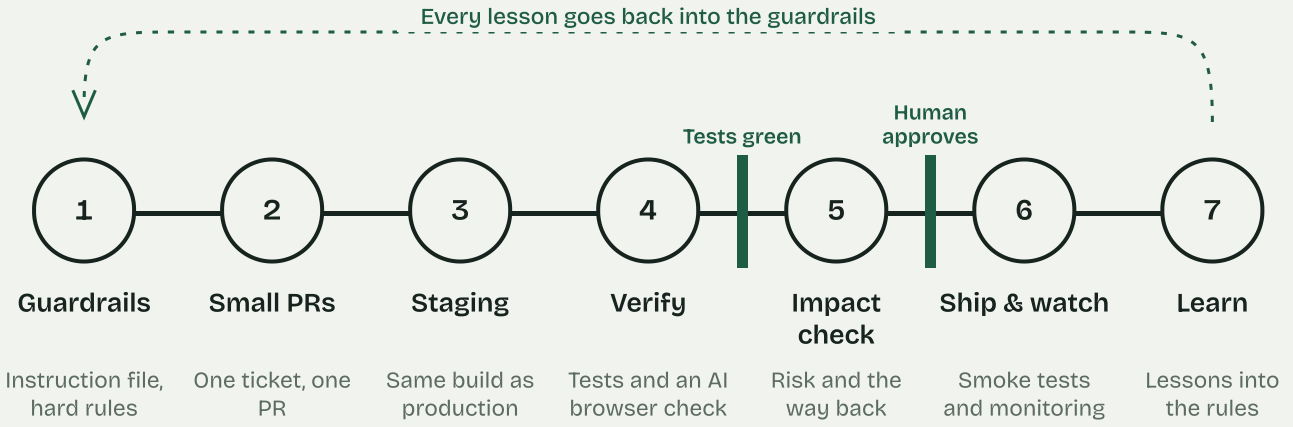


Dominik Heinrich, multi-cloud DevOps & AI solution architect

Ship with AI coding agents, safely

An adoption framework for an AI-assisted software delivery lifecycle (AI-SDLC). It is the process behind more than 5,000 merged pull requests on two production platforms.



Seven stages, two hard gates. Agents write the code; people approve what reaches production.

One production SaaS built with this process, anonymized

3,025 pull requests merged in ten months	**1,048** automated test files	**160** serverless functions	**3** apps: web, iOS and Android

The seven stages

Set them up once per team and repository. Tick them off as they go live.

01 Write the guardrails first

- [ ] A short instruction file per repository: architecture, conventions, what the agent may and may not do.
- [ ] **Hard rules:** authentication, payments, data deletion and secrets always need a human approval.
- [ ] Agents never touch production data or real customer accounts, only test accounts.

02 Keep every change small and reversible

- [ ] One ticket, one pull request. Branch protection and a PR-only workflow, no direct pushes.
- [ ] Database migrations idempotent and dry-run against the target database before merge.

03 Staging first, always

- [ ] Every change reaches a staging environment before production, with the same build and config.
- [ ] Only changed functions or services are deployed, to keep each release small.

04 Verify like a user

- [ ] Unit and end-to-end tests, plus type-check and lint baselines that can only improve.
- [ ] An AI browser test in a real Chrome: the flow described in plain language, a pass or fail with errors and a fix prompt.

05 Analyse the impact before production

- [ ] **A short table per release:** what changes, who is affected, the risk and the way back.
- [ ] A human approves the production merge.

06 Ship and watch

- [ ] Smoke tests on vital routes after every deploy, and the deploy turns red if one breaks.
- [ ] Outcome monitoring, and one issue opened automatically per failure, closed when it recovers.

07 Close the loop

- [ ] Customer replies drafted by the agent and sent by a person.
- [ ] Every lesson goes back into the instruction files, so the process improves itself.

Rolling it out, by company size

Startup: guardrails, staging and browser checks in one to two weeks. Speed comes from the loop, not from skipping it.

Mid-sized company: one pilot team for four to six weeks, a security review, then the rollout to the other teams.

Enterprise: governance first: an approved model and provider list, data classification, local models for sensitive code, an audit trail and a platform team that enables the others.

What to measure

Lead time from ticket to production, change failure rate, merged pull requests per week and bugs found by users.

Mistakes I see most often

- Agents pushing straight to the main branch, or holding production credentials.
- Pull requests with thousands of lines that nobody can really review.
- Skipping staging because the tests are green.
- No instruction file, so every session starts from zero and repeats old mistakes.
- Measuring lines of code instead of lead time and change failure rate.

Ways to work together

The same quality for a ten-person startup and a global group. The format adapts to you.

Startups

Fractional DevOps & AI lead

A few days a month: architecture, the release pipeline and AI features, so the founders can focus on customers. From prototype to production without a rewrite.

Mid-sized companies

A project with a clear outcome

A defined goal like a lower cloud bill, a migration or the first AI agents in production, with a fixed scope, weekly progress and a handover your team can run.

Enterprises

An architect inside your teams

Embedded with your platform, security and product teams: architecture decisions, governance for AI and regulated environments. For larger scopes I bring a trusted senior team.

How I work

Decisions written down: architecture decision records with the trade-offs, so your team knows why, not just what.

Secure by default: OIDC and managed identities, least privilege, secrets in a vault, an audit trail.

Operated, not just delivered: SLOs, alerts on business outcomes and an incident routine.

Measured: cost, lead time, uptime and hours saved, reported every week.

Knowledge stays with you: runbooks, docs and workshops for your team.

One point of contact who talks to engineering and to management, in German, English and Spanish.



Want this running in your team?

Book a 30-minute call

E-mail mail@dominikheinrich.ch
Web dominikheinrich.ch

Available worldwide, remote. On-site on request, depending on the country.