Vionsys IT
Solutions India Pvt.Ltd

Technical Business Proposal for

# Zinduka Risk & Decisioning Platform Proposal

**Empowering Intelligent, Inclusive, and Secure Decision-Making Across Borders**

Vionsys IT
Solutions India Pvt.Ltd

Secure | Scalable | Innovate

# TABLE OF CONTENT





## 1. Executive Summary:

Zinduka (**URDE**) is a next-generation **Unified Risk and Identity Decisioning Platform** that combines:

- **Transferable KYC Vault**: A secure, user-consent-driven vault enabling reusable identity verification across institutions.
- **Portable Risk Passport™**: A standards-based portable profile carrying a customer's credit, fraud, and behavioural history across borders.
- **Embedded Risk Decisioning Engine**: Real-time credit, fraud, AML, BNPL, and compliance decisioning powered by low-code orchestration and AutoML.

Designed for **Financial Services, Telco, Retail, and FMCG**, URDE empowers institutions with fast, explainable decisions while giving consumers ownership of their data and frictionless onboarding.



# Unified Risk Decision Engine (URDE) – Development Blueprint

## Executive Summary

URDE is a next-generation **Unified Risk and Identity Decisioning Platform** that combines:

- **Transferable KYC Vault**: A secure, user-consent-driven vault enabling reusable identity verification across institutions.
- **Portable Risk Passport™**: A standards-based portable profile carrying a customer's credit, fraud, and behavioural history across borders.
- **Embedded Risk Decisioning Engine**: Real-time credit, fraud, AML, BNPL, and compliance decisioning powered by low-code orchestration and AutoML.

Designed for **Financial Services, Telco, Retail, and FMCG**, URDE empowers institutions with fast, explainable decisions while giving consumers ownership of their data and frictionless onboarding.

**2. Project Objective**

- **Build a Dual-Market Decisioning Ecosystem (B2B & B2C)**

  Architect and deliver a cloud-native platform that fuses **real-time, AI-powered identity verification** with dynamic risk analytics, giving institutions split-second decision capability while offering consumers a frictionless onboarding journey.

- **Unlock Transferable KYC for Seamless Customer Mobility**

  Empower individuals to **securely export and share their verified KYC records**—whether as encrypted tokens, signed PDFs, or API payloads—so they can open

accounts, request services, or complete compliance checks anywhere, without redundant paperwork or delays.

- **Introduce Portable Risk Passports to Eliminate "Thin-File" Barriers**

  Create a **cross-border risk-profile exchange** that lets migrants, expatriates, and frequent travellers carry their creditworthiness and fraud-screening history to new markets, enabling lenders and service providers to make confident decisions from day one.

- **Deliver a Modular, Hyper-Scalable, Africa-Optimized Core**

  Design every microservice for **plug-and-play extensibility**, horizontal scaling, and **localization hooks** (currency, language, regulatory rules) so the solution adapts effortlessly to the continent's diverse financial landscapes while remaining compliant with POPIA, GDPR, and other global data-governance mandates.

- **Expose Enterprise-Grade APIs with Privacy-First Analytics**

  Offer a rich suite of REST/GraphQL endpoints, streaming webhooks, and developer SDKs that integrate seamlessly into banking cores, fintech apps, and compliance tools—backed by **real-time dashboards, AI explainability layers, and zero-knowledge encryption** to safeguard personal data and institutional IP alike.



## 3. Key Features — Putting Intelligence and Portability at the Core

| Feature | What It Does | Why It Matters |
|---|---|---|
| **Transferable KYC Vault** | Let's users pull down a **single, institution-signed KYC bundle** (encrypted PDF, blockchain-anchored token, or direct API hand-off) and present it anywhere. | Eliminates repetitive onboarding, speeds up account openings, and gives individuals full ownership of their identity data. |
| **Risk Passport™** | Packages a customer's **credit, fraud, and behavioural risk history** into a portable, standards-based profile that can be "stamped" by new lenders or service providers across borders. | Solves the *thin-file* problem for migrants, expatriates, and gig-economy workers, unlocking fair credit and better rates from day one. |
| **Behavioural Biometrics + Device Intelligence** | Continuously analyses keystroke cadence, swipe patterns, sensor data, and device fingerprint to deliver **real-time risk and identity scores**. | Adds a silent, friction-free security layer that thwarts account takeovers and synthetic-ID fraud without extra OTPs or user effort. |
| **Granular, Consent-Driven Data Sharing** | Every KYC export or risk-passport transfer is initiated by the user; the platform logs **immutable consent records** with time-stamps and receiving-party IDs. | Satisfies GDPR/POPIA "right-to-be-in-control" mandates and builds user trust through full transparency. |



