AGENT GOVERNANCE FOR REGULATED INDIAN ENTERPRISES

The accountable record beneath the AI agents you already run - and the lifecycle that certifies, watches, and re-certifies them.

Sakshi is a single-tenant governance layer, not another model or dashboard. It gives every agent a verified identity, a tamper-evident record of every decision, bounded autonomy with a drilled kill switch, and regulator-mapped evidence - then adds the part regulators are now asking for: a governed-agent lifecycle that stops problems before they become headlines.

THE DIFFERENTIATOR

The governed-agent lifecycle

certify → watch → re-certify

Certify before it ships

A signed, RBI-mapped fit-for-production certificate - adversarial red-team, fairness, evaluation gates, a formally-verified autonomy policy, verified identity - with an expiry. Optionally required before an agent can go live.

Watch in production

The Guardian monitors the whole fleet and halts, escalates or steers the moment an agent drifts, is poisoned, or goes off-policy - using the same drilled kill switch a human would, every intervention on the record.

Catch the silent change

Sakshi fingerprints each agent's behaviour and tells you the day it started behaving differently - and whether the change was declared or silent. A silent change automatically sends the agent back through certification.

The loop nobody else closes for regulated Indian BFSI: certify an agent before it ships, watch it in production, and a silent model swap or behavioural drift auto-triggers re-certification - the continuous monitoring, kill switch, red-teaming and independent validation RBI's draft model-risk directions name as obligations.

THE RECORD BENEATH IT - FIVE MODULES, ONE SPINE

REGISTER	**Know Your Agent.** A live inventory of every agent and model - owner, autonomy tier, provenance, cryptographically verified identity. Nothing runs unregistered.
BOUND	**Bounded autonomy.** Envelopes route each action to auto, human review, or block, with oversight telemetry and a drilled kill switch.
VISHWAS	**India-calibrated fairness.** Declared-first bias screens gated on statistical significance, so they don't cry wolf.
WITNESS	**Flight recorder.** Every decision hashed into a chain anyone can independently verify. PII is tokenized before it is ever stored.
VIDHI	**Regulator-mapped.** Signed RBI MRM, DPDP, SEBI and IRDAI evidence packs, generated from live evidence, clause by clause.

MAPPED TO THE INSTRUMENTS YOU ANSWER TO

Regulator coverage

INSTRUMENT	WHAT SAKSHI PRODUCES
RBI MRM draft directions	Model inventory (KYA), independent validation via signed certification, red-teaming evidence, continuous monitoring + a drilled kill switch, and clause-mapped evidence packs - the obligations named in the draft, produced as evidence.
DPDP Act 2023 + Draft Rules	Algorithmic due-diligence (SDF), an assembled DPIA + signed audit bundle, declared-first fairness screens, and data-minimisation / localisation governance over extraction.
SEBI Reg 16C (binding)	Agent/model accountability and third-party attribution - verified A2A identity for vendor models, cited in the securities pack.
IRDAI anticipated 2026	A skeleton map that scores against live evidence today and re-cuts on the final framework.

SAFE TO PILOT

Deployment & security posture

- **Single-tenant, in your environment.** Sakshi installs in your VPC or data centre. Customer and production data never leave India or your environment.
- **It governs the act; it never becomes the store.** PII is tokenized at ingest - Sakshi never holds a raw identifier, by design.
- **Tamper-evident and independently verifiable.** The decision chain recomputes and verifies itself; evidence bundles are Ed25519-signed over exact bytes, so anyone can verify without trusting Sakshi.
- **No agent rewrite.** A few lines of SDK, or a zero-code gateway for agents you can't instrument. Sakshi observes, governs, and records where your agents already run.
- **Separation of duties and access as governed config.** Officers govern decisions; admins administer credentials and the IdP-to-role mapping - itself chain-attested.

THE ASK

What a design-partner engagement includes

- A **single-tenant install** in your environment, on synthetic or shadow data to start - no production traffic required to see the value.
- Hands-on mapping of **your** highest-risk agent use-case to the RBI / DPDP / SEBI / IRDAI obligations, with the signed evidence packs it produces.
- The full lifecycle on your agents: certify before go-live, the Guardian in production, silent-change detection wired to re-certification.
- Direct engineering support through the pilot, and a say in the roadmap ahead of the final RBI directions.
- In return: your regulated-BFSI perspective on what matters most, and a reference-able first install.

Rotavision Consulting Private Limited · India

rotavision.com · docs.rotavision.com · live demo on request