

Fraud Management

Business Scenarios
Special Presentation: Mitigations from a provider perspective



Agenda



- Introductions
- Goals & Objectives
- Scope & Approach
- Deliverables / Outputs
- Teams, Roles & Responsibilities
- Current Status & Next Steps
- Special Presentation: Mitigations from a provider perspective

Introduction



Business Scenarios Project
Management

Charity Elkins, MBA
Regional Director, Crosslake
Technology



Special Presentation: Mitigations
from a provider perspective

Mercy W Buku LLM (UOL), CAMS,
ACIB (UK)
Anti Money Laundering and CFT
Practitioner and Consultant Digital
Financial Services

Project Goals and Objectives



- Bring together recommended partners to develop a cohesive business requirements best-in-class fraud management.
 - Develop primary and secondary fraud use cases and typologies that impact the poor.
- Create a collaborative view on how to reduce real-time payment fraud in developing countries.
- Make available as a public good and may inform the development of solutions by participants in the group, or external parties.

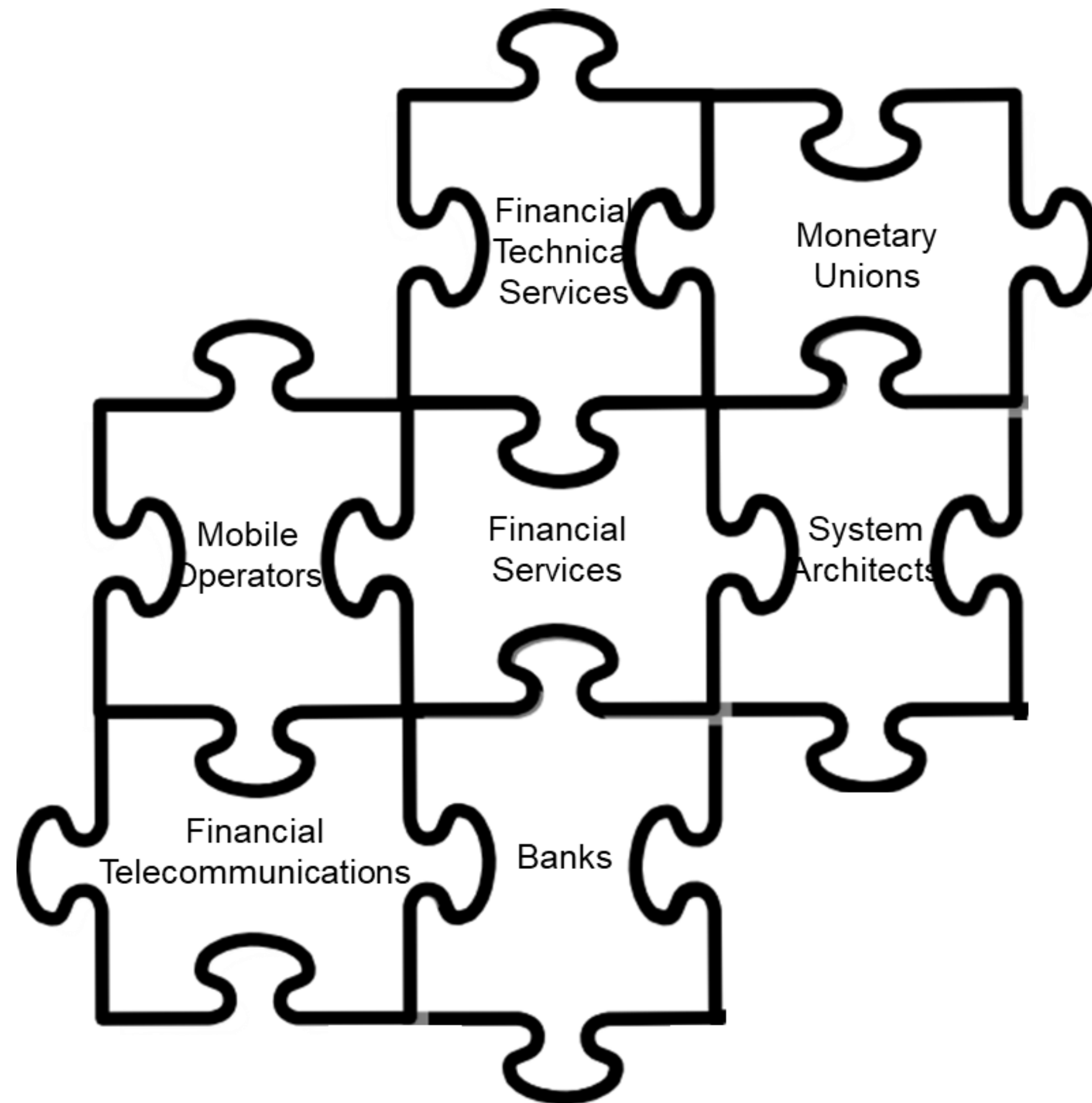
Scope and Approach



- Sub-Saharan geographies
- e-money providers
- Local and regional banks as users of fraud management tools
- High-level use cases
 - Transaction fraud (e.g., stolen credentials, fraudulent transactions)
 - Third-party fraud
 - Social engineering fraud

Current Partnerships

Industries and Companies



- Working group members include real-time schemes, banks, e-money issuers, and fraud software providers.
- BankservAfrica - Largest automated clearing house in Africa.

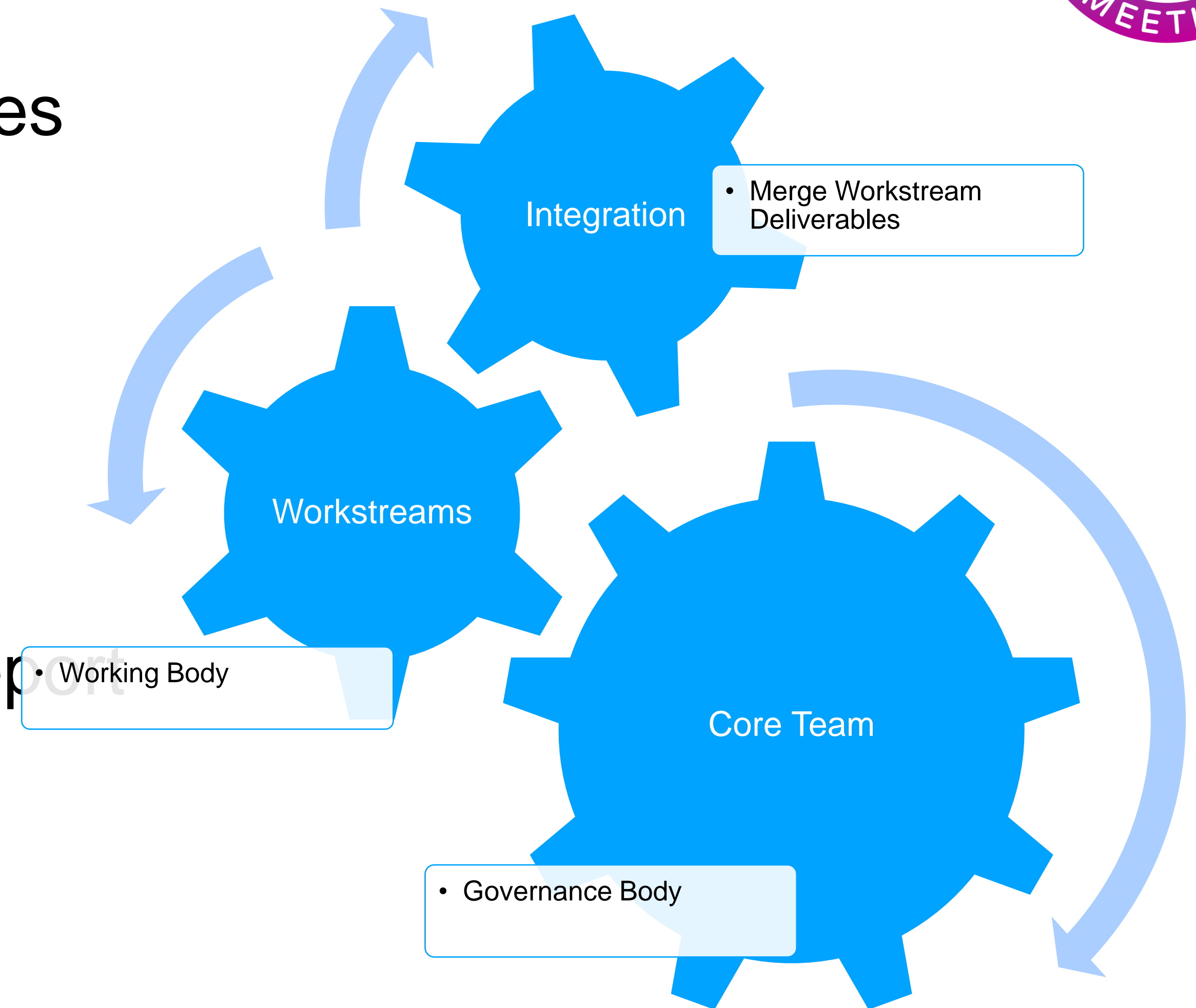
JoPACC – The Jordan Payments and Clearing Company develops and enhances digital retail and micropayment systems.

