

# ForgeTrace Executive Summary

ForgeTrace Client • Not Specified

## Engagement Details

- **Prepared By:** Peter Kolawole, BAMG Studio LLC
- **Generated:** 2025-11-08 08:32 UTC
- **Primary Contact:** peter@beaconagile.net
- **Classification:** Confidential - M&A Audit Report

## Recommendation

KEEP

No material blockers identified; continue routine IP hygiene checks.

## Negotiation Watchlist

- No material blockers detected; maintain watchlist as new code lands.

## Engagement Scope

ForgeTrace executed automated scanners and manual analytics to surface provenance, license, and security risks.

- Source code, licenses, and dependency manifests supplied in audit bundle.
- Historical git metadata (authors, churn, timeline).
- ForgeTrace scanners across secrets, SAST, similarity, and licenses.

# Narrative Highlights

## Executive Lens

- Recommendation: Keep — No material blockers identified; continue routine IP hygiene checks..
- IP composition is 0.0% foreground and 0.0% third-party across 2 audited components.
- No high-risk licenses surfaced across sampled manifests.
- Dependency scan cleared noise-floor filters; no actionable vulnerabilities in scope.
- Security, similarity, and dependency scanners reported a clean baseline.

## Board Lens

- Foreground ownership at 0.0% signals clear provenance; 0.0% external footprint requires contract alignment.
- No clean-room blockers identified in this pass; keep hygiene checks active.
- Dependency risk nominal; OSV noise filters suppressed all non-actionable hits.
- Risk snapshot: 0 open findings, primary theme is none dependencies exposure.

## Engineering Lens

- Average rewriteability score: 0.00. Focus on 0 low-score modules for isolation.
- Vulnerability queue: 0 items (noise rejection 0.0%). Patch highest-weight findings (0.00 avg score).
- Secrets + SAST backlog totals 0 items. Prioritise rotation and triage workflows next sprint.
- License scan flagged 0 reciprocal obligations; confirm NOTICE files before pushing release builds.
- Vulnerability coverage: OSV, GitHub Advisory, OWASP Dependency-Check.

## Key Performance Indicators

OPEN VULNERABILITIES  
**0**

VULN DENSITY  
**0.0%**

WEIGHTED VULN SCORE  
**0.00**

FOREGROUND LOC  
**0**

BACKGROUND LOC  
**0**

THIRD-PARTY COMPONENTS  
**2**

## HIGH-RISK LICENSES

0

## IP Composition

Origin	Files	Share
unknown	0	0.0%

## Third-Party Snapshot

- Detected 2 package entries across 1 manifest.
- python ecosystem represents 2 components in scope.

## Top Packages

- pyyaml (1 reference)
- requests (1 reference)

## Risk Overview

Area	Findings	Severity	Notes
Dependencies	0	NONE	Noise filters cleared the OSV backlog.
Secrets	0	NONE	No hardcoded secrets detected.
SAST	0	NONE	Static analysis returned no actionable findings.
Similarity	0	LOW	No significant code duplication detected beyond thresholds.

## Primary Signals

Total Open Items: 0  
Key Theme: No material risks flagged in this pass

## Duplicate Hotspots

File A	File B	Similarity
-	-	0.00

# Rewriteability Outlook

AVERAGE SCORE  
**0.00**

LOW SCORE FOREGROUND  
**0**

CLEAN-ROOM CANDIDATES  
**0**

## Recommendations

- No critical rewrite blockers detected; maintain periodic reassessment alongside refactors.

## Priority Modules

No critical modules identified.

## Playbook

- Document clean-room brief per high priority module.
- Assign independent implementers for guarded rewrites.
- Track escrow-ready deliverables with counsel oversight.

## Quadrant View

### Easy/Low-risk

- No modules identified

### Easy/High-risk

- No modules identified

### **Hard/Low-risk**

- No modules identified

### **Hard/High-risk**

- No modules identified

## **IP Composition**

### **Origin Share**

**Foreground:** 0%

**Background:** 0%

**Third-party:** 0%

### **Top Modules Requiring Attention**

Module	Origin	Rewriteable	Score	LOC
No modules analysed	-	-	0.00	0

## **License and Compliance**

### **Heatmap**

	Foreground	Background	Third-party
Permissive	0	0	0
Weak Copyleft	0	0	0
Strong Copyleft	0	0	0

### **High-Risk Identifiers**

No GPL-family or reciprocal licenses detected.

### **License Summary**

License	Count	Files
None Detected	0	

## Required Actions

### Obligations

- Ensure SPDX attributions accompany third-party packages in outbound deliverables.
- Track dependency provenance in data rooms alongside SBOM exports.
- Confirm permissive-license notices remain within corporate policy thresholds.

### Counsel Follow-Ups

- Review updated SBOM with legal counsel before diligence disclosures.

## Provenance Insights

### Summary

Sample User leads with 1 commits across 3 files.

**Commit Window:** 2025-11-08

### Commit Activity (Weekly)

Peak weekly commits: 1

### Milestones

- Initial commit observed 2025-11-08.

### Signals

- Net code delta for lead contributor: +16 lines.

### Deliverables

- Executive summary narrative (PDF/HTML).
- Machine-readable SBOM extracts (JSON).
- Risk, license, and rewriteability analytics.

# Similarity and Background IP

## Signals

- 0 similarity pairs exceeded diligence threshold.
- No public code matches surfaced in this pass.

## Public Matches

No public code overlaps were surfaced in this pass.

## Duplicate Highlights

File A	File B	Similarity
-	-	0.00

## Policy Engine Outcomes

BLOCK  
**0**

WARN  
**0**

INFO  
**0**

No policy violations were triggered.

## Recommended Next Steps

1. Maintain continuous SBOM updates as dependencies evolve across sprints.

---

Prepared for ForgeTrace Client by Peter Kolawole, BAMG Studio LLC (peter@beaconagile.net).

Generated 2025-11-08 08:32 UTC. Confidential analysis – coordinate with counsel before disclosure.