TelNex

Sample Agent Governance Review report

This is what an Agent Governance Review ends in. The company is made up. The kinds of findings are not: they are the gaps that appear when agents are adopted one project at a time. A real report runs longer and carries a cost range for every fix.

Summary

Varrowdale Supply distributes industrial parts and employs about 180 people. Leadership asked one question: what are our AI agents able to do, and is that what we intended?

- We found four agents in use. Leadership knew of two.
- We found eight gaps. Four should be fixed now. Four can wait a quarter.
- Three things we checked are fine as they are.
- The most serious gap: one agent can send a supplier payment to a bank account nobody at Varrowdale has confirmed.

1. The inventory

Agent	What it does	Owner	Runs on	Known to IT
Support agent	Answers customer email and chat about orders, returns and delivery	Customer service manager	The support platform's built-in agent	Yes
Invoice agent	Reads supplier invoices, matches them to purchase orders, schedules payment	Controller	A workflow automation tool with an AI step	Yes
Coding agent	Writes and changes code for the order portal	Nobody named	A coding assistant in agent mode	No
Outreach agent	Writes and sends first-contact emails to prospects	One sales representative	A sales tool on a personal account	No

2. The authority map

Agent	Can read	Can change	Can send or spend without a person
Support agent	Orders, customer contact records, shipping status	Order notes, return requests	Customer email. Refunds up to $200 each
Invoice agent	Supplier invoices, purchase orders, the general ledger	Supplier payment details, the payment schedule	Schedules payments of any size

Agent	Can read	Can change	Can send or spend without a person
Coding agent	The whole code repository	Any file. Can merge its own changes	Can deploy to the live order portal
Outreach agent	A full export of the customer database	Nothing in company systems	Email to anyone, from the representative's mailbox

3. Where a person approves today

- Support agent: nowhere. A manager reads a sample of conversations each Friday.
- Invoice agent: the controller approves the weekly payment run as a whole, by total. Individual payments are not shown.
- Coding agent: nowhere.
- Outreach agent: nowhere.

4. What is recorded

Each platform keeps its own log. The longest is kept 30 days. The support platform's log can be edited by any administrator. The outreach tool's log is visible only to the representative. No one at Varrowdale could reconstruct, across all four agents, what happened on a given day last month.

5. One failure, walked through

For each agent the report walks through the worst realistic mistake. This is the invoice agent's.

A supplier's email account is taken over. A message arrives with a new bank account and an invoice that matches an open purchase order. The invoice agent updates the supplier's payment details and schedules the payment in the next run. The controller approves the run by its total, which looks normal. The money leaves. Varrowdale learns of it when the real supplier asks to be paid.

- How far it reaches: one payment, up to the largest open purchase order. On the day we looked, that was $84,000.
- How Varrowdale would stop it today: it could not, before the bank sends.
- With the fix in gap 1: the payment waits until a person confirms the new account by phone.

6. The gaps, ranked

Effort bands: Small is days. Medium is one to three weeks. Large is more than a month. A real report gives a cost range for each.

#	Gap	Why it matters	The control	Effort	Call
1	The invoice agent can pay a bank account first seen that week	One forged email becomes a lost payment	A person confirms any new or changed bank account before the first payment. Payments above a set amount are shown one by one	Small	Fix now
2	The coding agent can merge and deploy alone, using a shared key	A wrong change reaches customers with no review, and nobody can tell who made it	The agent gets its own account. A person reviews every merge. The deploy key is taken out of its reach	Small	Fix now
3	The outreach agent runs on a personal account with the full customer export	The company cannot see it, limit it or stop it, and customer data sits outside company control	Move it under a company account or switch it off. Limit it to the fields it needs	Small	Fix now
4	Nobody could say how to stop any agent on a weekend	The first hour of an incident is spent finding the switch	One written stop step for each agent, tested once, with a named person and a backup	Small	Fix now
5	Logs are short-lived, scattered, and in one case editable	After an incident there is no reliable account of what happened	Action logs copied to a store the agents and their administrators cannot edit, kept 12 months	Medium	Fix later
6	Refunds are capped at $200 each with no daily total	A fault or a manipulated conversation can repeat the refund all day	A daily total and an alert to the service manager	Small	Fix later
7	Any support employee can rewrite the support agent's instructions, and changes are not recorded	The agent's behavior can change with no one deciding it should	Changes need the owner's sign-off and leave a record	Small	Fix later
8	The coding agent has no owner, and no written rule says what agents may do	Every question above gets answered case by case, or not at all	A named owner for each agent and a one-page agent policy	Small	Fix later

7. What is fine

- The support agent cannot see payment card numbers. The platform masks them before the agent reads a record. Checked.
- The invoice agent can read the general ledger and cannot write to it. Checked.
- All four vendors' terms say customer data is not used to train their models. The terms were read on the review date and are summarized in the appendix.

8. What happens next

The four "fix now" items are small. Varrowdale's own people can make three of them from this report. The report is theirs to act on alone, with us, or with anyone else.

Want this for the agents you run?

Book an agent governance review: telnex.com/services/agent-governance-review