payments
strategy
forum

November 2017

Payments Transaction Data Sharing and Data Analytics – Strategic Solution – Solution Implementation

Contents

Background

Payments in the UK can be made using multiple payments mechanisms (e.g. Bacs, CHAPS and Faster Payments). These payments systems can be used by criminals to launder stolen or misappropriated money, masking the trail of funds and making its origin unclear. This laundered money can be used to fund terrorism or organised crime, or allow criminals to profit from fraud.

In the Payment Strategy Forum's (the Forum) strategy published in November 2016, 'A Payments Strategy for the 21st Century' (the Strategy), the Forum proposed a Payments Transaction Data Sharing and Data Analytics solution to help fight financial crime that occurs through the misuse of payments systems. The solution will enable visibility across different transactional data sources to create a rich data repository and analytical capability.

The objective of the solution is to detect and prevent current and future financial crime by creating an industry-wide capability to analyse end-to-end payment transaction data from all retail interbank payment mechanisms in conjunction with other relevant sources of diagnostic information. Examples of financial crime solutions being targeted include: the identification of money mule accounts and the ability to return stolen money.

The Forum has recognised that whilst its focus is on strategic solutions, the current industry led and funded tactical solution should be seen as an opportunity to develop and test concepts that could form part of a strategic solution.

The tactical solution was initiated in early July with FPSL as a delivery body for implementation; this solution will transition into the NPSO at the end of 2017. The tactical solution will provide early benefit to aid the detection of money mule accounts, and pilot methods for funds repatriation. The tactical solution will run as an interim service, until the strategic solution is implemented.

In July 2017, the Forum consultation 'Blueprint for the future of UK payments' gave an initial proposal for the strategic solution. Following these responses, the Forum conducted further work and discussion to develop the solution. This document describes our suggested implementation approach to be followed by the future solution delivery body in order to create the strategic solution. This document includes the additional information gained from responses to the Forum consultation, as well as the further work of the Forum's working group.

1 Overview of Strategic Solution

1.1 Objective of this Document

The 'Payments Transaction Data Sharing and Data Analytics" strategic solution is a culmination of a number of activities begun in December 2015 with the aim of handing over to the New Payments System Operator (NPSO) in December 2017. Figure 1 below illustrates the timeline.

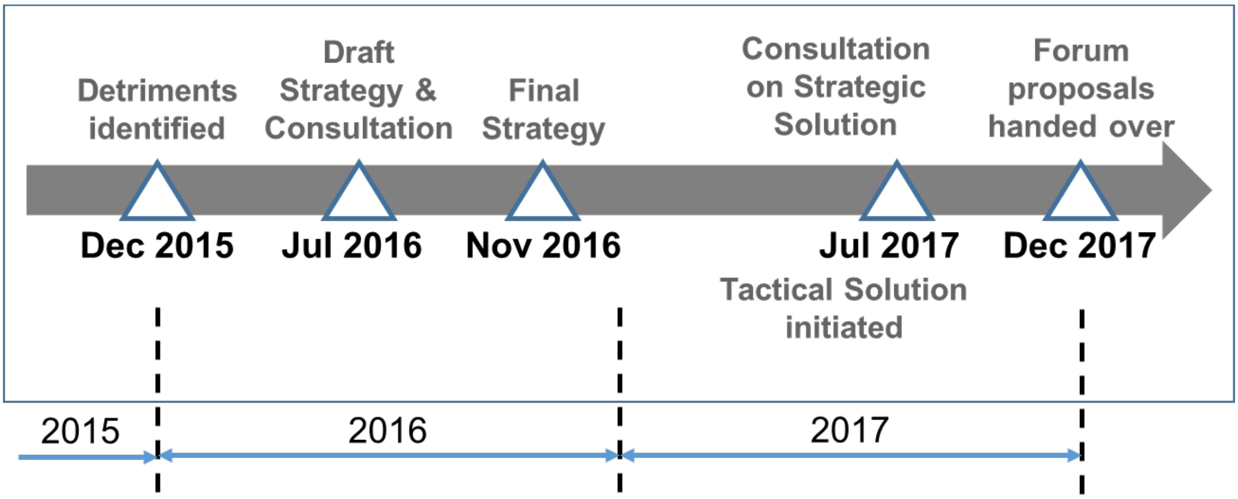
Detriments identified
Draft Strategy & Consultation
Final Strategy
Consultation on Strategic Solution
Forum proposals handed over
Dec 2015
Jul 2016
Nov 2016
Jul 2017
Dec 2017
Tactical Solution initiated
2015
2016
2017