### *Institution-Focused Capabilities*

| Feature Cluster | Core Benefit | Outcomes |
|---|---|---|
| **AI-First Risk Decisioning** Low-code orchestration of rules + ML | Combines rule engines, machine-learning models, and anomaly detectors for millisecond approvals, rejections, or step-ups. | Lower fraud losses, higher auto-approval rates, improved customer experience. |
| **Dynamic Customer Segmentation** | Auto-classifies users by behaviour, geo-risk, and lifetime value; instantly adjusts KYC tier, spending limits, and verification depth. | Personalised onboarding paths, optimised risk-reward balance, regulatory alignment by segment. |
| **RegTech Cockpit** | Unified dashboard showing real-time decision trails, model explainability, consent ledgers, and out-of-the-box regulatory reports. | Slashes audit prep time, simplifies compliance submissions, and gives teams confidence in AI outcomes. |
| **Plug-and-Play API Mesh** | REST & GraphQL endpoints, webhooks, and SDKs integrate with **core banking, credit bureaus, mobile-money rails, and fraud-signal partners**. | Rapid deployment, minimal vendor lock-in, and future-proof extensibility as the data ecosystem evolves. |

- **Decision Flow Builder**: Low-code orchestration of rules + ML.
- **Loan Origination & Management System (LOMS)**: Application to disbursement.
- **Embedded Finance**: BNPL, wallets, micro-loans, airtime lending.
- **Case Management**: Referrals, overrides, collections.
- **AutoML & Analytics**: Real-time scoring, model drift detection, retraining.
- **RegTech Cockpit**: Compliance dashboards, audit-ready reports.



Together, these feature sets deliver a 360° solution that **empowers consumers with data portability while giving institutions the real-time intelligence and controls they need to grow securely**.

## 4. Technical Architecture

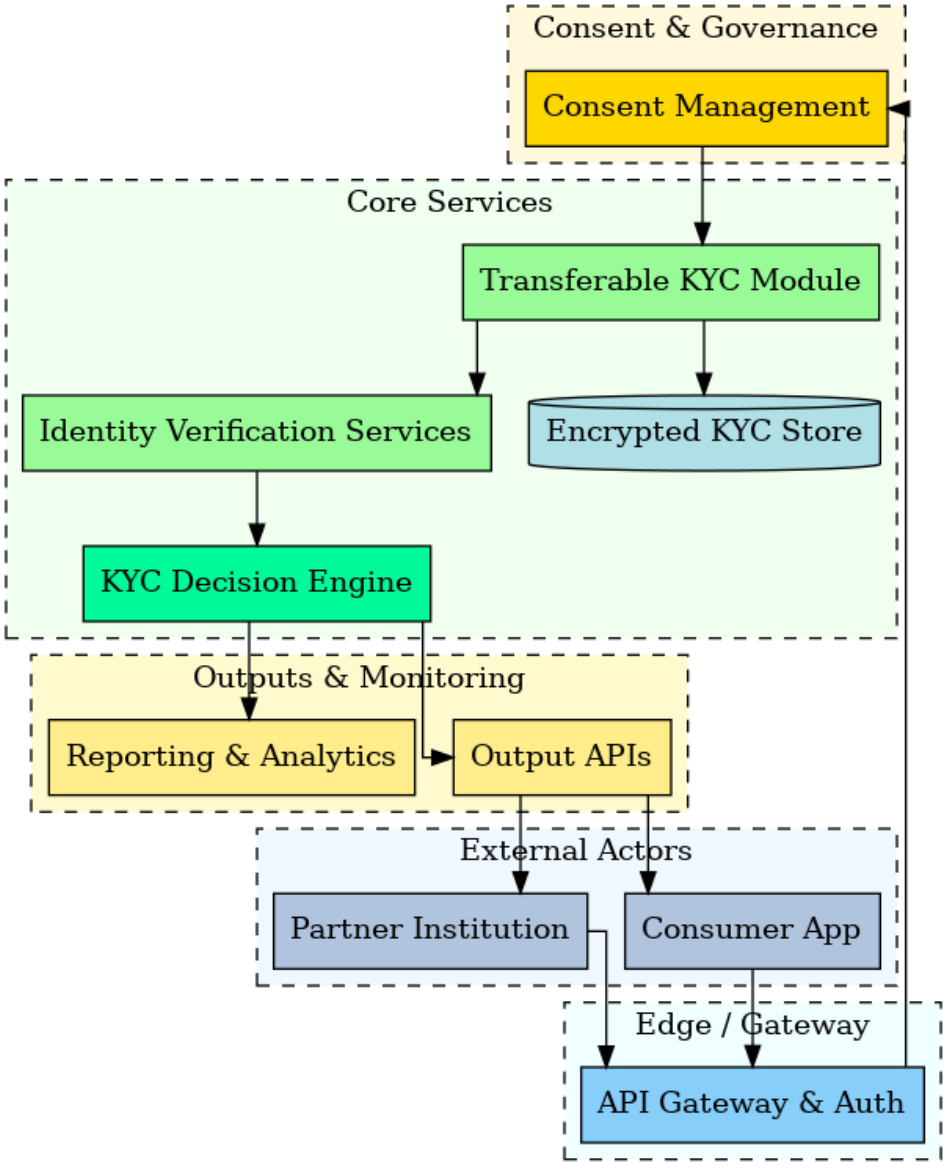


Fig1: **Transferable KYC block diagram**

# 4.1 Transferable KYC Architecture – Deep-Dive

The Transferable KYC subsystem is a **micro-service slice** of the wider Zinduka platform that lets a consumer retrieve, package, and re-use a verified Know-Your-Customer record anywhere in the ecosystem while giving institutions cryptographic proof of authenticity and regulators a clear audit trail.