Montran - Comprehensive platform-independent payment, clearing, and settlement solutions platform-independent.
- Sybrin - Provides a framework for rapid digital transformation.
- Individual industry consultants provide oversight and governance.

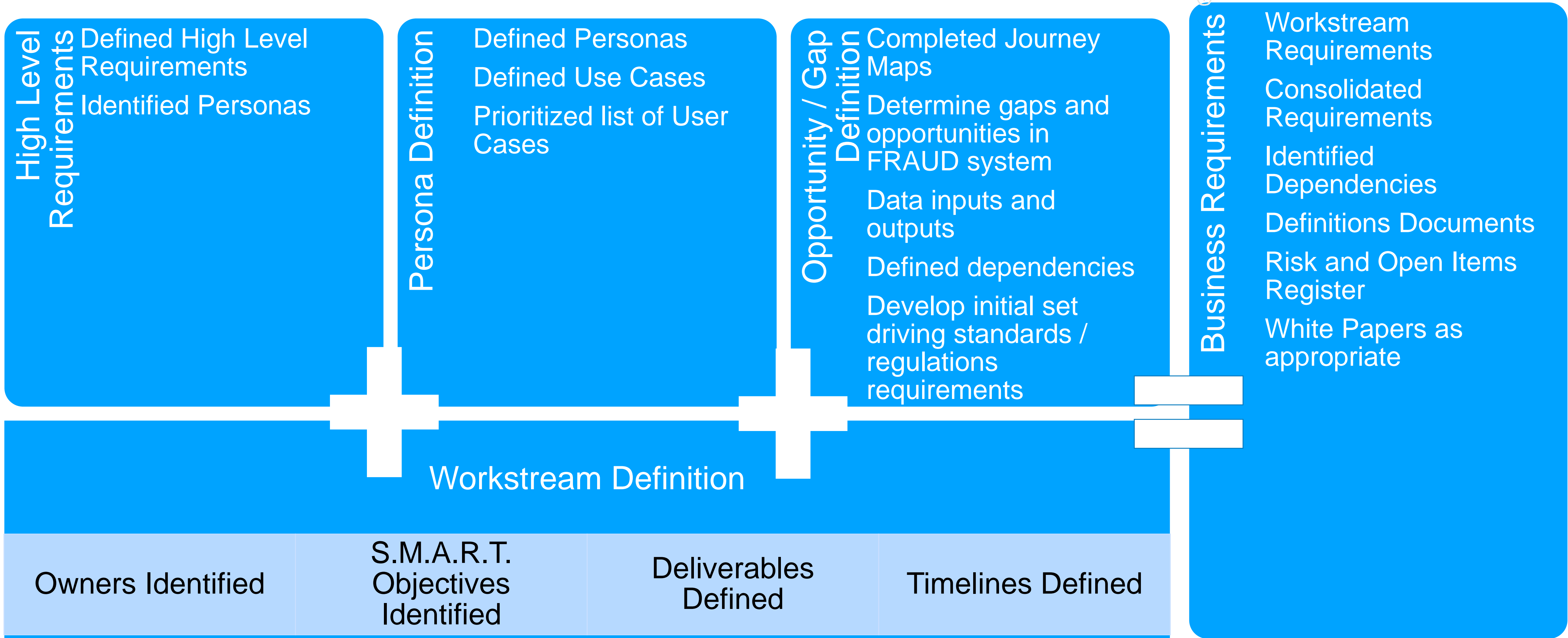
Project Management Approach



