Ten highest-leverage things to do first

If you do nothing else, do these ten — ordered by leverage. Check them off. One sitting gets you a real harness.

Layer: Context Capability Control Governance

- [ ] **1 Write a lean AGENTS.md**
  Canonical, version-pinned, real 3–10 line snippets. Keep it ~200 lines. This single file is the highest-leverage artifact you own.
  CONTEXT

- [ ] **2 Add the two thin adapters**
  CLAUDE.md (@imports AGENTS.md) and copilot-instructions.md (hard rules in first 4,000 chars). Author once, serve both vendors.
  CONTEXT

- [ ] **3 Port the starter skill library**
  code-review, secure-coding-checklist, pii-handling, regulatory-logging. Each with a description written as an explicit trigger.
  CAPABILITY

- [ ] **4 Add a code-intelligence MCP server**
  Replace grep/glob exploration with one AST/graph server. Prefer local-first; pin the version. Big token + tool-call savings.
  CAPABILITY

- [ ] **5 Create a security-reviewer subagent**
  Read-only, scoped tools, blocks on hard-coded secrets. Same prompt body compiles to a Copilot security-scout agent.
  CONTROL

- [ ] **6 Add a protect-paths hook**
  A PreToolUse gate (exit 2 blocks) plus a post-edit lint hook. Turns advisory rules into enforced ones, locally.
  CONTROL

- [ ] **7 Ship one gh-aw security-guard**
  Read-only token, safe-outputs only, compiled with --strict. Per-PR security pass that complements the inner-loop hook.
  CONTROL

- [ ] **8 Turn on mandatory review**
  Branch ruleset: auto Copilot review (non-blocking) + one required human approval + green CI. No AI change lands unreviewed.
  GOVERNANCE

- [ ] **9 Distribute policy you can't override**
  managed-settings.json via MDM: deny-list, model pinning, marketplace lock. New laptops come up compliant by default.
  GOVERNANCE

- [ ] **10 Wire the audit pipelines**
  OpenTelemetry (prompt/tool content) + Compliance API pull + GitHub audit log → SIEM. You need all three to reconstruct events.
  GOVERNANCE