

A title company's owner could already see where AI would take load off the team. **What was missing was a safe way to do it.**

The Challenge

Title work runs on handoffs. An order moves from entry to search and exam to processing and closing, and at each step someone rekeys data from a PDF or from one system into another.

A title company also handles wire instructions and buyers' Social Security numbers every day. One careless paste into the wrong tool turns a time savings into a disclosure problem. The goal was to move fast with someone watching the guardrails.

In IBM's research, **65%** of shadow AI incidents compromised customers' personal data, compared with 53% across all breaches.¹

The Solution

MSI recommended a business-tier AI platform the company owned, with the owner leading the build and MSI owning the governance. A monthly working cadence replaced a one-time project: each meeting ends with homework, and the next starts from what was built.

MSI reviewed the Claude Team settings, mapped the first automation candidates, and set up single sign-on and the Microsoft 365 connector. When the connector failed, MSI confirmed the tenant was right, traced the fault to the vendor's side, and escalated it.

Data rules came before rollout: no wire instructions in AI tools, PII redacted before processing, and six months of human review on every automation after go-live.

Engagement Snapshot

CLIENT	Title & Closing Company
INDUSTRY	Title & Real Estate Closing
RELATIONSHIP	Monthly AI Strategy Program
DELIVERED IN	About 2 Months

By the Numbers

9 working Claude projects within about two months of the first AI meeting.

65% of shadow AI incidents compromised customers' personal data, vs. 53% across all breaches.¹

The Results

About two months in, the company had nine working Claude projects, a closing-software data extractor, a closing-package parser, and a 15-page workflow map that is now the automation backlog.

"If your team's best automation ideas still live in one person's head, MSI's monthly AI program gets them written down and running under rules you can defend."

¹ IBM, Cost of a Data Breach Report 2025, research conducted by Ponemon Institute; IBM press release, July 30, 2025.