Below is a component-by-component walkthrough, mapping to the diagram you downloaded.

## 4.1.1. External Actors

| Actor | Role in the Flow |
|---|---|
| **Consumer App / Web Portal** | Mobile or web front-end from which the user requests a KYC export or grants an import consent. |
| **Partner Institution** | Any relying party (bank, telco, fintech, insurer, exchange) that requests or supplies KYC data through Zinduka APIs. |

## 4.1.2. Edge & Security Layer

| Component | Key Functions |
|---|---|
| **API Gateway & Auth** | • Terminates TLS, applies rate limiting.<br>• Issues/validates OAuth 2.0 (+ PKCE for mobile) or mTLS client certificates.<br>• Injects tenant & user claims into downstream calls. |



### 4.1.3. Consent & Governance Layer

| Component | Key Functions |
|---|---|
| **Consent Management Service** | • Presents fine-grained scopes ("share photo-ID", "share address proof", "share full KYC bundle").<br>• Stores immutable consent artefacts (hash-chained ledger or private blockchain).<br>• Exposes a Consent Status API for regulators and institutions. |

**Why it matters:** *Meets GDPR/POPIA and many African data-privacy statutes that require lawful basis + user control.*

### 4.1.4. Core KYC Services

| Component | Description | Typical Tech Choices |
|---|---|---|
| **Transferable KYC Module** | Orchestrates export/import logic. Wraps records into:<br>1) **Encrypted PDF** with embedded signed JSON,<br>2) **Verifiable Credential / JWT** anchored to a blockchain hash, or<br>3) **Direct institution-to-institution API payload**. | Node.js FastAPI; integrates with OpenID → Verifiable Credentials libraries like *jwt-vc*, *DIF* spec. |
| **Identity Verification Services** | Pluggable adapters that call out to OCR, face-match, liveness-check, Sanctions/PEP, mobile-device fingerprinting. Results stored back against the user's master KYC record. | REST adapters; gRPC sidecars to 3rd-party providers. |
| **Encrypted KYC Store** | Multi-tenant datastore that keeps the canonical record. Data-at-rest encrypted with tenant-specific | Postgres + pgcrypto, or AWS Aurora + KMS; optional IPFS/private-S3 |



| | | |
|---|---|---|
| | AES-256 keys; row-level encryption for PII columns. | object store for binary docs. |
| **KYC Decision Engine** | Applies rules (e.g., *must include live selfie + face-match ≥ 96 %*) and ML confidence scores, returning states such as **Verified / Partial / Reject / Review**. | Drools / Camunda rules + Python models (LightGBM, XGBoost). |

### 4.1.5. Output & Monitoring Layer

| Component | Functions |
|---|---|
| **Output APIs** | • /KYC/export – produces PDF / VC / token.<br>• /KYC/import – ingests payload, triggers verification.<br>• /KYC/status – polling or webhook callbacks. |
| **Reporting & Analytics** | • Real-time dashboards (success rates, median export time, request origins).<br>• Audit explorer with point-in-time consent snapshot + rule path. |

### 4.1.6. End-to-End Data Flow

1. **Request** – User taps *"Share my KYC with Bank B"*.
2. **Auth & Consent** – App calls API Gateway → Consent Service prompts scopes; user signs.
3. **Package** – Transferable KYC Module pulls latest record from Encrypted Store, fetches hash of supporting docs, creates chosen artefact (PDF/VC/API).
4. **Verify & Sign** – KYC Decision Engine re-checks completeness, signs artefact with platform private key, logs signature hash to Consent Ledger.
5. **Deliver** – Artefact sent via Output API → Partner Institution (or returned to user to upload).



6. **Import (inverse flow)** – Institution posts artefact to /kyc/import; engine validates signature & hash, runs any delta verifications, and issues final KYC status.
7. **Monitor** – Every step streams to Reporting so compliance teams can prove chain-of-custody.

### 4.1.7. Security & Compliance Highlights

| Control | Implementation |
|---|---|
| **End-to-End Encryption** | TLS 1.3 in transit; AES-GCM at rest; optional user-held PGP keys for self-custody exports. |
| **Tamper Evident Proof** | SHA-256 hash written to an append-only ledger or permissioned blockchain (Hyperledger Fabric/ Besu). |
| **Least-Privilege Tokens** | Each artefact contains only the attributes the requesting party needs (e.g., age-over-18 flag instead of full DOB). |
| **Regulator Access** | Read-only API that reconstructs full consent + artefact lineage for audits. |

### 4.1.8. Scalability & Extensibility

- **Horizontal scale** – stateless micro-services behind a service mesh (Linkerd/Istio).
- **New verification vendors** – drop-in via the Identity-Verification adapter pattern; environment variable toggles per tenant.
- **Standards ready** – Designed around W3C Verifiable Credentials and ISO 20022 Payment Messages for future interoperability.



