moring

SIX-STEP COMPANION / ONE DEPLOYMENT

One agent. Six control checks.

Pick one deployment. Find what you can show. Choose the next action.

Agent / environment: _____ Owner: _____

Highest-impact action: _____

01 Know it

Identify the deployed model, tools, skills, versions and relevant context stores. Match inventory to the running release.

State: [ ] Verified [ ] Partial [ ] Unknown Owner: _____
Record / date: _____

02 Own it

Name the agent identity and one accountable human. Record delegated authority and who may write shared context.

State: [ ] Verified [ ] Partial [ ] Unknown Owner: _____
Record / date: _____

03 Bound it

Set explicit read/write, tenant, destination and spending limits. Test a disallowed action outside the prompt.

State: [ ] Verified [ ] Partial [ ] Unknown Owner: _____
Record / date: _____

04 Approve it

Review consequential actions and material changes. Bind approval to exact scope; remembered text cannot grant authority.

State: [ ] Verified [ ] Partial [ ] Unknown Owner: _____
Record / date: _____

05 Prove it

Reconstruct request, source-labelled context, handoffs, tools, authority and actual outcome.

State: [ ] Verified [ ] Partial [ ] Unknown Owner: _____
Record / date: _____

06 Stop it

Test new-call refusal, revoke access, contain queued/delegated work and invalidate relevant poisoned context copies.

State: [ ] Verified [ ] Partial [ ] Unknown Owner: _____
Record / date: _____

Next action: _____ Owner / date: _____

Verified is your documented conclusion, not a certification. Partial: incomplete, absent or failed. Unknown: not known yet. Keep record reference, deployed version, date, owner and review/test basis. For enforcement, record a disallowed-case test and actual outcome. A yes alone is not evidence. No overall readiness score.