How to Implement AI Governance for Development Teams

Standing up governance, classification, and policy enforcement

Step 1: Establish the AI Governance Board

Form a cross-functional board with representatives from Security, Legal, Engineering, Compliance, and Risk. Define the charter including decision authority, meeting cadence (monthly minimum), and escalation paths.

- Appoint a board chair (typically CISO or VP Engineering)
- Define quorum requirements for decisions
- Create a decision log template for audit trail
- Schedule recurring monthly meetings with standing agenda

Step 2: Deploy Three-Tier Classification

Classify all AI tools into three tiers based on risk assessment:

- Tier 1 (Unrestricted): Tools approved for all use with public/internal data
- Tier 2 (Controlled): Tools approved with guardrails (e.g., telemetry off, specific repos only)
- Tier 3 (Prohibited): Tools banned due to data handling, licensing, or security concerns

Review classifications quarterly. New tools start at Tier 3 until evaluated.

Step 3: Configure Repository-Level Policies

Enforce AI usage policies at the code repository level:

- Create AGENTS.md or .aiconfig files in each repository
- Define which AI tools are permitted per repository based on data classification
- Set up pre-commit hooks to detect and flag AI-generated code
- Configure AI tool settings to disable telemetry for sensitive repositories

Step 4: Measure and Report

Track governance KPIs to demonstrate program effectiveness:

- Percentage of repositories with AI policy files configured
- Number of shadow AI incidents detected and remediated
- AI tool evaluation turnaround time (target: <30 days)

- Developer compliance rate with AI usage policies