Figure 1 Financial Crime Working Group – Activities Timeline

This document outlines the suggested implementation approach to be developed further by the solution delivery body overseen by the governance body. This implementation approach will be reviewed and validated with appropriate stakeholder groups.

A companion document details the suggested scope of the strategic solution, including the standards to be developed, and how the solution should be overseen by a governance body.[1]

2 Implementation Approach

Implementation will be conducted as two parallel strands; one for messaging standards definition and establishing the analytics ecosystem for payments transaction analysis and one for incorporating the solution into the design and go live of the NPA.

This implementation approach is underpinned by key principles that will guide solution development and delivery:

- The implementation should be planned as a phased approach with initial capabilities and a programme of enhancements and expansions planned for subsequent years.
- Regulators and other relevant bodies such as the Joint Money Laundering Intelligence Taskforce (JMLIT), Joint Fraud Taskforce (JFT), UK Finance and the Information Commissioners Office (ICO), should be fully engaged throughout the design / build / implement stages and be invited to participate and make use of the new capability.
- An economic model will be developed which may be based on usage of, and contribution to the solution.
- The analysis of the data must be carried out under tightly controlled conditions by regulated entities using approved analytical tools and in compliance with data protection, information security and competition regulations.
- The learnings from the tactical solution should be incorporated into the strategic solution. It should not however be limited to the tactical solution's constraints, participants or suppliers.

[1] "Payments Transaction Data Sharing and Data Analytics – Strategic Solution – Scope and Governance Oversight.pdf"

The above principles can be reviewed and amended as part of the solution development but only under clear and independent governance.
Identification of and resolution of legal and regulatory constraints to the acquisition, analysis and usage of the data will need to be considered as part of detailed scoping and implementation planning. This may limit the scope of the solution capabilities.

3 Indicative Implementation Timeline

The strategic solution implementation will be split into two parallel strands of activity. The intent is to ensure the establishment of an effective analytics data sharing environment, which could provide cross industry benefits in the short term and is not dependent on the implementation of the NPA. Figure 2 details the expectations for each strand.

Strand 1 **Standards definition and data sharing**	**Strand 2** **Incorporate solution into NPA design for FPS, Bacs ICS data**
• Approaching analytic vendors and data provider organisations for input into messaging solution. • Defining the messaging technical standards • Defining data quality and data standards to provide full coverage of payment journeys for financial crime analysis. • Defining and implementing methods and controls by which analytics vendors can access payments data for fraud prevention. • Ongoing exploration of legal considerations for solution implementation, either regarding the sharing of information or the ability to effectively take action from the derived insight.	• Ensuring that the solution is built into the work of the NPA and the re-procurement of current scheme infrastructure. • Including data quality designs so that the NPA captures the most suitable data to fight financial crime. • Re-procuring the tactical solution to integrate to Strand 1 standards and work with NPA. • Once live, the NPA would plug into the analytics solution standards provided by Strand 1.

Figure 2 - Two Stranded Approach to Implementation

Figure 3 below shows the key steps of strand 1 and of strand 2 of implementation, together with indicative timescales.

