OSFF NEW YORK 2026

Who's Checking the AI?

SDLC Controls for Agentic Coding Pipelines

Alex Kantor

Director of Technology, Kosli. FINOS SDLC controls maintainer.

Kosli

Who do you trust more: humans or AI agents?

Kosli

What makes a good review?

It meets the requirements

Nothing extra has been added and nothing removed without a justification

The code meets our standards and patterns

Kosli

What the evidence checks

The pull request was approved by at least one person who didn’t write the code

Nothing was added between the approval and the merge

The person was eligible to review it

Kosli

Of course all of these are always true

We have regular training on what a good review is

We always have enough time to review in the detail required

We never just glance through it because we trust the engineer and marvel at their talents

Of course all of these are always true

We have regular training on what a good review is

We always have enough time to review in the detail required

We never just glance through it because we trust the engineer and marvel at their talents

Right? 😐

A pretty standard delivery pipeline

HOW THE WORK GETS DONE

Ticket	Plan	Approve	Code	Gates	Review	Merge	Build	Deploy

Kosli

And the controls underneath it

HOW THE WORK GETS DONE

Ticket	Plan	Approve	Code	Gates	Review	Merge	Build	Deploy

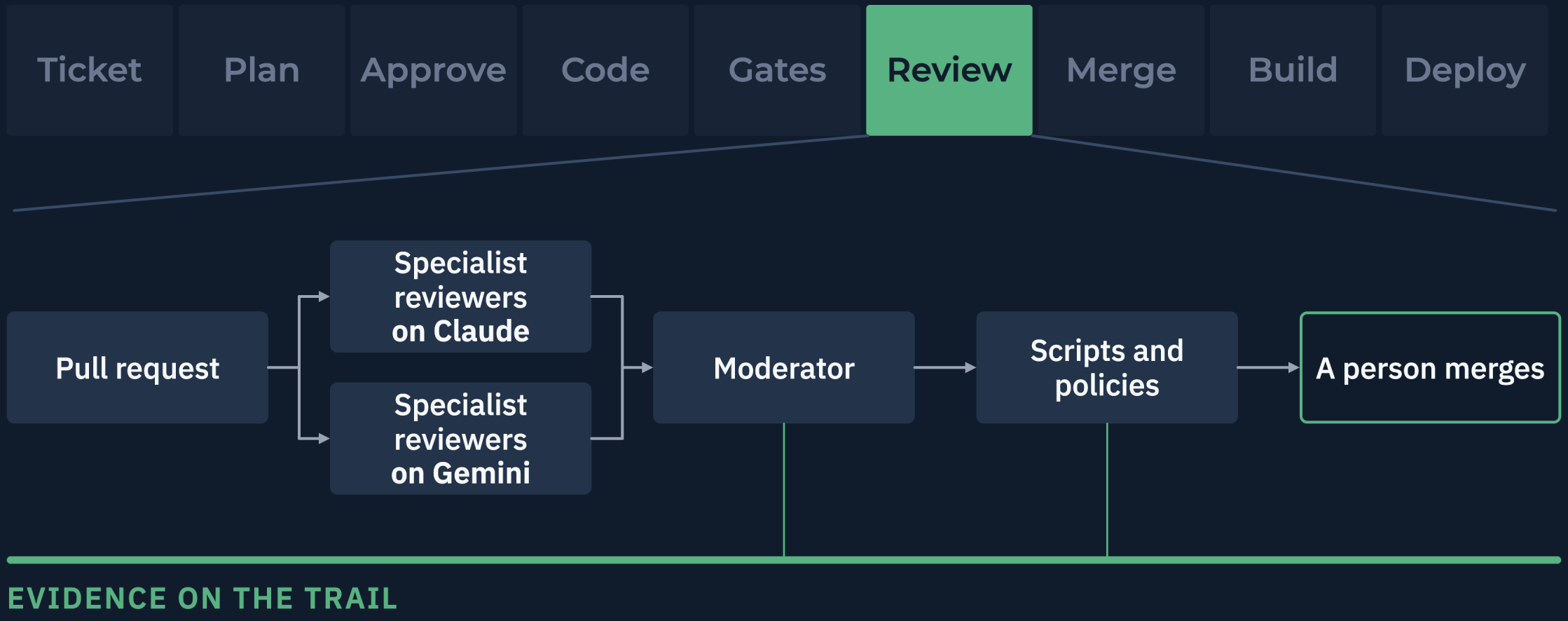
HOW WE SHOW IT WAS DONE PROPERLY

Requirements Approval	Vuln. Scanning	Quality Assurance	Code Review	Artifact Provenance

