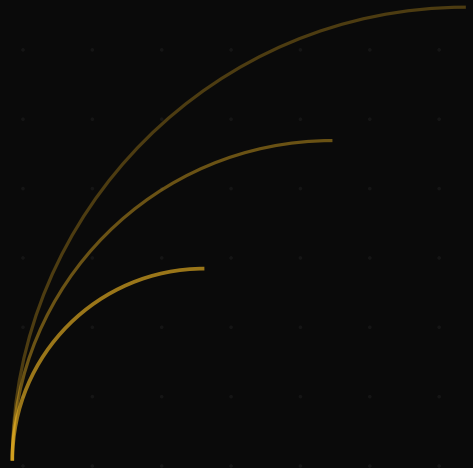
TECHNOLOGY, SECURITY, AND PROCUREMENT LEADERS

How to procure AI agents safely

Procuring AI agents is not procuring SaaS. A buyer's playbook for scoping autonomy, capping agentic spend, defining acceptance, and writing the clauses standard contracts miss.



AI agents act on your behalf: they call APIs, write to systems of record, and spend money.

WHAT'S INSIDE

4 steps in this guide

01 Scope the autonomy

02 Cap the agentic spend, with auto-pause

03 Define acceptance for behavior, not features

04 Land the clauses standard contracts miss

01

Scope the autonomy

Be explicit about what the agent may and may not do. List the systems it can read, the systems it can write to, the actions it may take without human approval, and the actions that require a human in the loop. An ambiguous scope is the foundation of the post-signature dispute.

02

Cap the agentic spend, with auto-pause

Agentic systems consume tokens and external APIs by acting. The contract needs a hard ceiling on agent-driven spend per day, week, or month, and an auto-pause clause that halts execution at a defined threshold, not after a $30,000 overage past a $100 alert.

03

Define acceptance for behavior, not features

Demos do not bind. Write acceptance criteria the agent must hit on your data and your tasks: success rate, escalation rate, and a defined behavior-change-notice window. Tie payment to passing these tests, not to access.

04

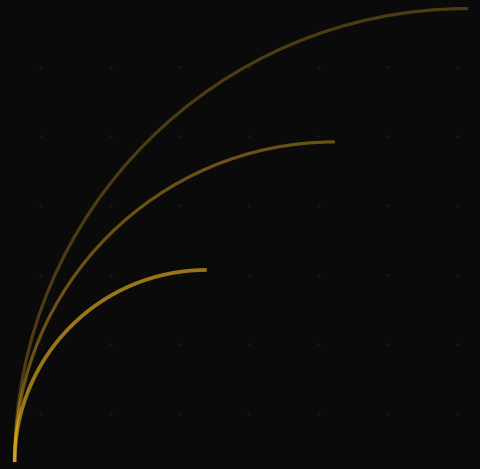
Land the clauses standard contracts miss

Training-data rights (does the vendor train on your interactions, can you opt out, is it indemnified), model-deprecation notice, a quality SLA distinct from uptime, weight return on exit if you fine-tuned, and EU AI Act / ISO 42001 alignment where applicable.

PUT THIS TO WORK

Walk into every evaluation with the vendor's own playbook.

- A vendor-proof scope, issued before any proposal
- Gap analysis scoring every proposal against your scope
- A risk-weighted interrogation kit for the vendor meeting
- Scope-drift detection across proposal versions



Start free at benchsideai.com

Your first project is free. No card required.