

How to Build an AI Operations System

Oct 2, 2026 · Bala Ananda, LU Corp Media

The idea in one minute

Build from the inside out: a brain first, then tools, then agents, then a manager. Each layer only works if the one beneath it is solid, so skipping ahead is the most common way these systems fail.

Think of it as a small company:

- 1. **The brain** is the company's memory. Every fact, rule and decision lives here, once.
- 2. **The tools and SOPs** are the equipment and the operating manual. They make work repeatable.
- 3. **The lead agents** are your employees. Each owns one area and uses the tools to get it done.
- 4. **The manager** is your operations lead. It takes your requests, hands them out, checks the work and reports back.

The rule that ties it together: everything reads from the brain before acting and writes back to it after. If a fact only lives in one chat, one agent or one person's head, the system will eventually lose it.

Step 1: Build the brain (your core)

The brain is a single source of truth that every tool and agent can read and write. Without it, every new chat starts from zero and your agents contradict each other.

Start with four stores. You don't need fancy software; a well-organized folder of Markdown files, a database or an Obsidian vault all work.

Store	What goes in it	Example
Memory	What is true right now: decisions, preferences, rules	"Never place more than 2 links per linking asset to one money site"
Wiki	Knowledge that builds up over time	How your rank-and-rent pages are structured
Ledger	What you intend to have and what exists	Every site, link, client and renter
Brain map	Which tool talks to which	"The links tool writes to the ledger"

How to build it:

- 1. Pick one home for the brain and stick to it. Everything else points here.

2. Write down your rules and decisions first. These are the things you repeat most often to people and AI.
3. Give every fact exactly one home. If the same fact lives in two places, they will drift apart and disagree.
4. Make it readable by machines. Plain text, clear file names and a short summary at the top of each file.
5. Set up a write-back habit. At the end of any job, new facts, fixes and decisions go back into the brain.

You're done with Step 1 when you can start a fresh AI chat, point it at the brain, and it knows your business without you re-explaining it.

Step 2: Build tools and SOPs (the hands)

Tools do the work; SOPs (skills) say exactly how. Together they make sure a job comes out the same way every time, no matter who or what runs it.

Start with SOPs, then automate them. Most people build tools first and wonder why results are inconsistent. Write the playbook, run it by hand a few times, then turn the stable parts into a tool.

1. **List your repeat jobs.** Anything you do weekly or more: publishing a page, checking rankings, placing a link, onboarding a client.
2. **Write one SOP per job.** Inputs, steps, rules, what "done" looks like. Keep it short enough to follow without thinking.
3. **Turn steps into tools.** Each tool does one job well: post to a site, check indexing, pull search data. Connect them so an AI can call them (MCP connectors are one way).
4. **Add guards.** Tools should block risky actions on their own: no deleting, spending or bulk changes without approval. A rule written only in a prompt can be skipped; a rule in the tool's code can't.
5. **Make every tool read and log.** Before acting, a tool checks the brain. After acting, it records what it did.
6. **Verify, don't trust.** A tool saying "done" isn't proof. Add checks that confirm the real result: the page is live, the link exists, the number moved.

You're done with Step 2 when a VA or an AI can follow an SOP, use the tools, and get the same result you would.

Step 3: Hire your AI employees (lead agents)

A lead agent is an AI model with a job description. It owns one area, decides what to do, and uses the tools from Step 2 to do it. Treat it like hiring a person: clear role, clear limits, clear way to report.

Every lead agent needs five things written down:

Part	What it answers	Example for an SEO lead
Role	What do you own?	Rankings and on-page health across all money sites
Tools	What can you use?	Rank tracker, Search Console, site audit, page editor
SOPs	How do you do each job?	Weekly audit SOP, title rewrite SOP

Part	What it answers	Example for an SEO lead
Limits	What needs approval?	Publishing new pages, anything that costs money
Reporting	What do you hand back?	A weekly summary plus tasks on the board

How to build them:

1. Start with one lead, in the area that eats most of your time. Get it working before adding a second.
2. Keep domains separate. SEO, content, links, ads and coding each get their own lead, so no two agents fight over the same job.
3. Let leads spawn helpers. For a one-off task, a lead can start a short-lived helper agent with a single job and a fresh start.
4. Keep knowledge out of the agent. Agents are swappable; everything they learn goes back to the brain, not into their own instructions.

You're done with Step 3 when you can hand a lead a task in one sentence and it comes back done, checked and logged.

Step 4: Add the manager (operations lead)

The manager doesn't do the work; it makes sure the work gets done. It's your single point of contact, so you talk to one agent instead of five.

The manager has five jobs:

1. **Intake.** Every request, from your phone, a chat or a session, lands on one task board.
2. **Routing.** It reads the request and assigns it to the right lead.
3. **Tracking.** It knows what's open, who has it, and what's stuck.
4. **Checking.** It confirms the result is real before marking a task done.
5. **Reporting.** It sends you results, and asks you only when a decision or approval is needed.

How to build it:

- Set up the task board first. The manager is only as good as its list of open work.
- Give it a routing table: which kinds of request go to which lead.
- Schedule a daily or weekly check-in where it reviews the board and flags anything overdue.
- Keep the risky keys with you. Spending, deleting and anything irreversible still waits for your yes.

You're done with Step 4 when you can send one message from your phone and the right work happens without you chasing it.

Rollout and common mistakes

Go one layer at a time and let each one run for a while before adding the next. A shaky brain makes every agent on top of it unreliable.

Mistakes to avoid:

- **Building agents first.** Without a brain and SOPs, agents improvise, and every run comes out different.
- **Storing knowledge in prompts.** When you switch models or start a new chat, it's gone. Put it in the brain.
- **Duplicate facts.** Two copies of a rule will eventually disagree. One home per fact.
- **Trusting "done."** Always verify the real result: the live page, the live number.
- **Too many agents too soon.** One working lead beats five half-working ones.

Starter checklist:

- ☐ Pick one home for the brain
- ☐ Write down your top 20 rules and decisions
- ☐ Create the ledger: sites, clients, links, tools
- ☐ Write SOPs for your 5 most repeated jobs
- ☐ Turn the most stable SOP into a tool with guards
- ☐ Set up a task board
- ☐ Launch your first lead agent with role, tools, SOPs, limits and reporting
- ☐ Add the manager once two or more leads are running