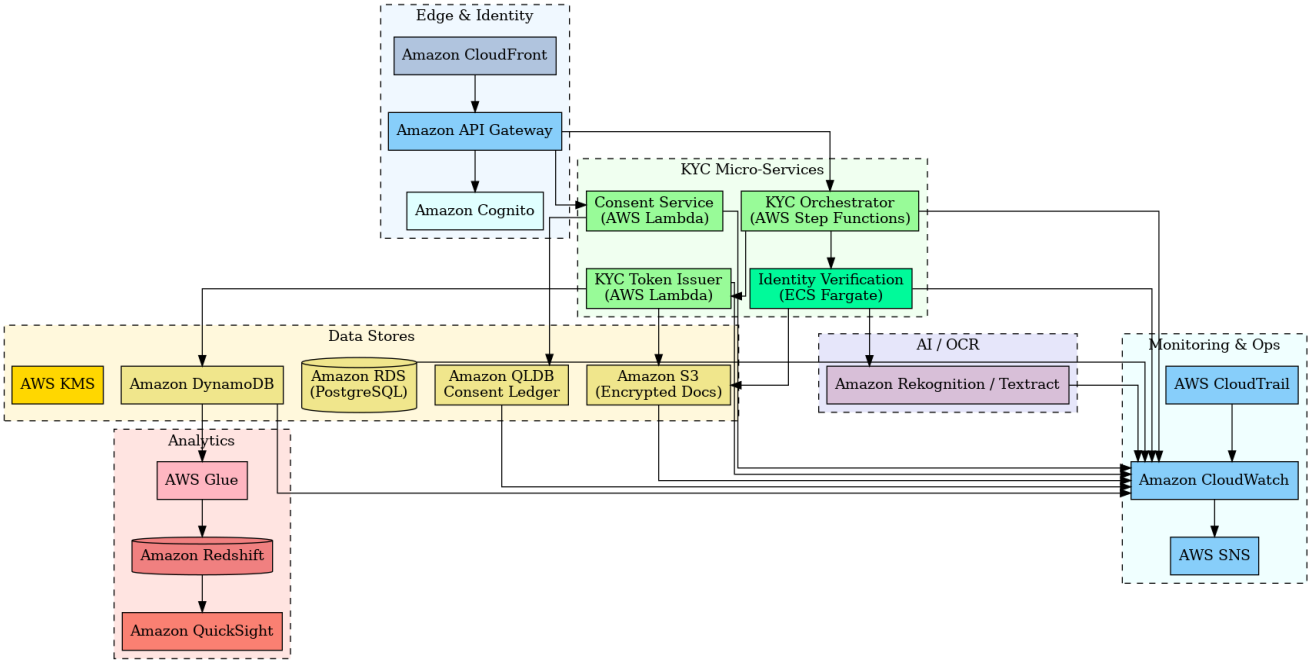


**Fig2: AWS Architecture – Transferable KYC Sub-System**

### 4.1.9

| Layer | Key AWS Services | Role in the Flow |
|---|---|---|
| **Edge & Identity** | **Amazon CloudFront** (global CDN), **API Gateway** (REST endpoints), **Cognito** (user pools, JWT) | Terminates HTTPS, accelerates traffic, authenticates consumers and partner apps. |
| **Consent & Governance** | **Consent Service (AWS Lambda), Amazon QLDB** (ledger DB) | Presents fine-grained scopes, stores an immutable, cryptographically-verifiable consent record. |
| **KYC Micro-services** | **AWS Step Functions** (KYC Orchestrator), **ECS Fargate** task for Identity Verification, **Lambda** for KYC Token Issuer | Runs liveness checks, document validation, packages KYC into a signed PDF / verifiable credential, pushes metadata to DynamoDB. |

| | | |
|---|---|---|
| **AI / OCR** | **Amazon Rekognition** (face match, liveness) & **Amazon Textract** (ID-document OCR) | Adds biometric and document authenticity signals to the verification pipeline. |
| **Encrypted Data Stores** | **Amazon S3** (secure document bucket), **DynamoDB** (KYC index), **RDS PostgreSQL** (relational look-ups), **AWS KMS** (key management) | Keeps raw docs and structured KYC data at-rest under tenant-scoped encryption keys; supports row-level and object-level audits. |
| **Analytics** | **AWS Glue** (ETL), **Amazon Redshift** (data warehouse), **QuickSight** (dashboards) | Nightly Glue jobs move KYC events into Redshift, powering adoption, verification-success, and SLA dashboards. |
| **Monitoring & Ops** | **CloudWatch**, **CloudTrail**, **SNS** alerts | Centralised metrics, logs, traces; audit trails for every API call; push notifications for failures or anomaly spikes. |

### 4.1.10 End-to-End Flow

1. **User/Institution** calls the public API; traffic accelerates through CloudFront to **API Gateway**, which validates the JWT from **Cognito**.
2. Request hits the **Consent Service**; user scopes and partner details are written to **Amazon QLDB** for an immutable audit trail.
3. **KYC Orchestrator (Step Functions)** triggers:
    a. **Identity Verification** task (ECS Fargate) → calls **Rekognition & Textract**, stores docs in **S3** and results in **DynamoDB**.
    b. On success, **KYC Token Issuer (Lambda)** signs a verifiable credential / encrypted PDF, persists a record, and returns it to the caller.
4. Raw events land in **CloudWatch Logs** and **DynamoDB Streams**, where **AWS Glue** curates them nightly into **Redshift**.
5. Risk/compliance teams explore **QuickSight** dashboards; ops receive alerts via **SNS** if error or latency thresholds are breached.