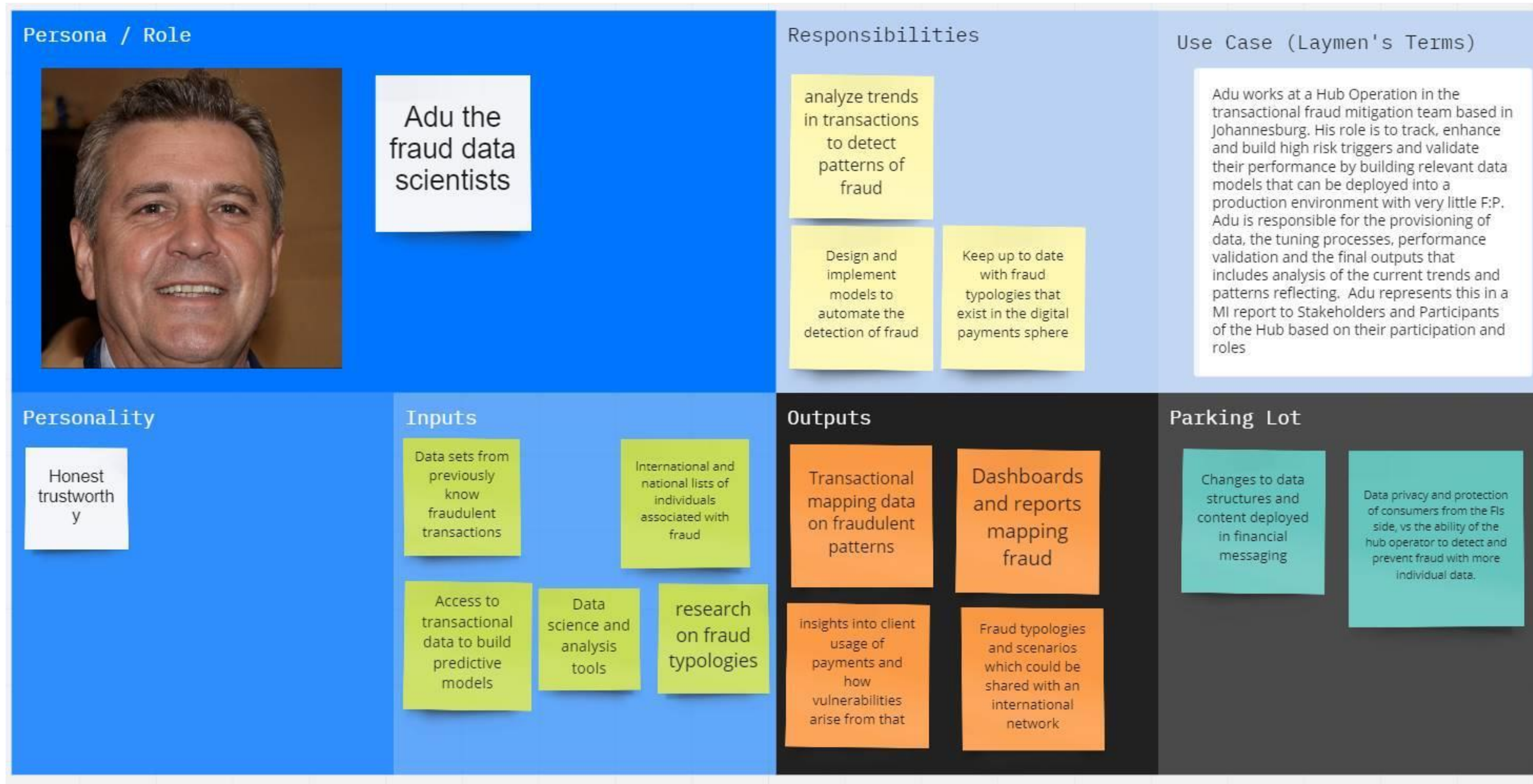
- Teams, Roles, and Responsibilities
 - Core
 - Workstreams
 - Governance / Oversight
 - Industry Expertise Sharing
- Workstream Check-Ins
 - Weekly / Bi-Weekly
 - Training / Status/ Help Wanted
- Workstream Deliverables and Report Outs Cadence
- Workstream Integration
- Business Requirement Delivery
 - 1HCY22



