MANATECH

RESEARCH REPORT

# Briefing Document: The 2026 State of Agentic AI for SMBs

## Executive Summary

As of mid-2026, AI agents have transitioned from experimental chat interfaces to core business infrastructure. For small and medium business (SMB) founders and operators, the launch of **Claude for Small Business** and specialized connectors for platforms like **QuickBooks, HubSpot, and PayPal** marks a shift from "augmentation" (AI as a helper) to "automation" (AI as a delegated worker).

Current data indicates that 80% of organizations already report measurable economic returns from AI agents. However, a significant "governance gap" exists: while 91% of organizations use AI agents, 44% operate without formal governance. This document outlines the practical decisions required to deploy these tools effectively, manage connector limitations, and determine when to move from off-the-shelf tools to custom systems.

---

## Analysis of Key Themes

### 1. Practical Workflow Automation: "Off-the-Shelf" Agentic Workflows

The 2026 release of Claude for Small Business introduces 15 "ready-to-run" agentic workflows designed to handle high-volume, repetitive tasks that typically consume founder time.

- **Financial Operations:** Automating payroll planning by reconciling QuickBooks cash positions against PayPal settlements and generating 30-day forecasts.
- **Month-End Closing:** AI-driven reconciliation that flags discrepancies, generates plain-English P&L statements, and prepares "close packets" for accountants.
- **Sales & Marketing:** Triaging leads in HubSpot, analyzing campaign performance, and generating creative assets in Canva based on revenue gaps.
- **Administrative Tasks:** Automated invoice chasing, contract reviewing, and document classification.

### 2. Connector Mechanics and Limitations

Connectors allow Claude to "read" and "write" within your existing software stack. Understanding their limits is critical for operational stability.

| Tool | Key Capabilities | Critical Limits/Notes |
|---|---|---|
| **QuickBooks** | Real-time P&L, cash flow reports, transaction importing, and industry benchmarking. | Data is accessed securely and **not** used to train models. Discrepancies should be verified in QuickBooks first. |
| **HubSpot** | Create/update CRM records, log activities/notes, and visualize engagement trends. | **Bulk Limit:** Can only create/update 10 records at a time. Custom validation rules are not applied via the connector. |
| **PayPal** | "Agent Ready" payments and "Store Sync" for product catalogs. | Designed for "Agentic Commerce"—allowing AI agents to shop and buy on behalf of customers. |
| **Google/MS 365** | Document analysis, email drafting, and calendar management. | Supports "Always available" expert guidance for non-technical founders. |

### 3. Security, Identity, and Governance

The rise of "Shadow AI"—where agents are deployed without oversight—poses a major risk. SMBs must treat AI agents as **Non-Human Identities** requiring a consistent framework for authentication and authorization.

- **Human-in-the-Loop (HITL):** Critical for high-stakes actions like sending $100k+ proposals or paying invoices. Systems like Okta use "Async Auth" (push notifications to a founder's phone) to approve an agent's proposed action.
- **Agent Registry:** Organizations must maintain a registry identifying who owns an agent, what data it can access, and its specific purpose.
- **Universal Logout:** A necessary "kill switch" to immediately revoke all agent access across every system if a threat is detected.

### 4. ROI and the "Context Bottleneck"

Strategic value in 2026 is driven by **Context Length**. Research shows that for every 1% increase in input context (the data you give the AI), output quality increases by 0.38%.

- **ROI Drivers:** 44% of organizations see ROI via faster task completion; 32% via direct cost savings/reduced operating expenses.
- **The Bottleneck:** Siloed or fragmented data prevents agents from executing complex tasks. Data modernization is often a prerequisite for high-impact AI adoption.

---

## Important Quotes with Context

> ***"Small businesses... adoption of AI has lagged behind larger enterprises... their use often stops at the chat window. Claude for Small Business is a toggle install that puts Claude to work inside the tools owners already use."*** *— Daniela Amodei, Co-founder and President of Anthropic*

- **Context:** Explaining the rationale for moving AI from a separate browser tab directly into QuickBooks and HubSpot to "close the gap" between SMBs and large enterprises.

> ***"The ROI ceiling isn't set by the technology—it's set by the willingness to redistribute authority, redesign workflows, and trust intelligent systems with consequential decisions."*** *— Alex Holt, Vice Chair, Accenture*

- **Context:** Highlighting that the primary barrier to ROI in 2026 is no longer model capability, but organizational change management.

> ***"What we used to think were the constraints are just not constraints anymore. It's empowering. Hours of looking at stuff that doesn't matter are gone."*** *— Mike Beckham, CEO, Simple Modern*

- **Context:** A founder's perspective on how agentic workflows remove "tedious clerical work," allowing for a focus on value-add tasks.

---

## Actionable Insights for NZ SMB Founders

### When to Build Custom vs. Buy Off-the-Shelf

- **Buy (Off-the-Shelf):** Use for standard workflows (QuickBooks reconciliation, HubSpot lead triaging). These are low-cost, fast to deploy, but lack deep customization.
- **Hybrid Approach:** The most common model in 2026. Use pre-built connectors for 80% of the work and use APIs to build custom "skills" for your unique proprietary processes.
- **Build (Custom):** Only when the AI system provides a fundamental competitive advantage (e.g., a proprietary medical coding system or a unique supply chain optimizer) and you have the engineering resources to maintain it.

### Deployment Checklist

1. **Audit for "Shadow AI":** Identify where staff are already using unmanaged AI tools to prevent data leaks.
2. **Toggle the Small Business Suite:** For those on Claude Team or Enterprise plans, enable the "Small Business" toggle to activate the pre-built 15 workflows.
3. **Set Approval Guardrails:** Configure all "Write" tools (actions that change data, send emails, or move money) to **"Needs Approval"** rather than "Always Allow."
4. **Clean Your Context:** AI agents perform only as well as the data they can see. Prioritize cleaning your HubSpot records and QuickBooks categories before syncing.
5. **Establish Human-in-the-Loop:** Ensure at least one human operator is responsible for "approving" the final output of any multi-step agentic chain before it hits a customer or a bank account.

### Operational Limit Warning

Operators should be aware that while the **HubSpot connector** is powerful, it currently limits bulk updates to **10 records per action**. For massive database cleanups, founders will still require traditional bulk-import tools or custom API scripts rather than a pure agentic conversation.

## Want to explore this topic further?

Book a free discovery call to discuss how ManaTech can help your business implement these ideas.

Book a Discovery Call