POL00400064

PRIVATE AND CONFIDENTIAL – SUBJECT TO LEGAL PRIVILEGE

'Bramble' – Interim Report

Draft for discussion

27 July 2016

This report and the work connected therewith are subject to the Terms and Conditions of the engagement letter dated 09 April 2014 (amended 11 March 2016) between POL and Deloitte LLP. The report is produced for the General Counsel of POL, solely for the use of POL for the purpose of assessing assurance sources and the design of certain controls relating to the Horizon system. Its contents should not be quoted or referred to in whole or in part without our prior written consent, except as required by law. Deloitte LLP will accept no responsibility to any third party, as the report has not been prepared, and is not intended for any other purpose.

POL00400064

Contents

POL00400064

Executive Summary

Background

POL continues to respond to allegations that the "Horizon" IT system used to record transactions in POL branches is defective and the processes associated with it are inadequate (the "Allegations"). In response to recent formalisation of these accusations into commencement of litigation proceedings, Deloitte has been instructed to plan and execute procedures against four scope areas to provide assurance that the Horizon system operates as expected, and there are reasonable controls and safeguards in place to prevent incorrect system operation that could have resulted in Sub-postmaster detriment.

The four scope areas over which Deloitte have been requested to perform procedures over are as follows:

(i) *Scope Area 1* - POL consider instructing a suitably qualified party to carry out an analysis of the relevant transaction logs for branches within the Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.

(ii) *Scope Area 2* - POL instruct a suitably qualified party to carry out a full review of the use of Balancing Transactions throughout the lifetime of the Horizon system, insofar as possible, to independently confirm from Horizon system records the number and circumstance of their use.

(iii) *Scope Area 3* - POL instruct a suitably qualified party to carry out a full review of the controls over the use and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed audit store throughout the lifetime of the Horizon system, insofar as possible.

(iv) *Scope Area 4* - POL commission forensic accountants to review the unmatched balances on POL's general suspense account to explain the relationship (or lack thereof) with branch discrepancies and the extent to which those balances can be attributed to and repaid to specific branches.

Against each of these four scope areas the main body of this interim report will outline further:

(i) Background and context in relation to this engagement;

(ii) The approach Deloitte have taken to planning the procedures;

(iii) The testing procedures POL has requested Deloitte undertakes in response to the planning activities; and

(iv) Findings to date against each scope area.

Preliminary Results from Procedures Performed to Date

At the time of writing this interim report, the status of the work is as follows:

(i) The planning work has been completed.

(ii) POL have articulated which procedures they wish Deloitte to conduct in light of the litigation.

(iii) A number of initial testing procedures have been conducted (in delivery of this plan), although a number remain to be performed.

POL00400064

A full run down of status of the procedures up to 28 June 2016 and the associated results has been included in the main body of this report (see section 2). The majority of procedures performed to date have been over scope areas 1, 2 and 3.

Overall, 30 out of 73 procedures have been performed. The reader should acknowledge that all results highlighted within this report are provisional as our QA processes remain ongoing and as a result our findings may change as the work performed is finalised.

In summary with two exceptions all procedures carried out to date for these scope areas have not revealed any issues against the assertion statements under test.

The procedures for which exceptions were noted were:

> *'Validate inherent system controls around Recovery of transactions in the event of connectivity failure.'*

and the related exception was that:

> *'For one of the transaction recovery scenarios tested as part of recovery scenario 6, whereby a user session is automatically logged out after a period activity, it was confirmed Post Office business rules are in place for Horizon to automatically commit unprocessed transactions to the branch database tables. As part of the walkthrough testing performed, it was observed that Horizon is configured to automatically lock a user account after 15 minutes of inactivity, at which point the user is required to re-enter their user credentials. After a further period of 59 minutes of inactivity, Horizon is configured to automatically log the user out, ending a user session and committing any unprocessed transactions within a basket to the branch database. When next authenticating into Horizon, after being automatically logged out, the user is immediately presented with a till receipt confirming that the transactions had been committed to the branch database. From review of the printed receipt, an enhancement point was noted in that there is scope for the till receipt to include further detail to the user, highlighting that an unattended transaction had automatically been committed by Horizon to provide greater visibility to Post Masters that a recovery session had been initiated.'*

And:

> *'Review case data for transactions indicating items of risk from a system functionality perspective (e.g. recovery transactions are present in the case data).'*

and the related exception was that:

> *'For the analytics performed, some potential exceptions were noted. These are being discussed with POL and further investigation will be needed to validate the impact of the exceptions to the overall assessment.'*

Our final report will be produced subsequent to completion of the remaining procedures.

