SAMPLE REPORT — illustrative only. The target company, codebase metrics, and findings below are a fictional composite for demonstration purposes and do not describe any real company or engagement. A live engagement is generated directly from access to the target's actual repository.



# Technical Due Diligence Report

Full Technical Diligence (T2) · Sample Report · Prepared for Deal Team Review

| TARGET (REDACTED) | SECTOR | CODEBASE SIZE |
|---|---|---|
| **Project Meridian** | **B2B vertical SaaS** | **~86,000 LOC** |
| PRIMARY STACK | REPOSITORIES SCANNED | REPORT TIER |
| **Node.js / React / PostgreSQL** | **4** | **T2 — Full Diligence** |

## 01 Executive Summary

OVERALL RISK RATING

**MODERATE**

| 3 | $185K–$260K | 6–9 mo |
|---|---|---|
| Critical findings | Est. remediation cost | Engineer-months to remediate |

Project Meridian's codebase is in line with what we'd expect from a company at this stage — functional, revenue-generating, and not architecturally broken — but carries three findings that should factor into deal terms: an unpatched critical CVE in a payment-adjacent dependency, concentrated ownership of the billing module in a single engineer, and a database schema that will need rework before the growth case in the model is reachable. None of these are deal-breakers on their own; together they represent a quantifiable body of post-close work that is not currently reflected in the asking price.

**Recommendation:** Proceed, with $185K–$260K in remediation costs and a 60-day talent retention plan for the lead payments engineer factored into deal terms or a post-close holdback.

## 02 Security Exposure

Risk rating: **HIGH** — driven primarily by finding S-1. Full scan covered 4 repositories, 212 dependencies, and CI/CD configuration.

| SEVERITY | FINDING | EST. FIX EFFORT |
|---|---|---|

| | | |
|---|---|---|
| Critical | **Unpatched critical CVE in payment webhook dependency**<br>A transitive dependency used in the Stripe webhook handler has a known critical-severity CVE (remote code execution), unpatched for 14 months. Direct exposure on a payment-adjacent code path. | 3–5 days |
| High | **No rate limiting on authentication endpoints**<br>Login and password-reset endpoints have no throttling, enabling credential-stuffing and account-enumeration attacks at scale. | 1–2 days |
| High | **Long-lived AWS credentials in CI configuration history**<br>A prior commit exposed static AWS keys in CI config; keys have since been rotated but exposure window and blast radius were not previously assessed. | 1 day + IAM audit |
| Medium | **Inconsistent tenant-scoping on 3 internal admin endpoints**<br>Three internal-only admin routes do not re-verify organization scope server-side, relying on client-side checks. | 2–3 days |
| Low | **11 dependencies with known low/medium-severity CVEs**<br>Standard patch-cadence backlog — no direct exploit path identified in this codebase. | 2 days |

## 03 Technical Debt

Debt is concentrated in two legacy subsystems rather than spread evenly — the newer product surface (roughly 70% of the codebase, shipped in the last 18 months) is in good health.

| SEVERITY | FINDING | EST. FIX EFFORT |
|---|---|---|
| High | **Billing module: 42% branch coverage, no integration tests on refund path**<br>The module handling proration and refunds — directly revenue-relevant — has meaningfully lower test coverage than the rest of the codebase (team avg. 78%). | 4–6 weeks |
| Medium | **Legacy jQuery admin panel maintained in parallel with the React app**<br>~9,000 LOC of pre-2021 admin tooling still in active use; no clean migration path currently scheduled. | 6–8 weeks |
| Medium | **Duplicated invoicing logic across API and background-job layers**<br>Two independent implementations of tax calculation have drifted; one was patched for a EU VAT edge case, the other was not. | 1–2 weeks |
| Flag | **No dependency-update process; 34 packages >18 months out of date**<br>Not urgent individually, but raises the cost and risk of any future major-version migration. | Ongoing |

## 04 Talent Concentration Risk

Risk rating: **HIGH** on one subsystem; low elsewhere.

> **68% of commits** to the billing/payments module in the trailing 12 months came from a single engineer, who — per the data room — is not identified as part of the post-close retention plan. Bus-factor on this module is effectively 1. The remaining codebase shows healthy distribution across a 6-person engineering team, with no single contributor exceeding 24% of commits in any other module.

**Recommendation:** Structure a retention incentive or a minimum 60-day transition/consulting period for this engineer as a condition of close, and budget knowledge-transfer documentation as part of the technical debt line item above.

## 05 Architecture & Scalability

Rating: **Will hold through Series B growth assumptions in the model; re-architecture required before Series C scale.**

- Current PostgreSQL schema uses a single-tenant-per-row multi-tenancy model that begins to show query latency degradation past ~2M active end-users in comparable deployments — the growth case in the model reaches this range in year 3.
- No read-replica or caching layer currently in front of the primary database for the highest-traffic endpoints; straightforward to add, not yet done.
- Background job processing is on a single-queue, single-worker-pool design; adequate today, a known constraint if transaction volume grows as projected.

## 06 Remediation Cost Estimate

| LINE ITEM | EST. COST | ENGINEER-TIME |
|---|---|---|
| Security findings (S-1 through S-5) | $25,000 – $35,000 | 2–3 weeks |
| Billing module test coverage & refund-path hardening | $60,000 – $85,000 | 4–6 weeks |
| Legacy admin panel migration | $70,000 – $95,000 | 6–8 weeks |
| Invoicing logic consolidation | $15,000 – $25,000 | 1–2 weeks |
| Talent transition / knowledge-transfer plan | $15,000 – $20,000 | Concurrent |
| **Total** | **$185,000 – $260,000** | **6–9 engineer-months** |

Cost estimates assume a blended fully-loaded engineer rate consistent with the target's existing team composition and geography, not a premium consulting rate.

## 07 Methodology

Generated by audit/bench's LLM-plus-static-analysis review engine against the target's repositories, dependency manifests, and CI/CD configuration, with findings reviewed for business relevance before inclusion. This sample uses anonymized, fictionalized data for illustration; a live engagement report is built directly from access to the target's actual codebase under NDA.