INTELLIGENT FRAUD DETECTION & RISK SCORING SYSTEM

Business Requirement Document

Business Analyst Project Report
Prepared By: Soundarya S
Role: Business Analyst
Date: October 2025
Version: 1.0

BUSINESS REQUIREMENT DOCUMENT (BRD)

PROJECT: INTELLIGENT FRAUD DETECTION & RISK SCORING SYSTEM

----

1. Executive Summary:

The bank's current fraud detection process is manual and slow, causing delays in identifying fraud and protecting customers. This project aims to implement an Intelligent Fraud Detection System that assigns real-time risk scores, blocks high-risk transactions, alerts customers immediately, and reduces overall fraud losses.

2. Problem Statement:

Currently fraud transactions are detected manually, which takes a long time and causes delays in blocking suspicious activity. Many high-risk transactions are missed because the system cannot detect fraud in real time. We need to upgrade the application to automatically detect at least 80% of suspicious transactions using a real-time risk engine.

3. Objectives:

- Detect suspicious transactions automatically using risk scoring.
- Reduce manual review workload by 40–60%.
- Trigger alerts, warnings, OTP or FaceID based on risk levels.
- Improve customer safety and reduce financial loss.

4. Scope:

In Scope:

- Real-time fraud detection
- Risk scoring model
- OTP / FaceID authentication
- Alerts (SMS/Email/Push)
- Fraud Review Queue
- Customer "Not Me" reporting
- Auto ticket/complaint creation
- ATM location + IP/GPS location comparison

Out of Scope:

- Redesign of bank mobile app
- ATM hardware changes
- Credit scoring features
- KYC/onboarding process

5. Stakeholder List:

Role	Responsibility
Fraud Analyst	Reviews High-risk Transactions
Compliance Manager	Handles regulatory escalations
Product Owner	Prioritizes features
Business Analyst	Requirements & Documentation
Tech Lead	System Design
QA Team	Testing & UAT
Customer Support	Customer Communication

6. AS-IS Process (Current State):

- Customer performs transaction
- Transaction is processed instantly
- Fraud team reviews transactions manually later
- Manual review takes long time
- Customer gets alerted *after* fraud occurs
- No real-time blocking or OTP check
- Fraud cases escalate slowly

7. TO-BE Process (Future State):

- Every transaction passes through risk engine
- System calculates risk (0–100)
- Based on score:
    - Low → Approve
    - Medium → Alert
    - High → OTP/FaceID
    - Very High → Block
- Customer receives immediate alert
- "Not me" → Block card + create fraud ticket
- Fraud team gets real-time dashboard
- Faster response and reduced financial loss

8.High-Level Business Requirements:

- System must detect suspicious transactions in real time
- System must assign risk score from 0–100
- System must compare IP, GPS, ATM location, device, amount, patterns
- System must trigger OTP/FaceID for high-risk
- System must block very high-risk transactions automatically
- System must send alerts instantly
- System must allow customer to block card immediately
- System must create auto complaint
- System must route high-risk to Fraud Queue
- System must show fraud dashboard

9. KPIs / Success Metrics:

- Reduce fraud losses by 30%
- Reduce manual review by 50%
- Detect 80% suspicious transactions automatically
- Alerts delivered within 5 seconds
- Fraud detection speed improved by 70%

10. Risks & Assumptions:

Risks:

- Too many false positives
- OTP overload may frustrate users
- Network delay in SMS/Email
- Missing location/device data

Assumptions:

- All customer contact details updated
- Bank core system supports real-time API
- Fraud rules will be fine-tuned