# M&A IT Due Diligence Playbook for SaaS Acquirers

Erik Jones April 23, 2026

## Executive Summary

Technical due diligence is the difference between buying a company and buying a company plus an unexpected $2M post-close infrastructure rebuild. Most SaaS acquisitions get a generalist diligence review (compliance frameworks listed, certifications confirmed) without any engineer actually examining the AWS account, the IAM hygiene, or the on-call burden. This playbook describes the diligence dimensions that matter, how to categorize findings by deal impact, and how to scope remediation pricing that survives the post-close reality.

# Why Engineering-Led Diligence Matters

The SaaS acquirer who skips technical diligence inherits an unknown set of risks. The acquirer who runs **engineering-led diligence** turns those unknowns into priced line items: "the IAM hygiene cleanup is 6 weeks of engineering time at ~$80K, the SOC 2 program needs a fresh Type II at ~$150K, the Postgres major version is 4 versions behind and needs a 3-week migration project at ~$60K." That changes the deal economics — sometimes the purchase price renegotiation, often the year-1 integration plan.

The depth of diligence required scales with the acquisition profile. A $5M acqui-hire of a 5-person team needs less rigor than a $50M strategic acquisition. PE-backed buy-and-build platforms running 10+ acquisitions per year need a repeatable playbook; one-off strategic buyers need a deep engagement on a single deal.

# Diligence Dimensions

## Infrastructure and architecture

> **AWS / Azure / GCP account audit:** Account hierarchy, IAM hygiene, networking architecture (VPCs, peering, Transit Gateway), data tier (RDS, Aurora, S3), observability stack

**Deployment pipeline:** CI/CD tooling, infrastructure-as-code coverage, deployment cadence, change-management discipline

**Technical debt:** Database major-version lag, deprecated runtimes (Python 2, Node 14, etc.), end-of-life dependencies, custom infrastructure that should be managed services

## Security posture

**IAM and identity:** Root account MFA, IAM Identity Center / Okta SSO, service account inventory, secrets management discipline

**Vulnerability management:** Scan history, remediation cadence, exposure reports

**Penetration test history:** Recent reports, scope, finding-to-remediation cycle time

**Incident history:** Past 12 months — incidents, root causes, remediations, customer notifications

## Compliance status

**SOC 2 reports:** Type I / Type II coverage, exception list, auditor's testing notes (not just the cover letter)

**HIPAA / PCI DSS / ISO 27001:** Scope, evidence quality, gaps to clean certification

**Vendor risk register:** BAAs, DPAs, subprocessor flow-down language, last-review dates

### Operational maturity

**SLOs and reliability:** Defined customer-facing SLOs, actual MTTR, on-call rotation health

**Runbook discipline:** Top-20 runbooks documented, exercised in last 6 months

**Key-person risk:** Bus-factor on critical infrastructure, hiring pipeline, single-point-of-failure individuals

## Finding Categorization

Findings categorized by deal impact:

**Deal-impacting:** Issues that materially affect purchase price or deal terms. Open SOC 2 exceptions, unresolved security incidents, key-person risk on irreplaceable engineers.

**Fix pre-close:** Issues the seller should remediate before closing. Root MFA, exposed credentials, IAM access reviews more than 12 months stale.

**Fix year-1:** Issues to address in the first year of integration. Database upgrades, deprecated runtimes, technical-debt paydown.

**Informational / out-of-scope:** Things noted but not actioned in this engagement.

### Remediation cost ranges

Each finding gets a cost range scoped to the actual systems we examined, not generic ballparks. Engineering hours estimated based on the team's actual deployment cadence and capacity. Vendor costs (e.g., a fresh SOC 2 Type II audit) priced from current engagement experience. The acquirer uses these numbers in negotiation; the seller uses them in pre-close remediation.

## Common Pitfalls

**Generalist diligence depth:** "We confirmed they have SOC 2" is not diligence. Diligence is reading the auditor's testing notes, the exception list, and the remediation status.

**No remediation pricing:** Findings without cost ranges are useless to deal teams. Acquirers can't negotiate; sellers can't pre-remediate.

**Diligence team that disappears at close:** Different firm runs the integration, knowledge is lost, the year-1 plan ignores half the diligence findings. Solution: same team across diligence and integration when possible.

**Only one perspective:** Tech-only diligence misses operational risk; operational-only misses architectural debt. Cover all four dimensions or accept the risk of what you skipped.

**Rushing under LOI pressure:** 5-day diligence engagements scope down — focus on highest-risk areas — rather than compromise depth. Better to know less, well, than to skim everything.

## Outcomes

**Two-week standard turnaround** from data-room access to written report

**Findings categorized** by deal-impacting / fix-pre-close / year-1 / informational

**Remediation cost ranges** on every finding, scoped to actual systems

**Live readout** with deal team and Q&A; written report supports purchase price negotiation

**Optional follow-on integration scope** if deal proceeds — same team across diligence and execution

## How Jacobian Helps

Diligence reviewers are senior SREs and security engineers who operate equivalent systems daily — they know what looks normal, what looks debt, and what looks like a six-figure post-close surprise. Findings come with remediation cost ranges that hold up under negotiation. And because we can run the post-close integration ourselves, the year-1 plan reflects the actual diligence findings rather than a different firm's reinterpretation.

## Resource Details

Author: Erik Jones

Published: April 23, 2026

Categories:

M&A Operations SaaS

## Download

## Full Document

## About This Resource

A practical IT and security due-diligence playbook for SaaS acquisitions — what to examine, how to categorize findings, and how to scope remediation pricing that holds up at deal close.

Categories:

M&A Operations SaaS