03	Security Hub not enabled · no central findings aggregation	HRI	M
SEC-04	23 IAM users with console access · should be SSO/IdC	HRI	M
SEC-05	S3 public access block not enforced at org level (SCP missing)	HRI	S
SEC-06	Secrets in environment variables (ECS task defs) · 11 instances	MRI	M
SEC-07	KMS key rotation disabled on 6 CMKs holding customer PII	MRI	S
SEC-08	VPC Flow Logs not enabled on 2 of 7 production VPCs	MRI	S
SEC-09	IAM Access Analyzer not enabled in any account	MRI	S
SEC-10	Inline IAM policies on 47 roles · drift risk	LRI	M

PILLAR · 03 / 06

Reliability — 6 / 10

Single-AZ deployment on the primary OLTP database is the dominant risk; failure modes during simulated AZ degradation were not exercised in the last 12 months.

Findings

#	Finding	Severity	Effort
REL-01	Primary RDS cluster Single-AZ · no automated failover	HRI	M
REL-02	No documented RTO/RPO targets per service	HRI	M
REL-03	Backups not periodically restore-tested (last test: 14 mo ago)	HRI	M
REL-04	ALB health checks too tolerant · 60s threshold	MRI	S
REL-05	No chaos / game-day program · no AZ-failure rehearsal	MRI	L
REL-06	Stateless services pinned to single AZ ASG	MRI	S
REL-07	Critical Lambda DLQ unconfigured on 8 functions	MRI	S
REL-08	No multi-region DR target (RTO ill-defined)	LRI	L

Recommended sequence: REL-01 (Multi-AZ enablement) is gated only on a brief failover window — see ADR on page 9. REL-03 should be paired with REL-08 in a single quarterly DR exercise.

PILLAR · 05 / 06

Cost Optimization — 6 / 10

Spend governance is partially mature: cost allocation tags exist but coverage is 64%. RI/SP coverage is mid-range. Detailed FinOps audit recommended (see linked engagement ANV-AUDIT for separate deliverable).

Findings

#	Finding	Severity	Effort
COST-01	Tag coverage at 64% · billing allocation gaps	HRI	M
COST-02	No budget alerts on 2 of 4 accounts	MRI	S
COST-03	RI/SP coverage at 41% (target: 70-80%)	MRI	M
COST-04	84 idle EBS volumes · R$ 18.9k/yr waste	MRI	S
COST-05	S3 lifecycle missing on 12 buckets	LRI	S
COST-06	Cross-AZ chatter on RDS replica · R$ 6k/yr egress	LRI	M

PILLARS · 01, 04, 06 / 06

Operational Excellence · Performance · Sustainability

Operational Excellence — 7/10

- Strong runbook coverage on top-5 services; 4 critical services without runbooks (OPS-01).
- Post-mortems written for 9 of 14 incidents in last 12 months · culture is forming.
- IaC coverage at 78% (Terraform) · 22% click-ops residual mostly in legacy networking.

Performance Efficiency — 8/10

- Strong. Right-instance-type discipline. Some latency budget over-provisioning detected.
- Caching layer (Redis) under-utilized — 22% of hit-eligible queries bypass.
- GP3 EBS adoption complete; gp2 fully retired.