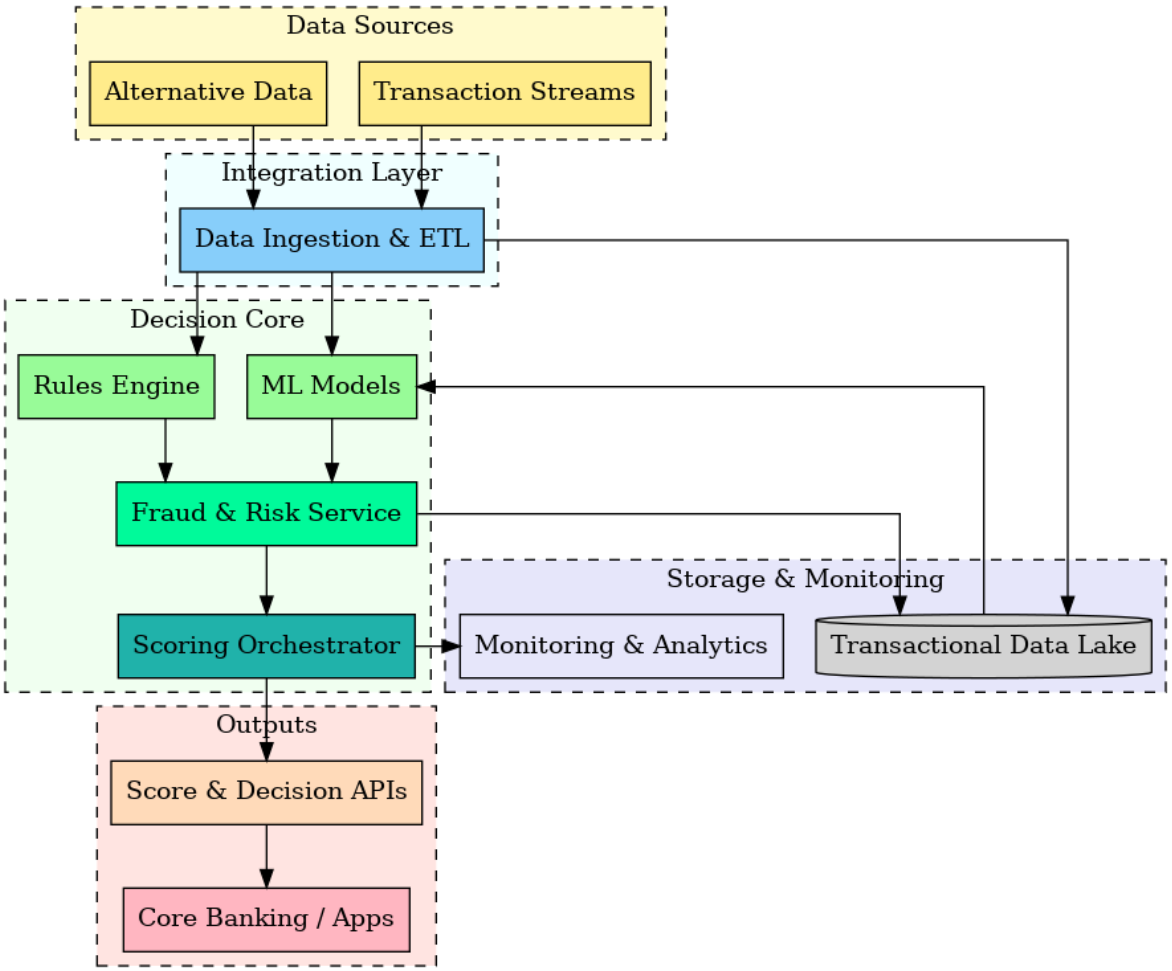


**Fig2: Fraud & Risk Decision Architecture block diagram**

# 4.2 Fraud & Risk Decision Architecture – In-Depth Explanation

The Fraud & Risk subsystem turns high-volume transactional data and alternative signals into real-time scores and decisions, protecting institutions while preserving a friction-free customer experience. It is architected as a stream-first micro-service fabric that can ingest millions of events per second, enrich them, and render a verdict in under a few hundred milliseconds.
Below is a component-level walkthrough that maps directly to the diagram you downloaded.

