**Risk Management Plan – Focused on Fraud, Downtime, and Compliance**

**Key Risk Categories & Mitigation Strategies:**

| **Risk** | **Likelihood** | **Impact** | **Mitigation Strategy** |
| --- | --- | --- | --- |
| SIM Swap Fraud | High | High | Multi-factor authentication, real-time alerts |
| Regulatory Non-Compliance | Medium | High | Early engagement with CBK, Data Protection Officer review |
| Downtime during Integration | Medium | High | Blue-green deployment, rollback plan, 24/7 support |
| API Breach or Token Hijack | Medium | High | Use of OAuth2, token expiration policies, HMAC |
| KYC Data Leakage | Medium | Critical | End-to-end encryption, role-based access control, data masking |
| Customer Trust Erosion | Medium | Medium | Transparent dispute resolution channels, UX testing |
| Vendor/API Downtime (e.g., Bank) | High | Medium | Redundant APIs, failover logic, monitoring integrations |
| Fraudulent Transactions | High | High | AI-driven anomaly detection, daily limit controls, velocity checks |
| Inadequate Agent Training | Medium | Medium | Curriculum design + LMS, training effectiveness tracking |