

IMPLEMENTATION GUIDE · AGENTIC AI 2026

Deploying an AI Agent

Over 40% of agentic AI projects are expected to be cancelled by the end of 2027, and the named causes are cost, unclear value and missing risk controls. All three are decided before you build.

■ Three things that get sold under one name

Thing	What happens when the caller goes off script
Chatbot or IVR	It fails, loops or falls to a default. There was never anything behind the list.
Automation	Nothing. It runs the same fixed sequence regardless of what was said.
Agent	It reasons about it: asks, looks something up it was not told to, or hands over with the context intact.

■ The six parts. Most failures build the first and skip the rest

- **The job**, in one paragraph, including what is out of scope. If it takes a page, it is too big.
- **The tools** it may call, each named, each with a defined input and output.
- **The context** it sees when the call starts: the matched customer, open jobs, recent history.
- **The guardrails**, written as prohibitions, not guidance.
- **The escalation**: the trigger, the destination at every hour, and what the customer hears.
- **The log**: every call, every tool call, every decision. Without it you cannot improve it or defend it.

Choose the first job on three variables, and get the same answer on all three

High volume (a few dozen a week, or you never learn anything), **low variance** (agents are impressive in demos and inconsistent where the work has many shapes), and **low consequence** (your process for catching mistakes does not exist yet). The job everybody wants to automate first, the complicated one eating a senior person's week, scores badly on all three.

Enforce guardrails in the tools, not only the instructions

An instruction that says "do not issue refunds" is a preference. Not giving the agent a refund tool is a control. Where the consequence is real, remove the capability rather than asking for restraint. The standing seven: no pricing beyond the published list, no commitments about time, no account changes without verification, no other customer's data, no claiming to be human, no handling distress, and no more than two attempts before escalating.

■ Ninety days, in four phases with exit tests rather than dates

- 1 **Days 1 to 14, shadow.** Real calls, nothing reaches a customer, no tool changes anything. Exit when you have read 100 transcripts and can predict it.
- 2 **Days 15 to 35, after hours only.** Live on calls that would otherwise reach a mailbox. The downside is bounded because the alternative was nothing.
- 3 **Days 36 to 60, supervised overflow.** Daytime, only calls that would queue past a threshold. Half an hour of review a day, named owner.
- 4 **Days 61 to 90, front line and narrow.** It answers first on the defined job, hands over everything else, widens one decision at a time.

■ Five numbers

- **Containment.** 40 to 70% for a good first job. Near 100% means broken escalation.
- **Resolution.** Sample fifty calls a month. Logs will not tell you this.
- **Repeat contact in 72 hours.** The decisive one.
- **Escalation quality.** Above 90%, or it is a config problem.
- **Cost per resolved contact,** including review time.

■ Five jobs that pay back fast

- After hours answering.
- Booking and rescheduling.
- Job and order status.
- Call notes written into the CRM.
- Overflow at peak.
- Four of the five are work nobody is doing now, so nobody has to give anything up.

Containment that pushes work into tomorrow is not containment

A caller told something unhelpful at 7pm who rings back at 9am has been counted a success by most vendor dashboards and has cost you two contacts instead of one, plus the goodwill. **Report containment and repeat contact as one line, never two.** If both rise together, the agent is deferring work rather than resolving it.

The Australian position, briefly

No standalone AI Act, and no economy-wide mandatory guardrails: the December 2025 National AI Plan confirmed reliance on existing law and sector regulators. That does not mean nothing applies. Privacy, Australian Consumer Law, record keeping and telco rules reach what your agent says exactly as they reach a staff member. **From 10 December 2026, privacy policies must disclose the kinds of personal information used in substantially automated decisions, and the kinds of decisions made.**