

Pitfall	Mitigation
Agent deadlocks	Add timeouts, loop limits, state checks, and escalation rules.
Context drift	Refresh indexes and test retrieval quality regularly.
Cost blowouts	Enforce budgets and route simple tasks to lower-cost models.
Missing audit trails	Log prompts, context, model choices, outputs, tools, and approvals.
Tool over-permissioning	Limit tool access by user role, workflow risk, and environment.