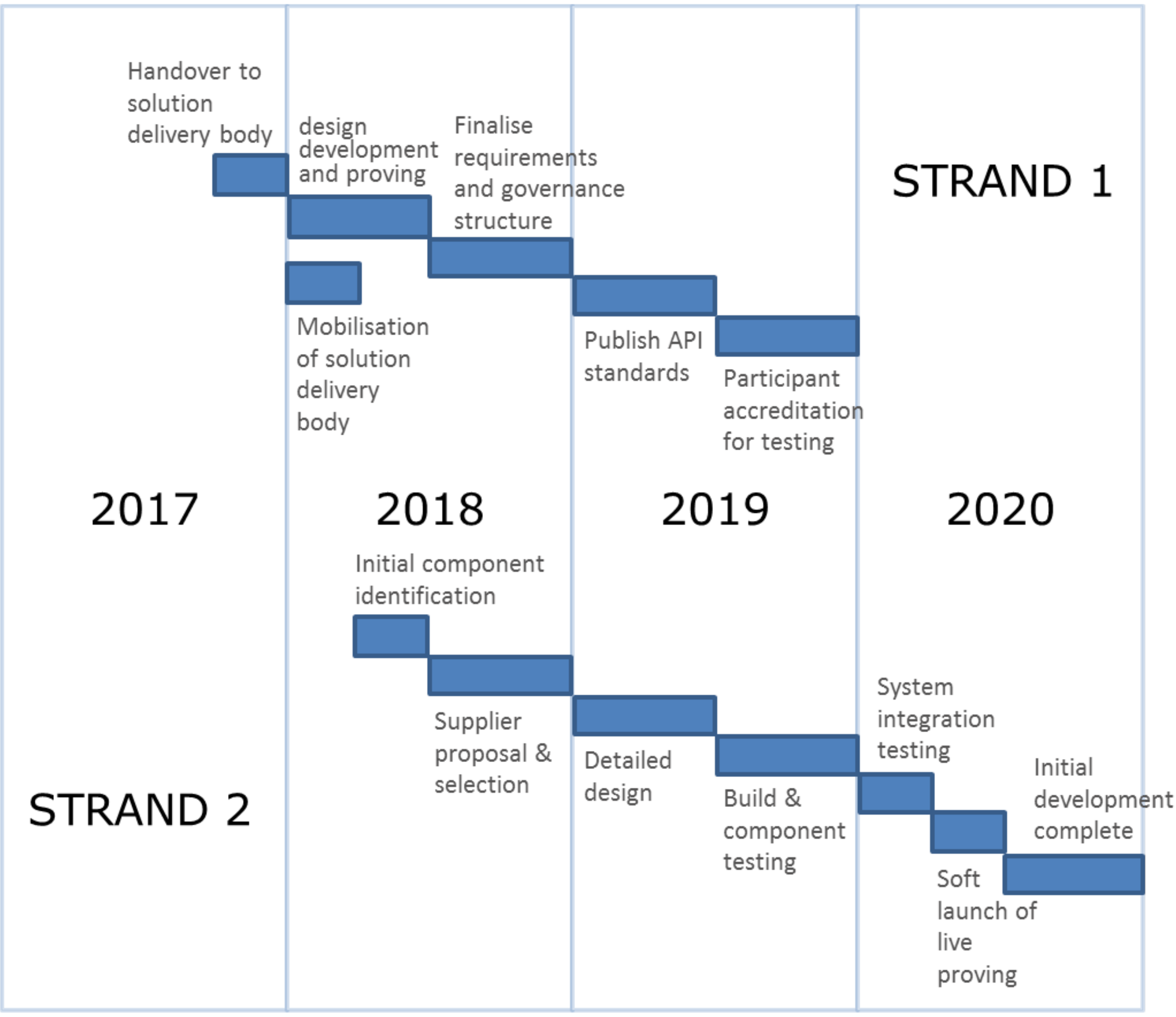
Handover to solution delivery body
design development and proving
Finalise requirements and governance structure
STRAND 1
Mobilisation of solution delivery body
Publish API standards
Participant accreditation for testing
2017
2018
2019
2020
Initial component identification
Supplier proposal & selection
Detailed design
Build & component testing
System integration testing
Initial development complete
Soft launch of live proving
STRAND 2

Figure 3 - Strand 1 & Strand 2 Timeline

Strand 1

The indicative implementation timelines foresee a design development and proving exercise in order to understand the usage of messaging types and potential industry use cases whilst simultaneously establishing a strong independent governance structure and solution delivery body. Activities to define the API and other required standards and controls should complete by H1 2019 with the ability for authorised participants to start using the messaging standards by the end of 2019.