## 4.2.1. Data Sources (Ingest Tier)

| Source | Typical Payloads | Frequency |
|---|---|---|
| **Transaction Streams** | Authorisations, deposits, withdrawals, e-commerce payments, P2P transfers. | Sub-second Kafka / Kinesis events |
| **Alternative Data** | Telco recharge, mobile-money patterns, device reputation feeds, geolocation pings, open-banking accounts, social / web signals. | Mix of real-time webhooks & hourly batch |

## 4.2.2. Integration Layer

| Component | Key Functions | Tech Choices |
|---|---|---|
| **Data Ingestion & ETL** | • Schemas-on-read (Avro/Protobuf).<br>• De-duplication, timestamp standardisation.<br>• Feature derivation (velocity counts, merchant risk scores, location mismatch flags). | Apache Flink / Spark Structured Streaming feeding Kafka topics with Schema Registry. |



### 4.2.3. Decision Core

| Component | Description | Value |
|---|---|---|
| **Rules Engine** | • Deterministic IF/THEN, velocity & threshold rules ("≥4 card-not-present attempts in 5 min").<br>• Country-specific compliance controls. | Immediate explainability; quick tweaking by risk analysts. |
| **ML Models** | • Supervised gradient-boosting, deep-learning anomaly nets, Graph ML for network fraud.<br>• Retraining pipeline writes back to Model Registry. | Captures complex, non-linear fraud signatures that static rules miss. |
| **Fraud & Risk Service** | Orchestrates outputs from Rules + ML; attaches reason codes, confidence scores, and recommended next-step. | Central API for any upstream channel needing scores. |
| **Scoring Orchestrator** | Applies tenant-specific weightings, business days, product risk appetite, and combines multiple model outputs into a single **Decision Bundle** (score, action, explainability blob). | Let's each bank/fintech tune false-positive / false-negative trade-off without code. |

### 4.2.4. Storage & Monitoring

| Component | Roles |
|---|---|
| **Transactional Data Lake** | Immutable event store (Parquet on S3/ADLS or HDFS) for replays, forensic queries, model training, back-testing. |
| **Monitoring & Analytics** | Live dashboards (fraud rate, rule hit counts, model drift), alerting into Slack/SecOps, auto-generated SAR/STR reports. |



### 4.2.5. Output Layer

| Endpoint | Principal Consumers | Typical Latency Targets |
|---|---|---|
| **Score & Decision APIs** | Core banking switch, card issuer processor, mobile-money gateway, e-commerce checkout, loan-origination portal. | P95 ≤ 120 ms (rules-only) / ≤ 250 ms (rules + ML) |
| **Core Banking / Apps** | Act on Decision Bundle: approve, decline, step-up authentication, queue for manual review, adjust credit line, etc. | Near-synch; response loops straight to customer UI. |

### 4.2.6. End-to-End Flow

1. **Event Arrival** – A card authorisation (or mobile-money transfer) lands on Kafka topic tx.auth.
2. **Ingestion & Feature Build** – ETL enriches with device fingerprint, geo-IP, merchant MCC risk, and emits a canonical event with derived features.
3. **Parallel Evaluation**
    a. Rules Engine checks deterministic thresholds.
    b. ML Models fetch latest parameters from Model Registry and return probability scores.
4. **Score Fusion** – Scoring Orchestrator merges rule verdicts + model scores using tenant weight matrix; stamps result with UUID.
5. **Decision Dispatch** – Fraud & Risk Service posts Decision Bundle to /score API; Core-banking switch approves or declines in real-time.
6. **Persistence** – Event, features, and decision pushed to Data Lake → enables replay & retraining.
7. **Monitoring Loop** – Metrics streamed to Monitoring service; drift detector triggers model retrain if KS statistic crosses threshold.



### 4.2.7. Scalability & Extensibility

- **Horizontal scale** – stateless gRPC APIs deployed on Kubernetes, autoscaled by RPS & lag metrics.
- **Bring-Your-Own-Model** – Institutions may upload PMML/ONNX models; orchestrator auto-wraps with standard scoring interface.
- **New data feeds** – ETL layer uses schema-on-read so adding new JSON/Avro fields or entirely new topics requires **no downtime**.
- **Multi-tenant guard-rails** – Namespace isolation in Kafka + per-tenant feature store prefixes; ensures one client's data never leaks to another.

**Outcome**: A resilient, explainable, and lightning-fast decision fabric that slashes fraud losses, **unlocks responsible credit, and feeds continuous intelligence back into the business**—all while meeting the stringent regulatory and uptime demands of modern African and global financial ecosystems.