Deliverables and Outputs



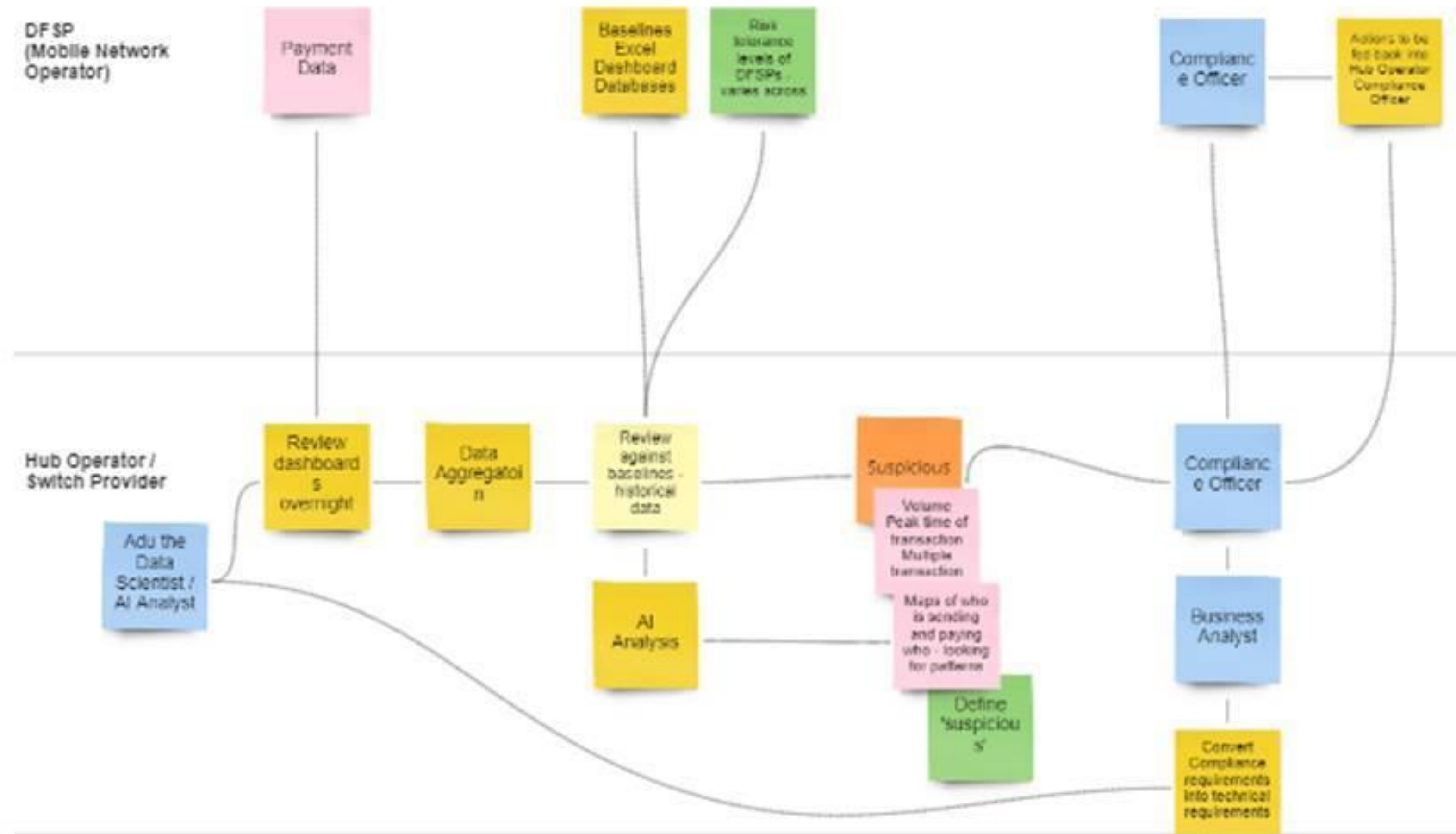
Persona Examples



Journey Map Example



- Focus on the User
 - Persona Swim Lanes
 - Processes
 - Data Inputs / Outputs
 - Key Dependencies
 - Gaps Identification