Strand 2

Parts of the strand 2 timeline may be dependent or subject to change based on the ongoing delivery timescales for the NPA. However, as an indicative timeline, based on current NPA timelines, the strategic solution detailed design would be completed by H1 2019 using fully competitive Request for Information (RFI) and Request for Proposal (RFP) processes which include the strategic solution requirements, system build and testing by H2 2019, with the first implementation live during 2020.

The high-level work plan outlined in this document must take planned industry and existing regulatory developments into account.

Re-procurement of the tactical solution

At the appropriate time the current industry tactical solution for transaction analytics should be re-procured using appropriate competitive processes to integrate to strategic solution design. This will include the usage of standards established during Strand 1, usage of any standardised services as required, and consideration to the Strand 2 NPA implementation.

4 Strand 1 - Implementation Steps and Activities

With implementation split into two parallel strands of activity, Strand 1 focusses on establishing:

- The standards that will allow participants to send and receive messages related to this solution.
- The operating model that will define how participants will interact, operating within the current legal environment.
- The requirements (if any) for legislative change to enable a greater number of use cases or more effective information sharing.

The implementation plans for Strand 1 can be further broken down into the following key activities which are outlined in Table 1 and are described below.

Period	Step		Activity
Q4 2017	**Step 1:** Handover to solution delivery body	1.1	PSF solution work stream post consultation deliverables are formally handed over to, and accepted by, the agreed solution delivery body for development and implementation
Q1 2018	**Step 2:** Mobilisation of solution delivery body	2.1 2.2 2.3	Project teams and detailed plans including management structures and support arrangements are designed and put in place, together with appropriate funding and governance procedures and responsibilities. Establishment of stakeholder working groups. Establishment of ongoing legal work stream.
H1 2018	**Step 3:** Design Development and Proving	3.1	Design development and proving will be conducted to understand the usage of messaging types and potential industry use cases
H2 2018	**Step 4:** Finalise requirements and governance structure	4.1	Following the completion of the design development and proving, the details of the solution governance structure, operating model, standardised services and API messaging requirements should be near final and appropriately documented.
H1 2019	**Step 5:** Publish API standards	5.1	Having established the messaging requirements, API standards are developed and published.
H2 2019	**Step 6:** Participant authorisation for testing	6.1	The process for participant authorisation is established and enacted to enable the first participants to be included in the solution testing activity.

Table 1 Recommended implementation approach.

Step 1: Handover to Solution Delivery Body

Activity 1.1: Handover

This document and its companion document as described in section 1 will facilitate handover to a solution delivery body which will be responsible for the development of the data analytics framework, and the establishment of, or the engagement with, an appropriate governance body.

Once agreed, the Forum will hand over responsibility for all further activity to the solution delivery body, who will be accountable for establishing the data sharing and data analytics framework.

Step 2: Mobilisation of solution delivery body

From the beginning of 2018, solution delivery body activities will include the establishment of a governance body, the provision of a project team and plans along with a management structure and support arrangements; design development and proving activities, the definition of a funding model and the publication of initial standards and requirements.

Activity 2.1: Establish Governance Body

The solution delivery body will set up a series of workshops to validate the core requirements of the governance body. These requirements should cover the following topics:

- Governance body objectives
- Members
- Responsibilities
- Authority
- Governance body administration
- Relationship to other bodies

During the workshops a potential governance body will be selected from existing bodies (industry or other) that may already satisfy the requirements outlined above. In the case that no suitable body can be identified the creation of a new governance body should be considered. The governance body should incorporate members from a wide variety of organisations representing different participant categories in the new data analytics environment.