## 4.2.8 AWS Reference Architecture – Risk & Decisioning Platform



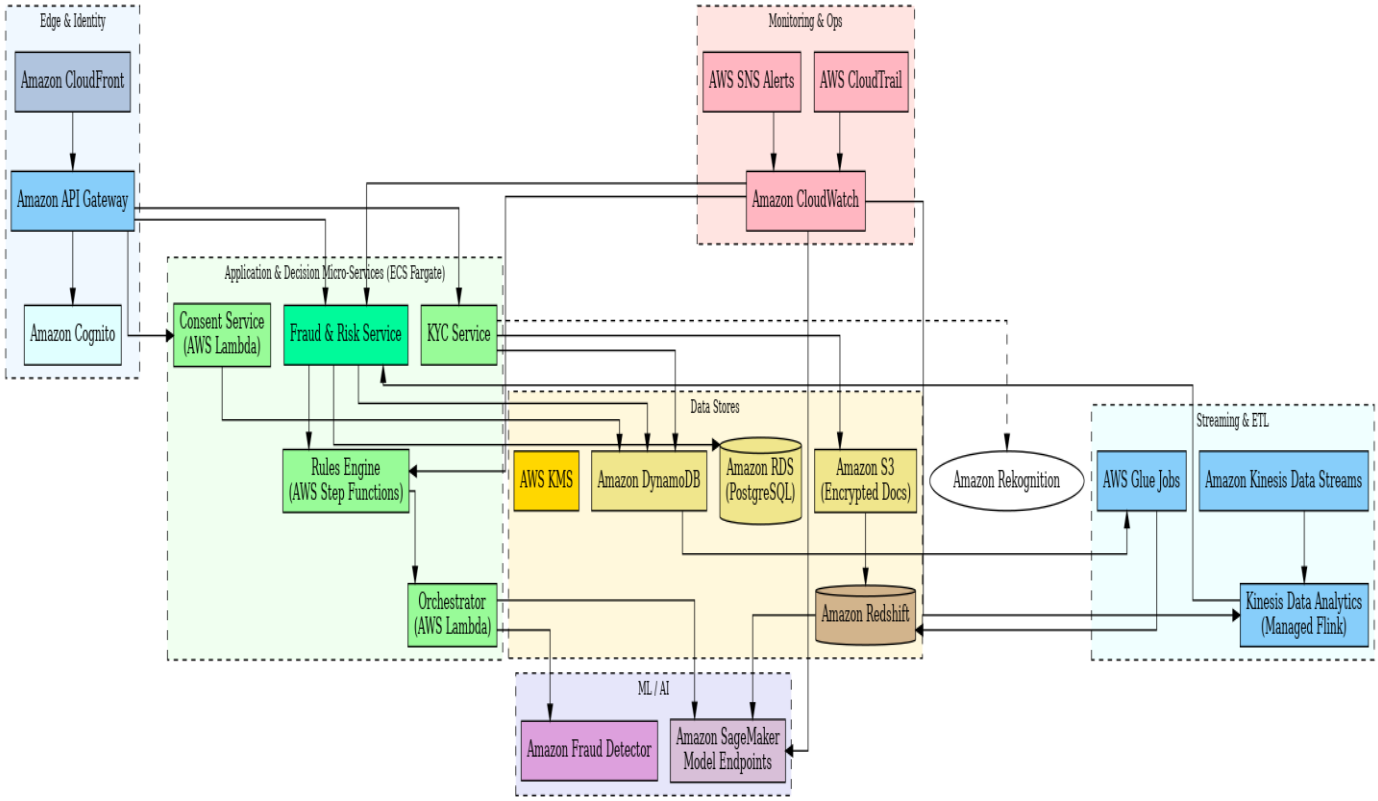


**Fig 3: AWS Reference Architecture – Risk & Decisioning Platform**

### *4.2.9 Explanation*

| Layer | AWS Services | Purpose |
|---|---|---|
| **Edge & Identity** | **Amazon CloudFront → API Gateway → Cognito** | Secures north-south traffic, provides global edge caching, OAuth2/JWT authentication and user pools. |
| **App & Decision Micro-services** *(ECS Fargate / Lambda)* | Consent Service, KYC Service, Fraud & Risk Service, Rules Engine (Step Functions), Orchestrator (Lambda) | Stateless containers/Lambdas execute core business logic; Step Functions coordinate multi-step rule flows. |
| **Streaming & ETL** | **Amazon Kinesis Data Streams / Data Analytics (Managed Flink) / AWS Glue** | Captures real-time transactions, performs stream analytics, enriches data and loads it into analytic stores. |
| **ML / AI** | **Amazon SageMaker** endpoints, **Amazon Fraud Detector** | Serves custom credit/fraud models and out-of-the-box anomaly detection, feeding scores back to services. |
| **Data Stores** | **DynamoDB** (low-latency NoSQL), **S3** (encrypted docs), **RDS PostgreSQL** (relational), **Redshift** (analytics warehouse), **KMS** (encryption keys) | Durable storage for KYC records, docs, features, and compliance data, all encrypted with tenant-scoped keys. |
| **Monitoring & Ops** | **CloudWatch**, **CloudTrail**, **SNS** alerts | Unified metrics, logs, tracing, and security audit trails; pushes alerts to Ops/SEC via SNS. |



### 4.2.10 Flow Highlights

1. Mobile/web traffic hits **CloudFront**, then **API Gateway**, which hands off JWT claims from **Cognito**.
2. API Gateway routes to consent, KYC, or fraud micro-services (Fargate/Lambda) inside a private VPC.
3. KYC Service stores documents in **S3**, metadata in **DynamoDB**, performs liveness checks via Amazon Rekognition (optional).
4. Live transactions land in **Kinesis Streams**; **Managed Flink** derives velocity features and invokes the Fraud & Risk Service for scoring.
5. Fraud & Risk Service calls:
    a. **SageMaker** endpoints for custom ML probabilities
    b. **Fraud Detector** for rule-plus-ML anomaly results
    c. **Step Functions** rule engine, then the Orchestrator to combine scores and return a Decision Bundle.
6. All events/decisions stream to **CloudWatch**, land in **Redshift** through **AWS Glue** for dashboards and model retraining.
7. **CloudTrail** + **SNS** ensure auditability and real-time alerting.