Business Requirements Example



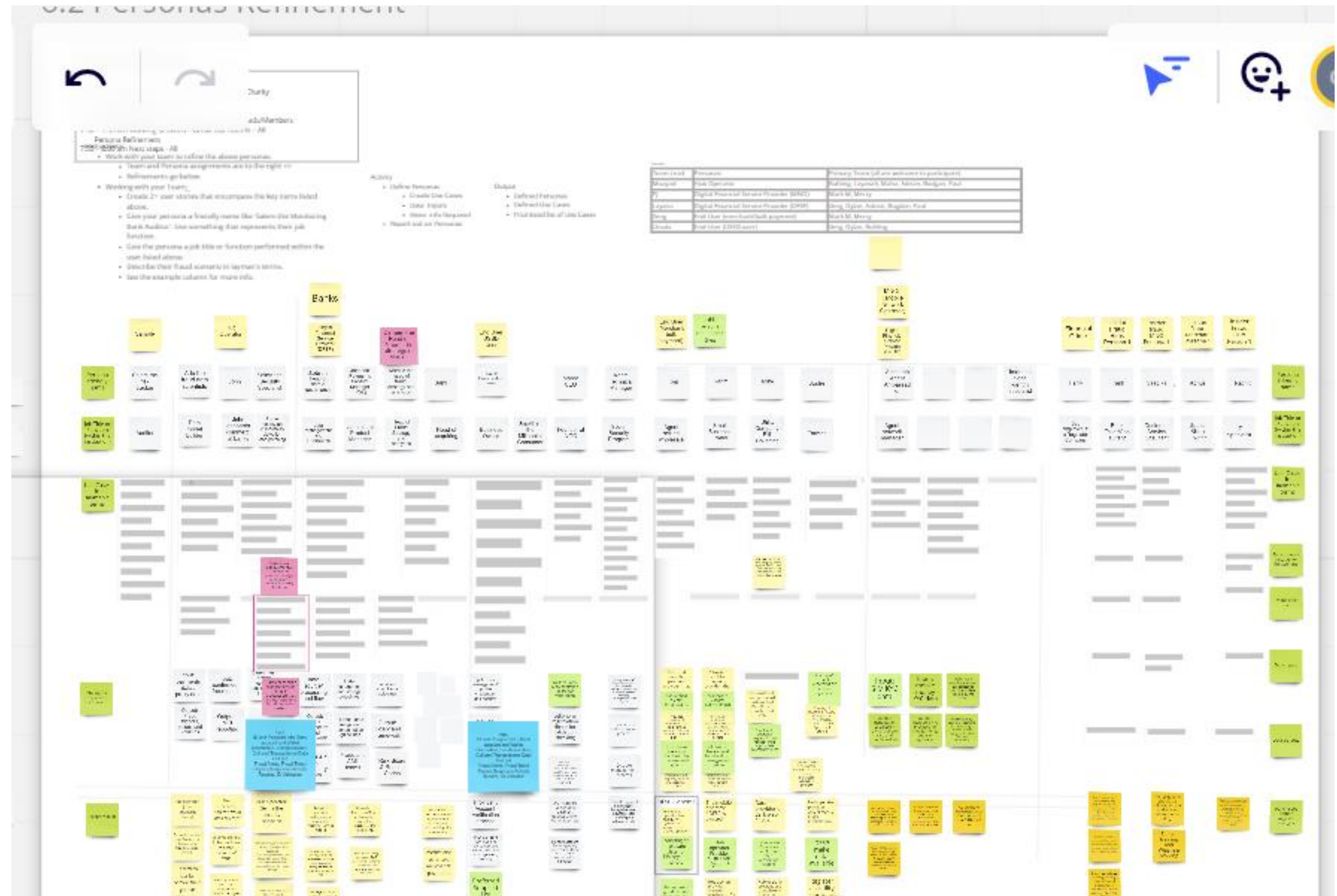
- Mapped to Journey Maps
- Business Requirements
 - Description
 - Operations
 - Inputs/Outputs
 - Error Handling
 - User Needs
 - Acceptance Criteria
 - Test Approach