Controlled Build Environment

Kosli

Our PR reviewer



Kosli

Peter’s pull request



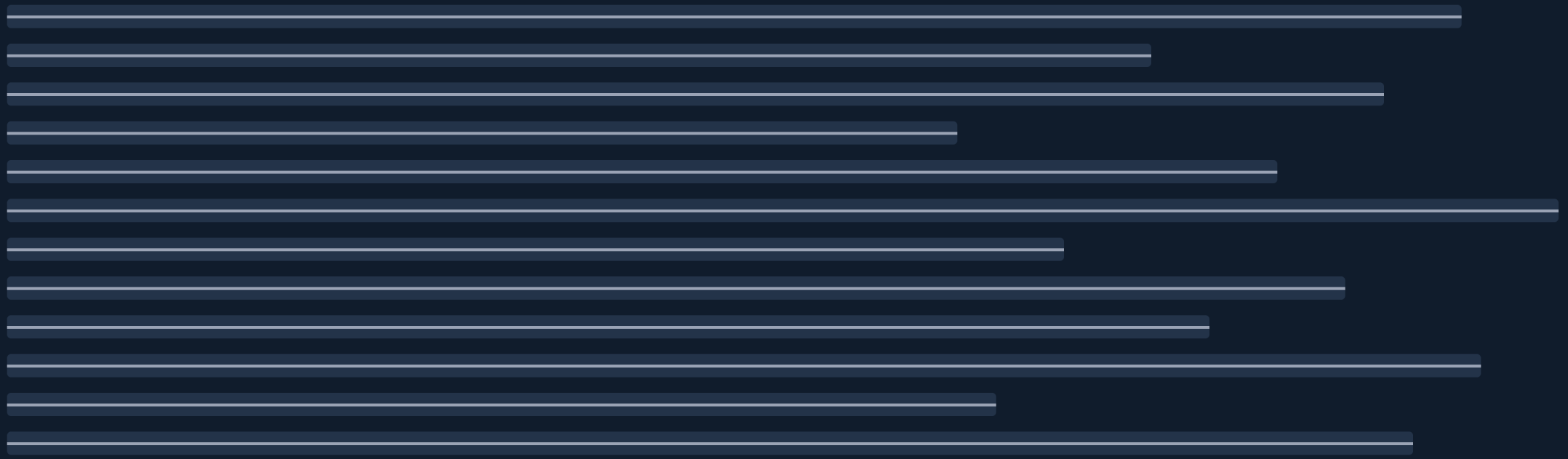
Round one properly reviewed about a third of the files

Kosli

Tore’s pull request

1 line changed

12 findings, none of them real



Kosli

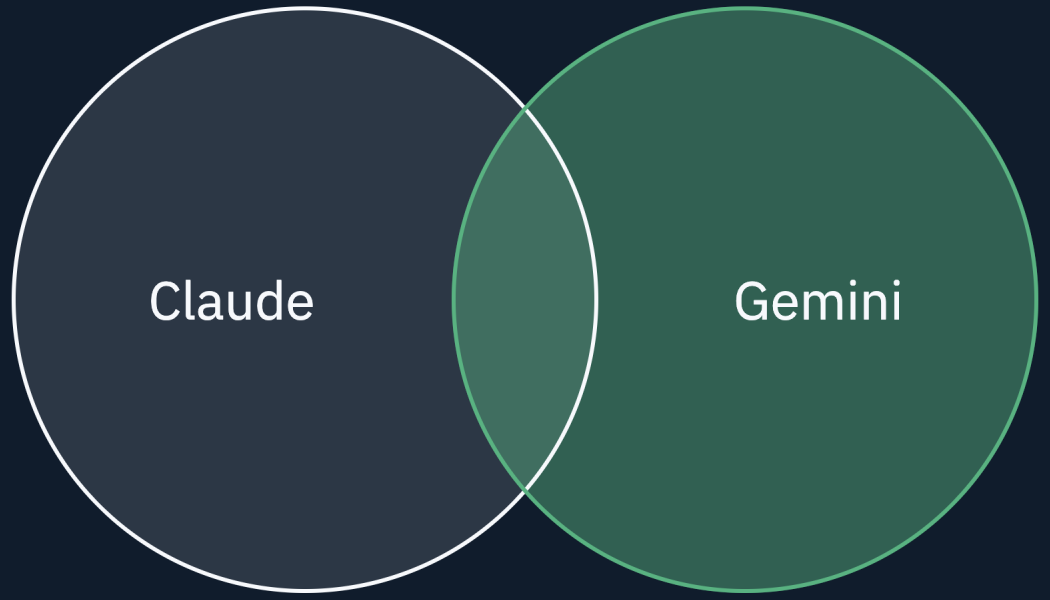
Reading doesn't mean applying

A reviewer can read a standard, summarise it perfectly, and still miss the one line that breaks it.



Kosli

Levels of agreement



They agreed on about a fifth to a third of what they found

Kosli

For low-risk changes from trusted authors, the automated checks are enough to merge without a human approving it.

- Anthropic, October 2026

Kosli

Two other examples

HOW THE WORK GETS DONE

Ticket	Plan	Approve	Code	Gates	Review	Merge	Build	Deploy

HOW WE SHOW IT WAS DONE PROPERLY

Requirements Approval	Vuln. Scanning	Quality Assurance	Code Review	Artifact Provenance

Controlled Build Environment

Kosli

LLMs for judgement.
Scripts for facts.
Policies for the decision.

Kosli

Rego says no.
Ergo says why.

ergo.kosli.com

Kosli

review-controls 49 checks on every review

SUBJECT	CHECK	VALUE READ	PASSED	CAUSE
review_round pr-reviewer-PR372-R1				
	two_vendors	claude.model_type = "claude" gemini.model_type = "gemini"	true	satisfied
	every_hunk_acknowledged	coverage.hunks_acknowledged = 25 coverage.hunks_total = 25	true	satisfied
coverage_file				
api.py	acknowledged	status = "reviewed_ok"	true	satisfied
auth.py	acknowledged	status = "summary_only"	false	value

Kosli

1 Your controls still hold.

Kosli

1 Your controls still hold.

2 Turn what you trust people to do into something you can check.

Kosli

1 Your controls still hold.

2 Turn what you trust people to do into something you can check.

3 A control decision should show its workings.

Kosli

Who do you trust more: humans or AI agents?

Kosli

Thank you.

ergo.kosli.com

FINOS SDLC controls working group



Who's Checking the AI? SDLC Controls for Agentic Coding Pipelines

Kosli