← Back to Credit Unions CREDIT UNIONS · WORKFLOW

Fraud detection and transaction monitoring

Automatically monitors all member transactions in real-time to detect suspicious activity and fraud patterns, triggering immediate alerts and protective actions to safeguard member accounts and credit union assets.

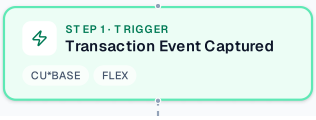
Download PDF | Get Your Blueprint

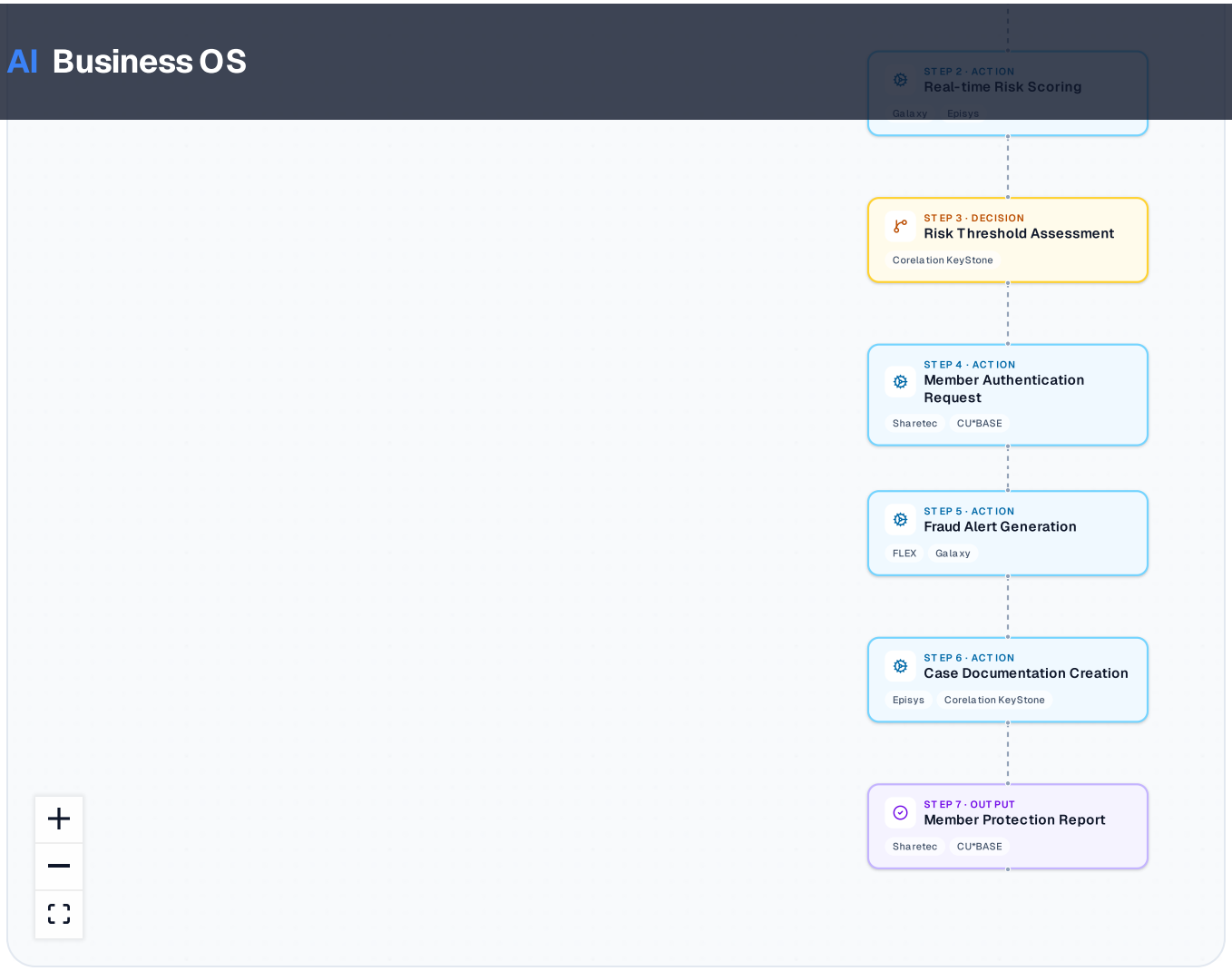
WORKFLOW TRIGGER

Member transaction is initiated through any channel (ATM, debit card, online banking, mobile app, or in-branch)

Visual Flow

Each node represents an automated step. Connections show how data and decisions move through the workflow.





Step-by-Step Breakdown

Detailed explanation of each automated stage in the workflow.

1

TRIGGER

Transaction Event Captured

A member transaction is detected and captured from the core banking system. Transaction details including amount, location, merchant, and

member behavior patterns are extracted for analysis.

CU*BASE FLEX

2

ACTION

Real-time Risk Scoring

The transaction is analyzed against member's historical patterns, velocity rules, and fraud algorithms to generate a risk score. Geographic, temporal, and behavioral anomalies are evaluated.

Galaxy Episys

3

DECISION

Risk Threshold Assessment

The calculated risk score is compared against predefined thresholds to determine if the transaction should be approved, flagged for review, or blocked immediately.

Corelation KeyStone

4

ACTION

Member Authentication Request

For medium-risk transactions, an automated verification request is sent to the member via SMS, email, or mobile app push notification. Member response is captured and validated.

Sharetec CU*BASE

5

ACTION

Fraud Alert Generation

High-risk transactions trigger immediate fraud alerts to the credit union's fraud team and potentially law enforcement. Member accounts may be temporarily restricted pending investigation.

FLEX Galaxy

6

ACTION

Case Documentation Creation

All fraud detection events are automatically documented with transaction details, risk factors, and actions taken. Compliance reports are generated for regulatory requirements.

Episys Corelation KeyStone

7

OUTPUT

Member Protection Report

A comprehensive summary of protective actions taken is generated including transaction status, member notifications sent, and any account restrictions applied.

Sharetec CU*BASE

Outputs

- Transaction approval or denial decision

- Fraud alert notifications to staff and members
- Compliance documentation and case files
- Account protection status updates

Key Metrics

- False positive rate
- Fraud detection accuracy percentage
- Average response time to suspicious transactions
- Member satisfaction with security measures

Tools & Integrations

- CU*BASE
- FLEX
- Galaxy
- Episys
- Corelation KeyStone
- Sharetec

AI Business OS

Actionable AI implementation strategies for business leaders ready to transform their operations.

COMPANY

About

Industries

RESOURCES

Articles

CONNECT

MVP.dev

LinkedIn