POL00400064

1. Background, Scope and Approach

1.1 Background

POL continues to respond to allegations that the “Horizon” IT system used to record transactions in POL branches is defective and that the processes associated with it are inadequate (the “Allegations”). In response to recent formalisation of these accusations into commencement of litigation proceedings, Deloitte has been instructed to plan and execute procedures against four scope areas to provide assurance that the Horizon system operates as expected, and there are reasonable controls and safeguards in place to prevent incorrect system operation that could have resulted in Sub-postmaster detriment.

The code name for this work is ‘Bramble’. Deloitte have been asked to contribute to a number of the scope areas within this piece of work, but it should be noted that other providers are also engaged by POL in relation to the ‘Bramble’ project, outside of the 4 scope areas referenced below.

POL00400064

1.2 Scope of Work

We have structured our work around the 4 scope areas POL have asked us to review, as shown in the table below:

Scope Area #	POL Instruction	Proposal
1	POL consider instructing a suitably qualified party to carry out an analysis of the relevant transaction logs for branches within the Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.	POL will instruct Deloitte to determine whether such an analysis/review is feasible, and if it is, to provide an indication of the cost, time and process that would be incurred.
2	POL instruct a suitably qualified party to carry out a full review of the use of Balancing Transactions throughout the lifetime of the Horizon system, insofar as possible, to independently confirm from Horizon system records the number and circumstance of their use.	POL will instruct Deloitte to determine whether such an analysis/review is feasible, and if it is, to provide an indication of the cost, time and process that would be incurred.
3	POL instruct a suitably qualified party to carry out a full review of the controls over the user and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed audit store throughout the lifetime of the Horizon system, insofar as possible.	POL will instruct Deloitte to undertake this review, throughout the lifetime of the Horizon system, insofar as is possible.
4	POL commission forensic accountants to review the unmatched balances on POL's general suspense account to explain the relationship (or lack thereof) with branch discrepancies and the extent to which those balances can be attributed to and repaid to specific branches.	POL will commission Deloitte to review any unmatched balances on POL's Suspense Account.

1.3 Summary of Approach and Work Performed

Phase 0

This first phase of work performed constituted 'Phase 0', the 'Discovery Phase', whereby Deloitte performed initial enquiries and investigations across the four scope areas named by POL to identify procedures which POL could undertake for each scope area.

In performing work for Phase 0, Deloitte conducted the following procedures:

a. Review of relevant technical documentation as provided for previous 'Bramble' work, or requested and provided by Fujitsu/POL during the course of this engagement. We have set out the documentation reviewed during the course of this work in Appendix 1.

b. Workshops with Finance staff in Chesterfield on 14th and 23rd March, and 18th April 2016.

c. Workshop with Fujitsu in Bracknell on 14th April 2016.

POL00400064

d. Workshop with Case Handlers on 8th April 2016

The aim of these procedures has been:

i) To enhance Deloitte's previous understanding of the *key concepts, processes, risks and controls associated with the Horizon system*, relevant to the four scope areas highlighted above (see 1.3.2).

ii) To identify the *fundamental limitations and assumptions* which will need to be made and considered by management when deciding which procedures they wish to conduct during Phase 1 (see 1.3.3).

iii) As a result of i) and ii) above the *identification of possible procedures* which could be adopted by management in order to provide assurance over the risks posed in relation to the four scope areas highlighted above (see 1.3.4).

Phase 1

The objective of the 'Discovery Phase' was to develop an understanding of the procedures in place, and to present a proposal of procedures which could be undertaken in Phase 1, the 'Delivery Phase', This has been completed and each scope area below has a 'Procedure's' section which details the procedures that POL have instructed Deloitte to perform for Phase 1. It should be noted that procedures performed in relation to scope area 4 are TBC.

In performing work for Phase 1, Deloitte conducted the following procedures:

a. Onsite review and visit to Fujitsu to test controls between 09 May 2016 and 10 June 2016.

b. Review of case data provided by POL case handlers and tested for characteristics which could illustrate the Horizon system has not operated as expected.

As of 28 June 2016 we have completed a proportion of the requested procedures with more remaining to test.