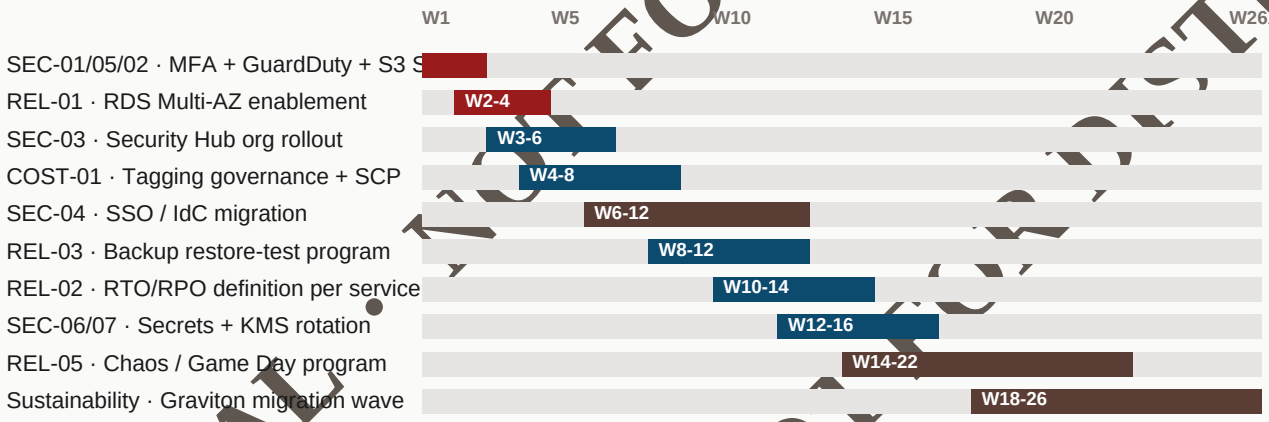
Sustainability — 4/10

- No carbon dashboard reviewed; AWS Customer Carbon Footprint Tool not consulted.
- Graviton (ARM64) adoption at 6% across compute fleet · target 50% within 12 months.
- No data-lifecycle policy → cold data persists in high-energy storage tiers.

REMEDIATION ROADMAP

Sequenced by blast radius

Priority order is determined by (1) failure-mode severity in the next 90 days, (2) regulatory exposure, (3) cross-team dependency depth. Quick wins first; multi-team changes (Transit Gateway, SSO migration) staged after foundations.



REMEDIATION ROADMAP · TARGETS

Post-roadmap target posture

Pillar	Current	Target (6 mo)	Target (12 mo)
Operational Excellence	7	8	9
Security	5	7	8
Reliability	6	7	8
Performance Efficiency	8	8	9
Cost Optimization	6	8	8
Sustainability	4	6	7
Aggregate	6.0	7.3	8.2

Sequencing rationale

- Weeks 1-4 close all open HRIs whose cost is low ("free" risk reduction).
- Weeks 5-12 attack identity & data perimeter — these unblock downstream cost work.
- Weeks 13-26 invest in the long-cycle structural items (SSO, chaos, Graviton).

ARCHITECTURE DECISION RECORD

ADR-WA-003 · Multi-AZ database failover strategy

Status	Accepted · 2026-04-29
Date	2026-04-29
Authors	Anuvia Cloud Practice + Empresa Anônima Eng. Lead
Pillar	Reliability · REL-01
Severity addressed	HRI
Context	Primary production OLTP cluster is Single-AZ (db.r6g.4xlarge). AZ-level outage would result in
Considered options	A) Multi-AZ deployment (synchronous replica, automated failover) — adds ~38% to RDS spen
Decision	Adopt option A: Multi-AZ deployment for primary cluster. Schedule a 45-minute controlled failo
Consequences	+ RTO reduces from 90 min to ≤2 min · meets business target. + RPO reduces from ~15 r
Validation criteria	1. Successful failover dry-run within 90 sec. 2. CloudWatch alarm fires within 30 sec of AZ

APPENDIX · METHODOLOGY & REFERENCES

Methodology

This review follows the AWS Well-Architected Framework (April 2026 revision). Each of the 85 questions across the 6 pillars was evaluated against direct evidence (IaC source, AWS Config, CloudTrail, runbook artifacts) rather than self-attestation. Findings are classified per the AWS WA Tool risk taxonomy: HRI (High Risk Issue), MRI (Medium Risk Issue), LRI (Low Risk Issue).

Evidence sources

- AWS Config aggregator export · 4 accounts · 2026-04-12
- CloudTrail event lake · 90-day window prior to engagement start
- Terraform repo audit · git log analysis · 12-month window
- Incident retrospective archive · 14 post-mortems reviewed
- Interviews · 9 engineers across platform, app, and security teams (6 hr total)

References

- AWS Well-Architected Framework · docs.aws.amazon.com/wellarchitected
- AWS Foundational Security Best Practices (Security Hub standard)
- AWS Resilience Hub · application resiliency policies
- AWS Customer Carbon Footprint Tool · 12-month emissions baseline

— End of report — Anuvia · contato@anuvia.com.br · anuvia.com.br