Korastratum

Switching from a Legacy Suite

A practical guide to replacing an enterprise financial-crime platform — coverage, migration, and total cost.

80% of the capability · ~20% of the total cost

THE INCUMBENT PROBLEM

You are paying tier-1 prices for capability a mid-market book doesn't use.

The enterprise financial-crime suites are genuinely capable — and genuinely built for global tier-1 banks. That heritage shows up on your invoice and your calendar: a six or seven-figure implementation, a multi-year licence, an annual maintenance line, and a dedicated team to tune it.

For a microfinance bank, PSB, or scaling fintech, most of that spend buys capability you will never switch on — market surveillance, consortium analytics, tier-1 enterprise fraud. The mandate you actually face — screening, monitoring, case management, effectiveness — is the 80% Kora delivers at a fraction of the cost.

Weeks	$0	No SI
to live, not multi-quarter	licence floor · pay for usage	no systems-integrator project

WHAT PARITY LOOKS LIKE

Module for module, where the coverage lands.

Watchlist filtering Sanctions · PEP · adverse media	**Real-time screening** Inline, screen-and-hold, fail-closed, surname-anchored matching
Transaction monitoring Rule library · scenarios	**30+ typology rule library** Self-serve, jurisdiction-aware, network & graph scenarios
Case management Alerts · workflow · audit	**Case management** Queues, SLAs, disposition, evidence trail
Model tuning / MRM Effectiveness · optimisation	**Effectiveness analytics** Precision, FPR and rule-firing health, built in

Plus the capability incumbents don’t have: Identity verification bundled · One platform, one data layer

WHAT WE DELIBERATELY CEDE

Honesty about the 20% — so you buy the right tool.

We would rather tell you where a legacy suite is the better fit than sell you a mismatch. Kora deliberately does not chase:

- ✓ **Market / trade surveillance** — insider-trading and market-abuse detection for a capital-markets desk.
- ✓ **Consortium analytics** — cross-institution fraud networks pooled across a member bank consortium.
- ✓ **Tier-1 enterprise fraud** — full account-takeover and device-intelligence platforms fed by auth-event and device telemetry streams.

If your mandate is AML, screening and monitoring for a mid-market book, that omitted 20% is capability you would pay for and never use. If you genuinely need it, a tier-1 suite is the right buy — and we'll say so.

> **The focus is the product.**
>
> Every dollar of engineering goes into the capability the mid-market actually runs — not a feature checklist for a buyer you aren't.

THE MIGRATION PATH

Run in parallel, prove it, then cut over.

01
Sandbox
Replay real traffic, no risk

→

02
Configure
Map your current rules

→

03
Shadow-run
Parallel vs incumbent

→

04
Cut over
Switch the live rail

Your rules, mapped

We translate your existing scenarios onto typed rule templates and confirm they fire identically before anything is live.

Prove it on your traffic

Shadow-run alongside the incumbent so you compare alert quality on your own book — not a vendor demo dataset.

No big-bang

Cut over a segment or a rail at a time. Effectiveness analytics show the alert-quality delta as you go.

Weeks, not quarters

Pre-integrated platform, no SI project — the timeline is configuration and validation, not a build.

THE COST CONTRAST

The same coverage, on a different cost curve.

	Legacy enterprise suite	Kora Compliance
Model	Licence + implementation + maintenance	**Usage-based** — per screen, per transaction
Entry cost	Six/seven-figure before go-live	**~Zero** — provision a tenant, pay for use
Time to live	Multi-month, SI-led	**Weeks** — pre-integrated
Tuning	Dedicated analyst team	**Self-serve** + built-in effectiveness
Scaling	Priced by scale / seats	**Usage** — a new branch doesn't raise the floor

Put us next to your incumbent — on your own traffic.

Start a shadow-run in the sandbox and compare alert quality directly.

korastratum.com · Talk to sales →