BSA_BR002 - 1 A solution to limit and prevent debit order abuse on client accounts	
Description	System generated alerts to be sent to a bank's client whenever their account is being accessed/viewed and debit/stop orders being loaded
Operations	The bank teller servicing a client logs into to the enterprise banking system to perform an account lookup The client is prompted to provide one of their unique identifiers to the bank teller The bank teller launches an account look up/search An alert is sent to the client's mobile device with "accept" or "decline" options (The alert asks the client if they give authorization to an account search on their details) The bank client accepts the request to have the account search done The customer banking profile page/screen is displayed with the client's details
Inputs	Unique client identifier "Accept and/or Decline" answer options
Outputs	An alert on the client's mobile device Successful account lookup/search
Error Handling	Alternative authentication method must be used by the bank teller to get information from the client with the client being aware of what is being asked of them e.g. security questions
User Need	To restrict debit/stop order abuse on unsuspecting bank clients
Benefits	A bank's good reputation is maintained
Acceptance Criteria	The bank teller must have an active user profile on the bank's enterprise account records system The client must be at the branch to give the bank teller sensitive account/personal information The bank's client must verify themselves by means of a personal identification document issued to them to prove that they are indeed the right client requesting bank teller services

Collaboration Tools



- Miro Fraud Workspace
 - Enables remote team collaboration.
 - Mirrors working in a conference room with whiteboards.
 - Sticky Notes
 - Synchronous and asynchronous work
 - Single system of record
 - Infinite whiteboard
- Zoom
 - Enables break out rooms for sub-team collaboration



