

CASE STUDY · FINTECH · SOUTHEAST ASIA

How BukuWarung put AI governance into production in 21 days

BukuWarung is a Y Combinator and Valar Ventures-backed fintech, building the operating system for Southeast Asia's MSMEs. In mid-2026 its organisation was adopting AI tools at speed: engineers in Claude Code, business teams running their own workflows in Claude Desktop and Cowork, and AI-powered services moving toward production. The tools were useful immediately. The evidence of how they were being used did not yet exist in one governed record.

Twenty-one days after signing, it did.

At a glance

21 days from signed agreement to organisation-wide governance in production	0 custom policies needed for the initial engineering-security baseline	1 planned, 4 integrated a single-service gateway integration plan grew to four services, validated in staging, expanded by BukuWarung's own team
1.3 million model and tool calls governed over the sixty-day evaluation, every one with a policy decision in the audit record	6,649 PII redactions applied at the point of the call, before data reached a model provider	121 users under governance across engineering and business teams

The requirement

Indonesia's personal data protection law, UU PDP, carries administrative sanctions of up to two percent of annual revenue, and OJK's supervisory toolkit for financial businesses reaches to licence conditions. For a fintech handling sensitive data, AI governance is a risk and compliance requirement before it is a productivity question. BukuWarung's own risk and control register treated audit logging, data masking and per-user attribution as preconditions for expanding AI access, and its Risk Committee had written a nine-point set of prerequisites before any vendor evaluation began. The sharpest of them was jurisdictional: personal data must not leave the jurisdiction, and any assistant surface that could carry it needed redaction at the point of the call, not review after the fact.



Why AxonFlow

At the start of the evaluation, AxonFlow mapped directly to five of the nine prerequisites without customisation; the remaining four were organisational and stayed with BukuWarung, as they should. Three properties carried the decision. It is self-hosted, so policy enforcement, the control plane and the retained governance records run inside BukuWarung's environment, and model calls go only to providers BukuWarung selects, after the applicable controls and redaction. It is vendor-neutral, governing Claude surfaces, internal MCP tools and the agent gateway from one control point. And enforcement is deterministic: the answer to "why was this allowed" is a rule, not a model's judgement.

What happened

Signed 23 June 2026

A sixty-day evaluation under a letter of intent, scoped to a single workflow.

Live inside the first week

AxonFlow was running in BukuWarung's own VPC within days, with Claude Code enforcement live for the engineering team. The 87 policies available out of the box covered the initial engineering-security baseline before a single custom policy was written. On the first review call the integration lead's word for the platform was "very stable."

Production, organisation-wide, by day 21

By mid-July the Phase 1 deployment governed Claude Code, Claude Desktop and Cowork through policy enforcement and OpenTelemetry ingestion, with PII redacted at the point of the call and each session attributed to an individual user. BukuWarung confirmed Phase 1 complete in writing on 13 July. The team went past the agreed scope in the same phase: cost dashboards and per-session summaries meant AI spend could be read by team and task rather than as a single line.

One workflow became four

The second phase put AxonFlow at the agent gateway layer, so model calls and tool calls from connected applications pass through policy enforcement before reaching a model or a tool. The plan was one workflow. BukuWarung's engineers integrated four: Cortex, the internal assistant; Sekar, the customer-facing chatbot; the company's direct API integrations; and the internal MCP tool surface, including the BigQuery data agent and Mixpanel analytics. The four-service integration was completed and validated in staging during the evaluation. The gateway adapter was deployed to production on 4 August in preparation for a cutover; no production traffic passed through the gateway during the evaluation period.

Identity followed the same pattern

Identity followed the same pattern. On 4 August BukuWarung published the SCIM provisioning endpoint in production, and the next day validated per-user JumpCloud tokens against the production governance API and audit reads. While confirming those facts for this story, the team authenticated against the production audit API with a personal token and got tenant-scoped data back.



Governance data became management data

The records built for risk and compliance turned out to be the records the people running AI adoption needed. In BukuWarung's words, the evaluation let them decide that Claude Code and Cowork "can be safely rolled out across the company, with AxonFlow providing the required policy and governance layer," gave the business team "clearer visibility into which tools are being used, by whom, and under what policies," and let them identify "users who would benefit most from premium seats rather than assigning them broadly." The business team received this reporting through BukuWarung's AI team, which acted as the bridge between business stakeholders and the underlying data. Over the evaluation, 6,649 PII redactions were performed at the point of the call across 121 users.

Built against their feedback

The evaluation shaped the product directly: a session-summary API, session-level audit search, fleet-deployment guidance for their JumpCloud environment, the OJK and UU PDP compliance report exports, and the agent-gateway adapter built for their architecture.

What made the 21-day rollout possible

The technology did not do this alone. Andika Rachman gave the programme senior sponsorship and kept it tied to BukuWarung's wider AI-adoption goals. Ajeya Krishna took end-to-end technical ownership: deploying from the documentation, surfacing precise gaps, validating fixes and expanding the gateway work from one planned workflow to four. And the organisation treated governance as part of adoption rather than a gate added afterwards, gave candid feedback fast, and started using the resulting records to run the programme. Senior sponsorship, a technical owner, and a short feedback loop: that is the repeatable part.

What it produced

Governed, redacted usage and audit records across every deployed Claude surface, in production, with the evidence created as AI was used rather than reconstructed afterwards. An audit record tied to the policy decision made at execution time gives risk, compliance and audit teams a stronger basis than logs assembled after the event. The OJK and UU PDP compliance exports extend the same principle to regulatory reporting: a report generated on demand from the governed records, in place of days of evidence collection across separate surfaces. And, by BukuWarung's own account, the evaluation "moved us from simply experimenting with these tools to having a clearer framework for secure company-wide adoption, governance, auditing, and cost optimization."

"I consider this to be a very successful pilot. Everyone across the whole company is already using it and finding value in it."

Andika Rachman, Head of AI Engineering, BukuWarung

"We planned to integrate one workflow. The documentation was clear and the integration was frictionless enough that we integrated four. It has been stable since the first week."

Ajeya Krishna, Lead AI Engineer, BukuWarung

For other regulated companies

Reproducing this takes three things BukuWarung already had: a risk register that names its preconditions, an executive sponsor who owns the outcome, and one engineer with the mandate to deploy. AxonFlow takes a small number of design partners each quarter on exactly that basis.

Apply as a design partner | getaxonflow.com/design-partner