# 5. Phase wise Task & Team structure

## 📌 Phase 0 – MVP (0–6 months)

**Scope:**

- Decision Flow Builder (basic Provenir-style)
- KYC/AML Onboarding (OCR, liveness, face match)
- Basic Credit Product (simple decision + disbursement link)
- Core API Layer

| Module | % Effort |
|---|---|
| Decision Flow Builder | 30% |
| KYC/AML Onboarding | 25% |
| Basic Credit Product | 25% |
| Integration & APIs | 15% |
| Security & Governance | 5% |

👉 Focus: Core Decisioning Flow Builder, KYC/Onboarding, Simple Credit Link, API Layer.

| Role | Effort (hrs) | Months |
|---|---|---|
| Solution Architect | 80 | 4 |
| Product Manager | 80 | 6 |
| Business Analyst | 100 | 6 |



| | | |
|---|---|---|
| Backend Engineers (1.5) | 240 | 6 |
| Frontend Engineers (1.5) | 240 | 6 |
| Data Engineers | 160 | 4 |
| Data Scientists | 160 | 4 |
| Integration Specialist | 20 | 3 |
| QA/Test Engineers (1) | 160 | 5 |
| DevOps Engineer | 20 | 6 |
| | | |

# Role-Wise Responsibilities

## 1. Solution Architect

- **Design system architecture**: Microservices, data flow, security, API-first integrations.
- Define **technology choices** (Java/Spring Boot, React, Kafka, ML pipelines).
- Ensure **scalability & compliance alignment** (GDPR, RBI, POPIA).
- Guide DevOps on CI/CD pipelines, high availability, container orchestration.
- Oversight of decision flow builder + risk engine integration.

## 2. Product Manager

- Owns **roadmap & backlog** (MVP → Full rollout → Run).
- Define **acceptance criteria** for Decision Flow Builder, LOMS, Wallet, AutoML.
- Interface with business stakeholders (banks, telcos, retail partners).
- Prioritize features for compliance (KYC/AML) vs revenue (BNPL, embedded wallet).
- Track **KPIs** (approval time, fraud loss reduction, automation %).

## 3. Business Analyst

Gather requirements for **industry-specific customizations** (Telco onboarding, BNPL, SME credit).

- Write **functional specs** for onboarding flows, case management, reporting.
- Work with QA to **map test cases** against compliance and workflows.
- Support PM in preparing regulatory/governance documentation.

## 4. Backend Engineers

- Build **Decisioning Core APIs** (scoring, rules, case referrals).
- Develop **LOMS workflows** (loan application → underwriting → disbursement).
- Implement **integration adapters** (credit bureaus, telco APIs, POS).
- Maintain **audit & logging services** (linked to consent ledger).
- Support **rule versioning + rollback mechanisms**.

## 5. Frontend Engineers

- Develop **low-code Decision Flow Builder** (React Flow-based).
- Build **dashboards**: Approval rates, fraud trends, CLTV, regulatory reports.
- Implement **case management UI** (referrals, overrides, collections).
- Integrate **consent workflows** for KYC exports/imports.
- Optimize usability for **non-technical risk/fraud managers**.

## 6. Data Engineers

- Set up **data pipelines** (Kafka/Kinesis → Data Lake → Redshift/Snowflake).
- Build **feature stores** (velocity counters, device fingerprints, merchant risk scores).
- Manage **ETL/streaming enrichment** for fraud detection.
- Ensure **low-latency ingestion** (<200ms) for scoring APIs.
- Support **model retraining pipelines** with clean datasets.

## 7. Data Scientists

- Build **AutoML risk models** (credit scoring, fraud detection, anomaly nets).
- Monitor **model drift** and trigger retraining.
- Use **SHAP/LIME** for explainability of ML decisions.



- Support **behavioural biometrics/device intelligence models**.
- Collaborate with backend for **real-time scoring APIs**.

## 8. Integration Specialist

- Develop and maintain **connectors**:
  - Telco subscriber data (prepaid/postpaid).
  - Retail POS systems for BNPL.
  - Core banking APIs for disbursement/collections.
- Ensure **data mapping, validation, and error handling** across systems.
- Test and **certify third-party integrations** for compliance.

## 9. QA / Test Engineers

- Write **manual + automation test cases** for decision flows.
- Conduct **compliance testing** (audit log completeness, GDPR checks).
- Stress-test APIs for **latency benchmarks** (≤120ms rules-only, ≤250ms rules+ML).
- Regression testing for new rules/models before production.
- Validate dashboards, KYC flows, and consent logging.

## 10. DevOps Engineer

- Set up **CI/CD pipelines** for microservices & ML models.
- Manage **Kubernetes cluster** (EKS/AKS/GKE) with autoscaling.
- Configure **secrets management** (Vault/KMS), monitoring (Prometheus/Grafana).
- Automate **rollback/redeploy** for failed model/rule changes.
- Monitor **SLA compliance** (uptime, latency, throughput).

Conduct a joint **Deep-Dive Discovery Workshop** (5~ days) to freeze functional & non-functional requirements.

- Produce a refined backlog with estimated story points and sprint allocations.



• Derive a baseline burn-rate and 3-phase budget (MVP, Pilot, Scale-Up).

• Present a Not-To-Exceed (NTE) estimate within 5 working days post-workshop

# Thank You.