Status By Workstream

Target completion 6/2022

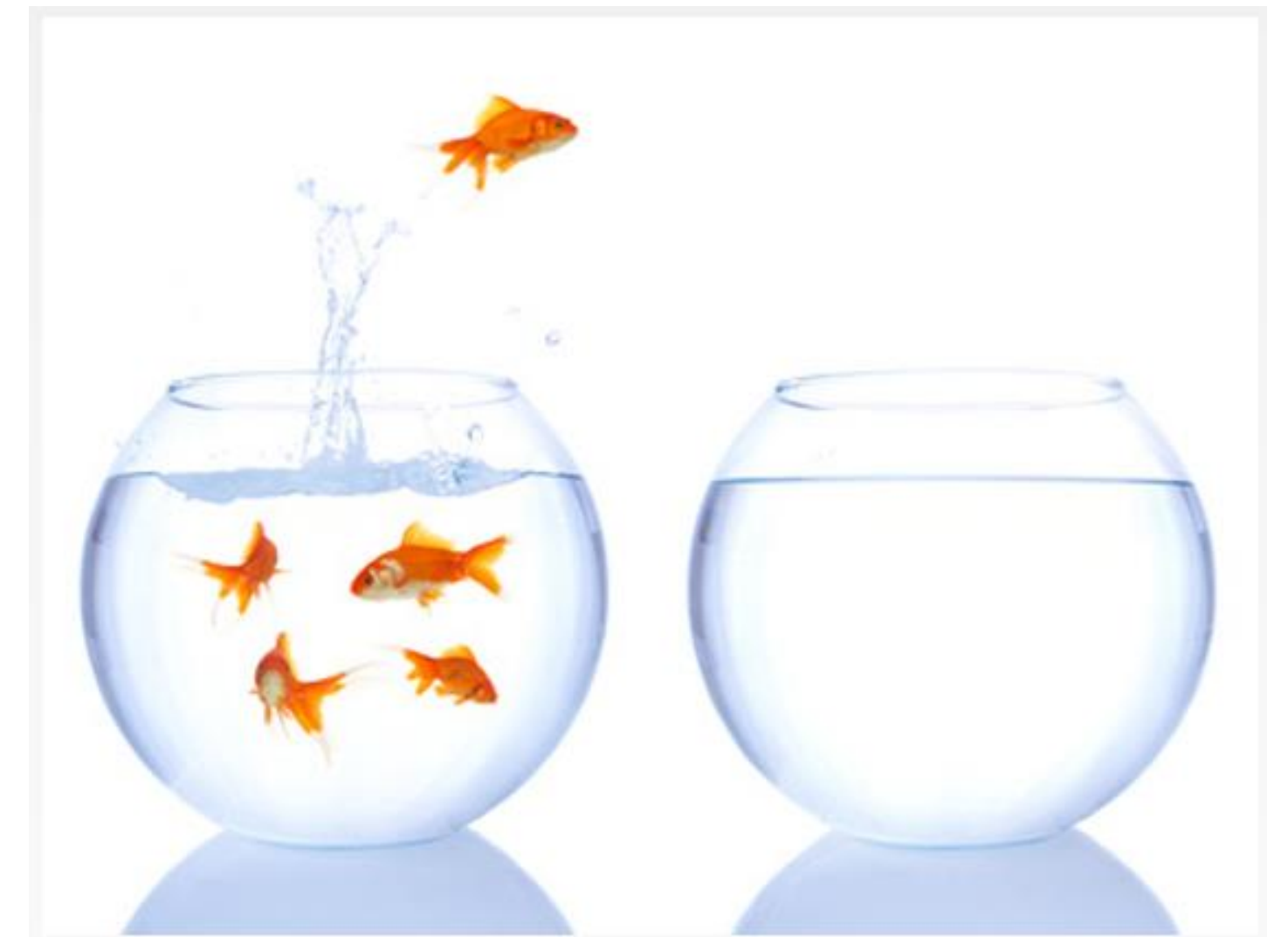


WORKSTREAM	WORKSTREAM OWNER	BA RESOURCE	PERSONA CARDS	JOURNEY MAPS	BUS. REQ. % COMPLETE	COMMENT
FINANCIAL CRIME	BankservAfrica	Ursula Pearson Selby Gumbi	✓	✓	80%	
HUB OPERATOR	JoPACC	Layanah Wreikat Moayad Ghannam	✓	✓	40%	
END-USER	BankservAfrica	Ursula Pearson Selby Gumbi	✓	✓	0%	Will begin once Financial Crime nears completion.
CENTRAL BANK	Montran	Adrian Carcu	✓	✓	45%	
DFSP BANKS	Sybrin	Greg McCormick Arthur Munjeri	✓	✓	20%	

Next Steps



- Continue working on Business Requirements
- Report out to Governance team
- Possible Collaborative FTF Meeting in Q22022.



Next Up



Mitigations from a provider perspective

Presented By:

Mercy W Buku LLM (UOL), CAMS, ACIB
(UK)

Legal and Risk Management Consultant
Digital Financial Services

