

The Executive Guide to AI Code Governance

Turn unbounded agent output into a controlled enterprise change: validate the plan, calculate the blast radius, block P0 risk, and retain decision evidence without retaining source payloads.

01 / THE STRATEGIC CHALLENGE

Velocity without control

AI coding agents can multiply pull-request volume while review capacity, system context, and control evidence remain fixed. A locally correct diff can still violate a cross-repository contract, expose a secret, or ship beyond the approved architecture.

01 PLAN DRIFT

Code is generated before the architecture and business requirement are validated.

02 CONTEXT LOSS

Repository-local review misses owners, contracts, dependencies, and runtime impact.

03 QUEUE SATURATION

Machine-scale output converts reviewer delay into an undocumented risk decision.

04 EVIDENCE GAP

Approval cannot be reproduced when policy, identity, and blast radius are not recorded.

02 / THE GOVERNANCE ENGINE

Control before merge

codecr sits between business intent, source control, AI coding agents, and the production gate. It narrows what an agent may change and proves why a merge was allowed or blocked.

01 PRE-CODE GOVERNANCE

Index approved repository and Jira context; produce an editable plan before code generation.

02 BLAST-RADIUS GATING

Map dependencies and affected owners; evaluate .codecr.yaml before merge authority is available.

03 P0 CONTAINMENT

Block the pull request with a stable rule ID, evidence set, approver requirement, and fix path.

04 BOUNDED REMEDIATION

Send only the finding, permitted files, tests, and policy constraints to the approved coding agent.

05 ZERO-RETENTION ANALYSIS

Process source and diffs in an ephemeral microVM workspace; destroy memory and derived workspace when the job closes.

03 / CISO ASSURANCE MATRIX

Boundaries that survive review

DATA SOVEREIGNTY

Dedicated region, customer VPC, or on-premises processing boundary defined in the data-flow schedule.

AIR-GAPPED PARITY

Same policy decision model with offline, signed release bundles and no external telemetry requirement.

RETENTION

Source, diffs, embeddings, and prompt payloads excluded from persistent application storage in zero-retention mode.

KEY AUTHORITY

Customer KMS or HSM owns key material, rotation, revocation, and audit evidence.

REQUESTED VALUE BENCHMARK*

\$4.2M / YEAR

* Modeled input, not an audited cohort average. Validate PR volume, review time, developer rate, incident assumptions, and methodology before using it in a financial claim.

DECISION PATH

1. Bound VPC > 2. Import policy > 3. Baseline review queue > 4. Measure 14 days