Once established, the governance body will set up and sign-off the governance scope requirements, define the mechanisms to oversee the solution, and define the process for updating the data analytics standards (now controlled by this body). It will supervise the regulation process for participants that are compliant against the defined data analytics standards, and will have the authority to revoke system access for participants that no longer meet those standards.

Overall responsibilities of the governance body will include the following activities:

- **Define the standards** of the messaging and other technologies used to communicate payments transactions across the analytics system.
- **Evolve the standards** to meet the needs of the full range of participants (SMEs, PSPs and analytics service providers).
- **Enforce compliance** of the defined data analytics standards.
- **Oversee participation** take-up and utilisation in the data analytics environment.

A project team will be provisioned by the identified body which will create a detailed project plan spanning the activities outlined in this document. In the first step, all activities until end of 2018, i.e. until the detailed design is completed, should be itemised in detail and prioritised.

This will include the design and provisioning of a management structure and support arrangements as well as the appropriate funding and governance procedures as defined by the governing body.

Activity 2.2: Establish Stakeholder working groups

The continued input of stakeholders from across the payments community is an essential component to the success of this solution. As such, the solution delivery body should establish stakeholder working groups that will provide ongoing feedback and support throughout the design and implementation phases of the solution. As a minimum, it is recommended that working groups are established to represent the following participants:

- Financial Institutions that will be contributing their data.
- Insight and technical providers that will be looking to build analytics engines and services.
- 3rd party data providers.

If necessary, additional working groups should be established, or other appropriate stakeholder management performed to ensure that input can be received from all relevant interested parties. This may involve government and law enforcement stakeholders, as the solution develops further.

Activity 2.3: Establish ongoing legal work stream

The solution delivery body will work with appropriate industry representatives (this may include other organisations or trade bodies) to discuss and begin to address legal considerations that arise during the implementation of the strategic solution. This may be related to the sharing of data, the content of shared data or the legislation associated with the operating model for particular anti-financial crime use cases (for example, the legislation regarding the repatriation of funds to victims of financial crime).

In addition, the legal work stream should investigate the requirements that participants will need to fulfil to be able to share and receive payments transaction and other data related to the solution. In particular it should be considered whether specific accreditation or regulation is needed before participants are authorised.

This activity will be ongoing, and will require constant attention particularly as the solution expands in future years to address broader financial crime typologies.

Step 3: Design Development and Proving

The aim of the design development and proving is to understand the usage of messaging types and potential industry use cases whilst proving the value of cross participant data sharing. Note that this could be achieved by a series of walkthrough workshops with key participants/architects, rather than by using any hardware infrastructure.

Activity 3.1: Conduct a design development and proving exercise with a wide set of participants

It is recommended that a wide range of payment transaction participants are invited to contribute to a design development and proving exercise that is designed to:

- Demonstrate that analytical results can be produced when payments transaction data is made available between and from multiple disparate payments system participants.
- Help define the message types required to support use cases.
- Provide further understanding of potential additional use cases that could be included in the strategic solution delivery.
- Validate the viability of the strategic solution standardised API approach to solving the known use cases (mule accounts, repatriation of stolen funds amongst others).

- Engage data analytics companies to elicit further valuable use cases made possible from access to payments transaction data.
- Act as an input into the Strand 2 procurement process by providing further understanding of vendor and data analytics capabilities.

Step 4: Finalise API requirements and governance structure

Following the completion of the design development and proving, and consideration of the identified use cases, the details of the solution governance structure, operating model, standardised services and API messaging requirements should be near final and appropriately documented.

Activity 4.1: Formally establish the solution governance structure, operating model, standardised services and API messaging requirements

Using the learnings and outputs from the design development and proving, the governance structure should be finalised, documented and put in place. The operating model should be confirmed and the first set of standards requirements should be published.

Careful considerations should be given to the necessity of having any standardised services, e.g. communication hubs or analytics broadcasting capabilities to send messages to all participants etc. However such services may not be required, dependent on the level of service provided by individual analytics providers and/or individual 3rd party service providers.

