**Preliminary Risk Assessment: Security, Fraud, Regulatory Compliance**

**Project:** Mobile Money Platform Integration for ATelco  
**Date:** [Insert Date]  
**Prepared By:** Risk Management Team

**Risk Identification & Analysis**

| **Risk ID** | **Risk Description** | **Category** | **Likelihood** | **Impact** | **Risk Level** | **Mitigation Strategy** |
| --- | --- | --- | --- | --- | --- | --- |
| RSK-01 | API Vulnerabilities Leading to Data Breaches | Security | Medium | High | High | Conduct regular security audits, penetration testing; implement WAF and IDS/IPS |
| RSK-02 | Fraudulent Transactions via Mobile Money Platform | Fraud | Medium | Very High | Very High | Implement real-time fraud detection and transaction monitoring |
| RSK-03 | Non-Compliance with AML/KYC Regulations | Regulatory | Low | High | Medium | Regular compliance training; automate AML/KYC workflows |
| RSK-04 | Delays or Failures in Payment API Availability | Operational | Medium | Medium | Medium | SLAs with providers; implement API failover and retry mechanisms |
| RSK-05 | Insider Threats with Elevated Access Rights | Security | Low | High | Medium | Enforce RBAC, monitor user activity logs |
| RSK-06 | Data Privacy Breach due to Insufficient Controls | Compliance | Low | Very High | High | Encrypt data, enforce strict access policies, conduct DPIA |
| RSK-07 | Regulatory Changes Mid-Project Impacting Scope | Regulatory | Medium | Medium | Medium | Maintain change control processes and regulatory monitoring |
| RSK-08 | User Resistance to New Mobile Money Workflows | Change Management | High | Medium | High | Conduct comprehensive training and change communication |
| RSK-09 | Third-Party Vendor Non-Compliance | Compliance | Low | High | Medium | Due diligence, contract clauses enforcing compliance |
| RSK-10 | Loss of Transaction Data during Migration | Data Integrity | Low | High | Medium | Data validation plans and backup strategies |