Process Mapping – AS-IS & TO-BE

Purpose:

The **AS-IS process** shows how fraud detection currently works (manual, reactive).

The **TO-BE process** illustrates the improved, more automated, insight-driven system.

AS-IS Process: Current Manual Fraud Handling

```
                          ┌─────────────────────────┐
                          │ Customer Makes Transaction │
                          └─────────────────────────┘
                                      │
                          ┌─────────────────────────┐
                          │  Transaction Enters System │
                          └─────────────────────────┘
                                      │
                          ┌─────────────────────────┐
                          │ Transaction Flows into Analytics Layer │
                          └─────────────────────────┘
                                      │
                          ┌─────────────────────────┐
                          │ Stored in Data Warehouse/Mart for Processing │
                          └─────────────────────────┘
                                      │
                          ┌─────────────────────────┐
                          │ Rule-Based & Behavioral SQL Logic Applied │
                          └─────────────────────────┘
```

- Detects: Multiple failed logins
- Detects: Unusual transaction time
- Detects: New device or location
- Detects: First-time high-value amount

Each Transaction is Scored for Risk

Risk Score Triggers Alert or Dashboard Tag

Only High-Risk Transactions are Flagged

Lower Risk Gets Monitored Silently

Fraud Dashboard Displays Summary

- Power BI Dashboard Shows: Real-time Fraud Count
- Power BI Dashboard Shows: Alerts by Geography/Device/Time
- Power BI Dashboard Shows: Risky Customers List
- Power BI Dashboard Shows: Trends Over Time
- Fraud Team Takes Action

- Team Focuses Only on Top-Priority Cases
- False Positives are Reduced
- Cases are Documented and Traceable for Compliance