Step 5: Develop and Publish API Standards

Develop the messaging standards and controls based on the published set of requirements.

This would include methods and controls for data quality, API technical standards as well as operating models for different types of participants.

Activity 5.1: Standards Publication

The project team both directly, or with the aid of 3rd parties, develops and publishes the standards. This includes data quality, data standards, API standards, any standardised services and operating models.

An initial pricing model is finalised and put in place based on the recommendations from interaction with the established stakeholder working groups.

Step 6: Participant authorisation for live solution

Every participant to the solution will need to be properly authorised to ensure that they are conforming to the defined rules and controls as determined by the governing body.

Activity 6.1: Authorisation of Participants

Define and instantiate a process by which participants to the solution can prove that they are meeting the defined rules and controls and can therefore be deemed authorised to access the solution.

Setup and maintain ongoing monitoring and enforcement controls which are designed to identify breaches of rules and controls and can take appropriate action against offending participants. Including, but not limited to suspending of access to the solution.

Activity 6.2: Consideration of further enhancements and ongoing activity

The solution delivery body and governance body should work with stakeholder working groups to consider future industry use cases and ongoing enhancements to the solution. This may involve further engagement with stakeholder groups such as government and law enforcement agencies.

5 Strand 2 - Implementation Steps and Activities

Strand 2 implementation activities are intended to enable real-time interaction with the New Payments Architecture and to transition the tactical solution into the strategic solution.

It requires that the NPA architecture includes real-time financial crime monitoring and data enrichment capabilities as well as conformity to the Strand 1 API and messaging standards, controls and data quality requirements.

Period	Step		Activity
Q2 2018	**Step 1:** Initial component identification	1.1	Based on the PSF solution work stream documentation, a more detailed high level architecture design is developed to support a Request for Information (RFI) to be issued to a range of potential vendors, potentially as part of other procurement activity underway in connection with the NPA.
H2 2018	**Step 2:** Supplier proposal and selection	2.1	Issuance and evaluation of responses to the RFI. The high level architecture is refined as necessary, following which a Request for Proposal (RFP) is issued to appropriate vendors. Appropriate suppliers identified.
H1 2019	**Step 3:** Detailed design	3.1	Suppliers produce detailed specifications that are agreed under suitable governance and used as the basis for low level design of the component parts of the architecture, including how these will integrate together and interface with users.
		3.2	Consider re-procurement of tactical solution
H2 2019	**Step 4:** Build and component testing	4.1	Infrastructure is procured and individual components constructed and tested to ensure that their functionality and performance is in line with the agreed detailed specifications.
Q1 2020	**Step 5:** System integration testing	5.1	End to end testing is carried out to ensure data feeds and storage operate, analytical tools are effective, and that the overall solution objectives of identifying, analysing and investigating financial crime related payment transactions have been met.
Q2 2020	**Step 6:** Soft launch of live proving	6.1	The full system will be available but with restricted access and controlled analytical usage to ensure that any operational issues are identified and resolved before full capability is available to all participants.
H2 2020	**Step 7:** Initial development and implementation complete	7.1	Development and testing completed. Planning for subsequent phases of enhancement and funding.

Table 2 Strand 2 recommended implementation approach.

Step 1: Initial Component Identification

The aim of the initial component identification is to develop the architecture design which can support a request for information (RFI) to be issued to a range of potential vendors.

Activity 1.1: High Level Architecture Design and RFI Issuance

The high-level demands articulated in the handover documents – see supporting document 'Payments Transaction Data Sharing and Data Analytics – Strategic Solution - Scope and Governance Oversight' - need to be translated into requirements which can be included in an RFI. These requirements need to be developed by the solution delivery body and signed off by the governance body and could include inputs from the design development and proving carried out as part of Strand 1.

The objective of the RFI is to inform the potential suppliers about the requirements of the solution. The RFI should focus on describing the facts and constraints of the processes and not the IT and process solution itself. The RFI should give the supplier the freedom to propose solutions to meet the requirements.