1.3.1 Key Concepts, Processes, Risks and Controls Associated with the Horizon System

System Context

The Horizon system was developed by Fujitsu and is the core operational and EPOS platform for the Post Office network. Whilst formal benchmarking data is not available, it is considered by interviewed stakeholders to be one of the largest computer systems in existence in terms of the number of transactions it processes on a daily basis, and it sits at the core of a complex systems estate with multiple interfaces with other Post Office systems as well as third party systems.

The system has been in use for over 15 years and is audited by multiple parties for statutory audit, service auditor reporting, and accreditation purposes. Given its size and scale, and the considerable intellectual property that Fujitsu has built within the system, in relation to this piece of work, there is a significant quantity of documentation articulating how the various modules and features comprising the system operate. Much of this documentation has formed the focus of our review during Phase 0 of the work.

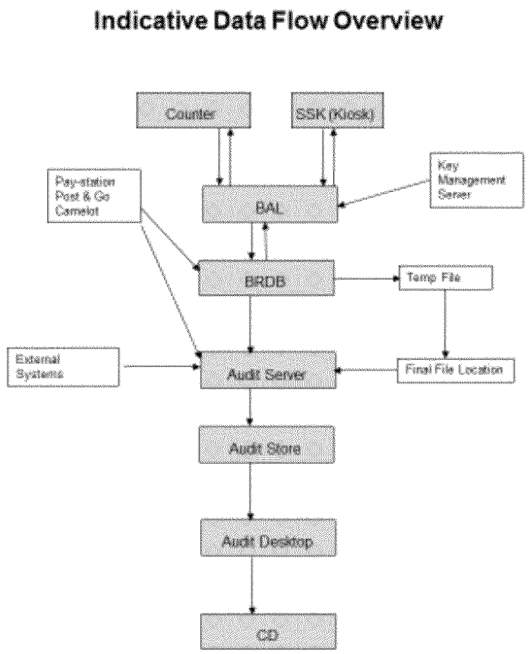
In addition to Horizon, POLSAP is of relevance to Scope Area 8 as a key Finance system where suspense accounts are located and processed, and with interfaces back to the Branch Database via Transaction Corrections (see below).

In understanding Horizon it has been important to distinguish between features which are of relevance today, and the time period to which that relevance applies. In particular we would highlight the migration between the system commonly referred to as Legacy Horizon, and the online variant operated today, referred to as Horizon HNG-X. The key difference between these two iterations of the platform is the way data is stored. In the Legacy version data was replicated between the data centre to also be local to the branches (this system was called Riposte), whilst over the course of 2010 a migration event occurred whereby the Riposte system was replaced by the Branch Database model, the Branch Database being a data centre only database storing the transactional and accounting

POL00400064

data for the branches, with a Counter application held locally within the branch which interfaces data across as relevant. This change may have influenced the relevance of some of the controls in existence at the present time and care must be taken to consider this when prioritising procedures.

The Branch Database is also key to understanding the flows of data to the Audit Store given that it acts as a hub for all branch transactional and accounting records. The diagram below provides clarity on the high level flow of data from transaction origination through to the Audit Store:



System	Description & Detail
Counter	Front end of the system, located behind the 'counter' in Branches. Transactions are input here by the Postmaster.
SSK (Kiosk)	Configured the same way as the Counter, but for Kiosk outlets.
BAL	Transactions are bundled into 'Baskets' and sent from the Counter / Kiosk to the BAL once they are complete. All baskets must balance to 0 (Debit = Credit). Data is then transferred from the BAL – BRDB on a daily basis.
BRDB	The Branch Database is an Oracle database and sits at the heart of the Horizon system. It receives transactions from the BAL and also from other sources as illustrated. Transactions input into BRDB from sources other than the Counter/SSK are fed back to the Counter/SSK and have to be 'Transaction Accepted'.
Audit Server	The Audit Server run a Daemon process which searches for new data in the BRDB. When relevant transactions are identified they are pulled into the Audit Server from the BRDB. Data is held in the Audit Server for approximately 5 days.
Audit Store	After approximately 5 days data is written from the Audit Server to the Audit Store where it is stored semi-permanently (currently 8.5 years of data is stored). Transactional data is stored in a message journal, whereby the completeness of the audit data is confirmed by JSN sequencing.
Audit Desktop	Upon request the Audit Desktop can query the audit store to extract specified data. Upon extraction from Audit Store – Audit Desktop, the interity of the data is confirmed via public/private key encryption.
CD	A CD is produced with the requested Audit Data.

