

Five Gates Before an AI Agent Changes Cryptographic Code

Original KIS editorial framework; not an official CSA/NIST checklist.

1. Scope Task to Single Repository

Restrict the agent to a narrow test branch with zero access to production secrets or environment variables.



2. Isolate Execution in Ephemeral Environments

Run the agent in disposable development environments with approved tools and restricted outbound network access.



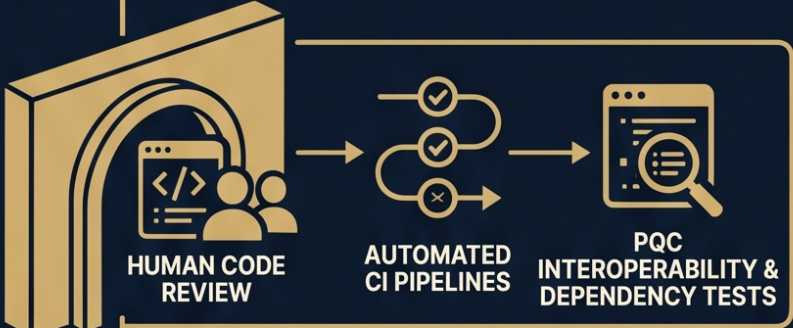
3. Limit Identity to Short-Lived Credentials

Scrape personal developer tokens and use least-privilege, task-specific credentials that log and revoke automatically.



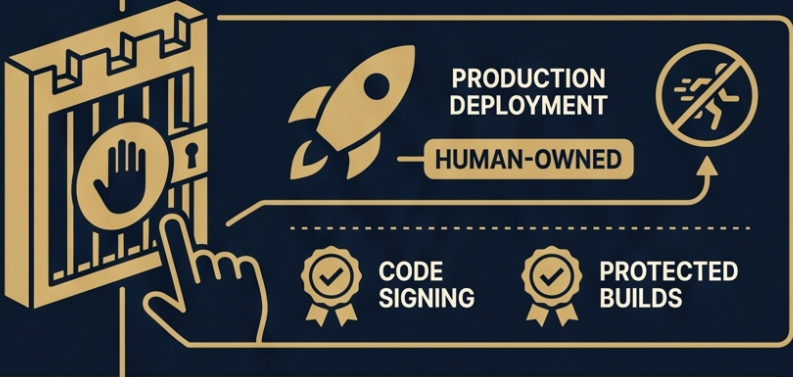
4. Verify Diff via Independent Review

Require human code review, automated CI pipelines, and post-quantum crypto interoperability and dependency tests.



5. Keep Production Release Human Owned

Ensure code signing, protected builds, and production deployments remain completely outside agent authority.



For PQC, the accountable cryptography owner sets the target and tests; the agent does not choose policy or approve release.

IMPLEMENTATION TIMELINE (30-DAY PLAN)

 Phase 1 First 72 Hours	 Phase 2 Days 4-14	 Phase 3 Days 15-30
Inventory active AI tools & repos (Owner: Engineering + Security)	Non-production trust-boundary & prompt injection tests (Owner: AppSec + Platform)	Bounded human-reviewed pilot on test repo (Owner: Product Engineering + Crypto/Architecture)