The document should be designed to impart information to the potential suppliers as well as to include a questionnaire with the aim of capturing a range of information from the respondents.

Once completed, the RFI can be issued to a range of appropriate participants including insight providers, software vendors, 3rd party data providers and other appropriate bodies.

Step 2: Supplier Proposal and Selection

Issuance and evaluation of responses to the RFI which then act as input into the development of an RFP to be issued to cover procurement of the components of the strategic solution.

Activity 2.1: RFI Responses Evaluated and RFP Issuance

The high level architecture design is refined following receipt of RFI responses. A high level design is created for the overall solution and an RFP is produced and issued to vendors. Preferred suppliers to participate in the initial implementation are chosen and commissioned by the end of 2018.

It is advisable to avoid producing a lengthy RFP as this tends to generate similar text-heavy and uniform proposals from competing firms that are hard to distinguish from each other. A shorter RFP with clear and concise questions will tend to generate very distinct proposals, making it easier to make an informed choice.

The RFP should not be too prescriptive and should not ask leading questions. Asking prescriptive questions will also lead to uniform answers. Similarly, asking leading questions will not provide innovative answers from vendors.

Step 3: Detailed Design

The expectation is that the preferred suppliers are suitably engaged so as to fully understand the solution requirements and are able to produce detailed specifications to meet the solution requirements.

Activity 3.1: Suppliers Produce Detailed Designs

Suppliers produce detailed specifications which are reviewed and approved under suitable governance. These are then developed into low level designs of the component parts of the architecture.

Activity 3.2: Consider re-procurement of tactical solution

At this time the detailed designs for the NPA architecture and the requirements for the API and data standards and standardised services should be sufficiently understood to be able to make an initial plan for the re-procurement of the tactical solution into the strategic solution analytics data sharing framework.

The timelines will need to be established allowing for appropriate competitive processes and should take into account dependency that this re-procurement may have to the implementation of the NPA.

During the transition from the tactical to the strategic solution, it will be important to ensure that there is minimal disruption to any industry service currently in place; and to end-users: this may involve a phased transition, where both solutions are run in parallel for a short time.

Step 4: Build and Component Testing

Component build is completed by the preferred suppliers to the agreed timeframes.

Activity 4.1: Infrastructure Procurement, Component Build & Testing

Suppliers procure the infrastructure and develop the components required to deliver the solution against the detailed specifications and low level designs.

System testing is completed on each component to ensure quality ahead of the wider system integration testing.

Step 5: System Integration Testing

The objective of the system integration testing is to comprehensively check system execution and prove that the system meets its requirements and performs in accordance with expectations.

Activity 5.1: End to End Testing Completed

The various component systems of the solution will be combined and tested end-to-end to ensure that they work correctly together and meet requirements and performance expectations.

It is expected that the preferred suppliers do not work in isolation and should involve participants of the solution to test and refine interoperability. PSPs, client service providers and technical providers that will be participating in the strategic solution should be involved with the end-to-end testing so that they can validate their own systems changes in support of the strategic solution.

Step 6: Soft Launch of Live Proving

Once end-to-end testing is complete and shown to fulfil the requirements set out in Step 5, the system can be operationalised and moved to production in a soft launch. This may involve incremental enablement of functionality or limiting functionality to subsets of data in a progressive launch.

Activity 6.1: Integration with Solution

Once live, participants will be able to integrate their internal systems fully to the solution.

The full system will be available but with restricted access and controlled analytical usage to ensure that any operational issues are identified and resolved before full capability is available to all participants.

Step 7: Initial Development and Implementation Complete

Once the initial development has been completed, it should be possible to enrich payments in real-time.

Activity 7.1: Full Access and Operation in Place

At this stage, the governance body priority will change to monitoring the risks in the data analytics environment and adoption by a wider set of participants.

The governance body will decide on the further role of the solution delivery body. One option is that the governance body takes over the remaining responsibilities from the solution delivery body. In the case of a large expected number of future enhancements, it is more likely that the solution delivery body will continue to remain involved.