This diagram shows most but not all of the data feeds associated with the Branch Database, but does show all of the direct transactional feeds to the Branch Database. It demonstrates the convergence of the dataflows at the Branch database and the chain of subsequent data movements of the aggregated data post this rationalisation.

In considering these diverse data feeds a key concept is those which use a public key infrastructure (Counter and SSK) for completeness and accuracy of the message journals to the Branch Database, versus those which use a combination of interface controls (header and footer records) for completeness, combined with manual interventions from Branch staff around the completeness of the associated data (being the data feeds external to the Horizon infrastructure e.g. Paystation).

Potential Risks

Our view of the potential risks which are inherent in the high-level procedures requested by POL are listed below. In creating this list of potential risks we have considered the high-level procedures themselves, our understanding of the allegations made by the sub postmasters and our knowledge of the Horizon system through workshops with POL and Fujitsu personnel.

POL00400064

The table below shows how each potential risk relates to POL instruction

	Requested Scope Areas			
	1 - POL consider instructing a suitably qualified party to carry out an analysis of the relevant transaction logs for branches within the Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.	2 - POL instruct a suitably qualified party to carry out a full review of the use of Balancing Transactions throughout the lifetime of the Horizon system, insofar as possible, to independently confirm from Horizon system records the number and circumstance of their use.	3 - POL instruct a suitably qualified party to carry out a full review of the controls over the user and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed audit store throughout the lifetime of the Horizon system, insofar as possible.	4 - POL commission forensic accountants to review the unmatched balances on POL's general suspense account to explain the relationship (or lack thereof) with branch discrepancies and the extent to which those balances can be attributed to and repaid to specific branches.
R1	✓			✓
R2		✓		
R3		✓		
R4		✓	✓	
R5	✓			✓

Key to potential risks

R1. **If Horizon does not process transactions correctly and these are not identified and resolved**, *these could lead to sub postmaster financial loss*

R2. **If inappropriate transactions can be created centrally by POL or Fujitsu which branch staff and sub postmasters are unaware of**, this would undermine the sub postmasters' ability to trust the transactions in Horizon are authentic and could cause sub postmaster financial loss.

R3. **If data flow to the audit store is not complete, accurate or valid**, the conclusions from the investigations by case handlers or other parties dependent on these records cannot be relied on.

R4. **If once data is in the Audit Store or extracted to support case investigation it is subject to amendment, modification or deletion**, this would also reduce confidence in case handlers' conclusions.

R5. **If suspense accounts mismanaged leading to sub postmaster loss**, suspense account transactions are by nature unusual and require investigation. The risk is that there are suspense account transactions which relate to a mediated sub postmasters, are capable of being identified as such byPOL and if corrected would be favourable from the perspective of the sub postmaster.

Controls

POL management are responsible for ensuring there is a system of internal control designed to mitigate these potential risks and that these controls are operating effectively.

No system of internal controls can be expected to guarantee the associated potential risk has not been realised. For example, in our experience it is not reasonable to expect any enterprise software to be free from bugs throughout the duration of its use. However, the design of enterprise software should take into account the key risks to the application's ongoing security and operation. Where possible inherent system controls should be developed to prevent these potential risks being realised. Monitoring controls may also be implemented to detect issues so they can be resolved in a timely manner by the right people. A robust change management process

POL00400064

should be in place to ensure only authorised changes are made and changes are tested thoroughly prior to being implemented.

Based on discussions and workshops to date we have identified the following as key controls relevant to the potential risks above.

a. In order for Horizon to accept a transaction, the transaction must balance to zero (double entry principle).

b. Counter transactions are committed atomically, a transaction is either successful in its entirety or it is not successful at all.

c. If a transaction is not successful, due to loss of connectivity / power in a branch mid-way through a transaction for example, then Horizon has various recovery procedures it attempts in order to recover the transaction if possible. Following this attempt it will then notify the Counter of the success or otherwise of the recovery attempt.

d. Transactions are recorded in message journals when they are transferred from the Counter / SKK through BAL to the Branch Database. There is a JSN sequence associated to each Counter / SKK and the density of this data log allows the completeness of message journals to be validated.

e. Other data feeds are input into the Branch Database, however prior to this data being committed, the Branch must acknowledge the data-feed is accurate by way of a 'Transaction Acknowledgement'.

