CONSULTING REPORT

Acme Pty Ltd – Engineering Review

PREPARED

May 28, 2025

REFERENCE

DOC-1

CLASSIFICATION

Confidential

1.0 Program Overview

The platform engineering group continues to focus on stabilising the build pipeline and enabling faster feature delivery.

This report summarises the current state of delivery health, major milestones, and the engineering risks being tracked through the next quarter.

1.1 Milestone Status

- CI/CD consolidation is 80% complete with remaining teams migrating during April.
- Service Level Objectives for the data ingestion tier have been drafted and are undergoing stakeholder review.
- The observability refresh shipped a new Grafana baseline with production adoption scheduled next sprint.

1.2 Risks and Mitigations

Vendor lead times for load-testing infrastructure remain longer than planned. Procurement has opened an expedited order and the SRE team prepared a contingency plan using internal hardware.

Security review of the multi-region ingress controller is pending. The architecture guild has scheduled a focused workshop to burn down the outstanding actions.

1.2.1 Deployment Readiness Metrics

Release frequency is averaging two production pushes per week, up 35% quarter-over-quarter. Mean Time to Restore across critical services is stable at 24 minutes with further automation identified around rollback tooling.

2.0 Executive Summary

This security assessment identified several areas requiring attention across authentication, data protection, and network security.

While no critical vulnerabilities were discovered, the findings outlined below should be addressed to maintain a strong security posture.

2.1 Critical Findings

FIND-001: Insecure API Key Storage

API keys are currently stored in environment variables without encryption at rest. Recommendation: Implement a secrets management solution such as HashiCorp Vault or AWS Secrets Manager.

FIND-002: Missing Rate Limiting

Public-facing endpoints lack rate limiting, exposing the application to potential brute-force attacks. Recommendation: Implement rate limiting middleware with configurable thresholds per endpoint.

2.2 Medium Priority Findings

- Session tokens do not include secure flags in all environments
- Logging configuration may expose sensitive data in error messages
- Dependency scanning revealed outdated packages with known CVEs

3.0 Strategic Recommendations

Based on the findings from this assessment, the following recommendations are provided to strengthen the security posture and operational resilience of the platform.

3.1 Short-term Actions

1. Implement secrets management solution within 30 days
2. Deploy rate limiting to all public endpoints
3. Update dependencies with critical CVEs
4. Enable secure flags on all session tokens

3.2 Long-term Initiatives

1. Establish a regular security review cadence
2. Implement automated dependency scanning in CI/CD
3. Conduct quarterly penetration testing
4. Develop incident response playbooks

4.0 Glossary

CVE: Common Vulnerabilities and Exposures

SLO: Service Level Objective

MTTR: Mean Time to Restore

CI/CD: Continuous Integration and Continuous Deployment

5.0 References

- OWASP Top 10 (2021)
- NIST Cybersecurity Framework
- ISO/IEC 27001:2022
- AWS Well-Architected Framework