f. Similarly POL finance staff can input / amend a Transaction directly in BRDB, for this Transaction to be committed the Branch to which it relates must agree the accuracy of it by way of a 'Transaction Acknowledgement'.

g. The only transaction that can enter the audit trail without being input on a Counter / SKK, or accepted by a Branch is a 'Balancing Transaction' which can be input by Fujitsu. There are various system controls to ensure the use of a Balancing Transaction is recorded in the Audit Store.

h. Audit Store data has controls around it (including JSN controls as above) to ensure the permanency of data (cannot be deleted) and uses public/private key encryption in the data retrieval process to validate the integrity (cannot be amended) of the data.

i. POL Finance performs a monthly 'Probity Review' of Suspense accounts to monitor movements in suspense.

1.3.2 Fundamental Limitations and Assumptions

Any procedures performed during our work against each scope area are subject to a number of assumptions and inherent limitations.

Specifically it should be noted that controls tested/to be tested for Phase 1 relating to the system will be tested on the current system (HNG-X), and Finance controls testing will cover controls currently in place. It must be noted that at the time of some allegations the Legacy Horizon system was still in use, and further there is currently a refresh of POL Finance Centre controls underway. In performing our testing we will comment on the historical pertinence of the control under review, where we are able to do so.

Further all analytical procedures for Phase 1 are subject to the availability of data / evidence, it is noted that while a full transactional audit log is available for up to 8.5 years, logistical / time constraints may limit the volume of data that is able to be retrieved and interrogated. Also any controls testing is subject to the availability of evidence, and it was noted during Phase 0 that POLSAP archival and hard copy data retention is subject to data retention policies.

Finally our work performed for Phase 0 and proposed/tested procedures for Phase 1 are specifically limited to the four scope areas outlined in the scope section above. Our work is focused on identifying, and performing procedures to validate, the facts in relation to the Horizon system with regard to the four scope areas as above.

Please see Section 4 for a full list of assumptions and inherent limitations.

POL00400064

1.3.3 Identification of Possible Procedures

Following our understanding of the system, the risks posed in the context of our four scope areas, and our provisional understanding of the control environment, we have identified three core procedure typeswhich we will utilise/have utilised during Phase 1:

i) Analytics – Procedures using data tools to analyse large volumes of data for particular characteristics of interest or the absence thereof. For example verification for a given set of case data that the JSN sequence is complete.

ii) Controls review and testing – Verification through walkthrough, enquiry, and subsequent evidence gathering that controls relating to the Horizon system operate as expected or otherwise, to support in mitigation of the associated risks. For example testing the population of Fujitsu users who can administer the Oracle DB estate underpinning Horizon directly is appropriate.

iii) Substantive procedures – Direct inspection of selected samples or information for confirmation of its qualities or characteristics of note (Analytics is an example of 'full population' substantive procedures). In this instance the main substantive procedures expected will be inspection of source code to verify that the system functions as expected.

The remainder of this document articulates our procedures performed in Phase 0, the results of those procedures, and the Phase 1 procedures which have or will be performed against each of the four scope areas as per POL instruction.

POL00400064

2. Work Performed

2.1 Summary of Work Performed

Below for each scope area we have laid out our work performed as follows:

i) Setting the Scene – We have described in a narrative format the work we have performed, and our understanding of the relevant subject matter.

ii) We have then set out in a tabular format the procedures performed in Phase 0, and the key learnings relevant to our planning.

iii) As a result of the above, and discussions with POL, we highlight the procedures which will or have been performed in Phase 1 as per POL instruction, and where procedures have already been carried out we comment on the conclusion of that procedure.

POL00400064

2.2 Scope Area 1

Scope Area 1: *POL consider instructing a suitably qualified party to carry out an analysis of the relevant transaction logs for branches within the Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.*

2.2.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 1.3 above. In addition specific to this scope area we reviewed the case data which had been provided to us, and assessed the feasibility of performing analytics over the available case data in order to ascertain whether evidence of the system not operating in accordance with expectations could be identified.

Our work has highlighted a number of fundamental system controls designed to ensure the integrity of processing, and correct functionality. Key principles/items identified include:

i) At a holistic level, IT change control processes and procedures operate over the Horizon system, and the related controls around testing, approval, and the overall software development lifecycle should provide assurance over the correct operation of the system. The operational effectiveness of this control framework is assessed on a regular basis via Service Auditor Reports (ISAE3402 produced by EY), ISO27001 certification and ongoing audit and attestation regime, and ongoing IT focused Internal Audit and External Audit activity. 'Bugs' in the system would be more likely in an environment with inadequate change control procedures, and the level of comfort that can be gained over such controls provides a view on the inherent risk of such errors.

ii) There are some fundamental inherent system controls, specifically designed to support correct processing within the system. These include:

   a. Journal Sequence Numbers (JSNs) are applied to each Counter transaction within the Horizon system. These JSNs are generated using Public Key Encryption and are used by each piece of Counter Hardware to 'digitally sign' a transaction. The digital signature is passed to all latter stages of the infrastructure including the Audit Store (and beyond). This signing process provides two critical control points over the data captured:

      i. The completeness ('density') of the flow of transactions for a particular Branch, meaning that completeness of the audit trail behind transactions can be ascertained.

      ii. The validity and accuracy of the transactions as any changes to a transaction after the application of the digital signature would invalidate the signature. The Audit Store extraction routines check for this at the point of extraction.

   b. Transaction Acknowledgements – Whilst JSNs are a powerful inherent system control over the correct origination and completeness of the Message Journals from the Counter, other feeds to the Branch Database are not subject to this control. However as an alternative control mechanism the interface files, which issue data to the Branch Database contain Header and Footer records which allows Horizon to automatically check the completeness of data. In addition Branch staff accept these interface files into their Branch accounts via Transaction Acknowledgements, meaning these staff are directly responsible for verification that the data being received into the Branch Database via sources outside the Counter are valid and accurate.

   c. Recovery Procedures – In acknowledging that the Horizon system is dependent upon connectivity between a data centre, a branch, and various third parties, seven recovery processes have been designed to combat instances when a loss of connection causes an error in the completion of transaction processes. The recovery processes used depend on the nature of the connectivity issue. Recovery scripts designed by POL are an integral part of this process.

POL00400064

d. The commit of transactions to the Branch Database is all performed as one Oracle DB write action, i.e. it is atomic in nature.

e. All transactions from the Counter are checked by Horizon to ensure they balance to zero (double entry principle). If the Counter attempts to write a transaction which does not balance to zero, this will be rejected via the Counter.

f. External file feeds (i.e. for data feeds not from the Counter or Kiosks) are received by the Branch Database and interpreted into the database by Horizon before being sent to the Audit Store. Alongside this data flow, the raw interface files are also processed directly to the Audit Store. As a result, a reconciliation of processed data versus the raw data files is theoretically possible to test for completeness.

iii) Alongside the inherent system controls available for our review, there are two tranches of data analytics work that we can perform to highlight the inherent risk of system failure or 'bugs':

a. Using the case data we have been provided with we can perform specific profiling tests which support the operation of these inherent controls or rule out the occurrence of particular risky events from within the relevant data set.

b. The BRSS (Branch Support Database) is a copy of the main Branch Database used by Fujitsu staff for support purposes. This database contains the most recent six months worth of transactional data (the Branch database itself contains only 5 days worth). Using tools already available via Fujitsu we can profile this data to look for characteristics of risk (such as recovery situations, Balancing Transactions, transactions posted by staff not related to a Branch etc).

POL00400064

2.2.2 Summary Table of Phase 0 Procedures and Conclusions

POL Instruction	Procedures Performed	What we have discovered
POL consider instructing a suitably qualified party to carry out an analysis of the relevant transaction logs for branches within the Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.	Identified relevant business processes and areas of interest. Review of existing technical documentation and identification of key inherent system controls. Workshops with Case Handlers (POL) in order to understand how to interpret the case data. Workshops with Systems Architects (Fujitsu) in order to understand how to interpret the case data and technical documentation. A walkthrough on-screen as to how the system works.	There are a set of inherent system controls within Horizon targeting the completeness, accuracy and validity of the flow of data from Counter and other in-branch data sources, onwards to Branch Database, and ultimately the Audit Store. Central to these controls is the digital signature applied to each message journal of branch transactional data sent from Counter to Branch Database and beyond. Connectivity issues are managed via Recovery processes, and so issues with loss of connectivity have been built into the design of the system from the outset, in recognition this could be an area of potential data corruption or loss. A strategy for our analytic procedures is to profile the available case data for characteristics of interest in relation to the correct operation of the system.

POL00400064

2.2.3 Phase 1 Procedures

POL instructed procedures. (Scope Area 1)

Procedures
Controls 1. Validate inherent system controls around: a. All transactions on Counter system balancing to zero. b. Atomic write and commit controls of transactions to the Branch Database. c. Digital Signature controls applied to Message Journal during initiation of transfer to Branch Database. d. Transaction Acceptance in relation to interface file receipt for non-Counter originated interface files. e. Recovery of transactions in the event of connectivity failure. 2. Review of existing sources of assurance around Change Control and confirmation of relevant coverage– plus targeted testing to attempt to identify changes relevant to the key controls on Horizon. **Data** 3. Review case data for transactions indicating items of risk from a system functionality perspective (e.g. recovery transactions are present in the case data). See Appendix 2. 4. Review of population of balancing transactions (to validate population of Balancing Transactions relative to total transaction volumes) **Substantive** 5. Review source code on screen at Fujitsu headquarters which supports the key inherent control operation around digitally signing transactions posted from the Counter to the Branch Database. 6. Review source code on screen at Fujitsu headquarters which supports the key inherent control operation around: a. All transactions on counter balancing to zero. b. Atomic write and commit controls of transactions to the Branch Database. c. Digital Signature controls applied to Message Journal during initiation of transfer to Branch Database. d. Transaction Acceptance in relation to interface file receipt for non-Counter originated interface files. e. Recovery of transactions in the event of connectivity failure.

POL00400064

Phase 1 Procedures Performed at Interim Reporting Date

It should be noted this work is still going through our 'internal review process' and as such the below statements are subject to change. Any change in conclusions will be communicated immediately and also included in the final report.

Procedures	Conclusions
Controls 1. Validate inherent system controls around: a. All transactions on counter balancing to zero. b. Atomic write and commit controls of transactions to the Branch Database. c. Digital Signature controls applied to Message Journal during initiation of transfer to Branch Database. d. Transaction Acceptance in relation to interface file receipt for non-Counter originated interface files. e. Recovery of transactions in the event of connectivity failure.	1a. No Issues Noted 1b. No Issues Noted 1c. No Issues Noted 1d. No Issues Noted 1e. For one of the transaction recovery scenarios tested as part of recovery scenario 6, whereby a user session is automatically logged out after a period activity, it was confirmed that Post Office business rules are in place for Horizon to automatically commit unprocessed transactions to the branch database tables. As part of the walkthrough testing performed, it was observed that Horizon is configured to automatically lock a user account after 15 minutes of inactivity, at which point the user is required to re-enter their user credentials. After a further period of 59 minutes of inactivity, Horizon is configured to automatically log the user out, ending a user session and committing any unprocessed transactions within a basket to the branch database. When next authenticating into Horizon, after being automatically logged out, the user is immediately presented with a till receipt confirming that the transactions had been committed to the branch database. From review of the printed receipt, an enhancement point was noted in that there is scope for the till receipt to include further detail to the user, highlighting that an unattended transaction had automatically been committed by Horizon to provide

POL00400064

Procedures	Conclusions
	greater visibility to Post Masters that a recovery session had been initiated.
Data **3.** Review case data for transactions indicating items of risk from a system functionality perspective (e.g. recovery transactions are present in the case data). See Appendix 2.	3. For the analytics performed, some potential exceptions were noted. These are being discussed with POL and further investigation will be needed to validate the impact of the exceptions to the overall assurance assessment.

POL00400064

2.3 Scope Area 2

Scope Area 2: POL instruct a suitably qualified party to carry out a full review of the use of Balancing Transactions throughout the lifetime of the Horizon system, insofar as possible, to independently confirm from Horizon system records the number and circumstance of their use.

2.3.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 1.3 above.

Balancing Transactions are exceptional processes used by Fujitsu support staff to correct exceptional errors in system processing/fix issues or bugs in the recording of data. The inherent controls around the integrity of data recording are designed to ensure that such issues manifest themselves in the data on an exceptionally rare basis, and therefore volumes of Balancing Transactions should be inherently low.

Balancing Transactions should not be confused with Transaction Corrections which is a more routine process, used to centrally correct issues by POL Finance staff, which are then subject to Transaction Acknowledgement by sub postmasters prior to being accepted into a Branches accounts.

Fujitsu have advised that whilst there have been several hundred instances of Balancing Transactions used throughout the known lifecycle of the system (predominantly limited to HNG-X due to previous Audit Store retention limitations), only one has been a complex usage of the functionality, to correct a bug around double writing of a transaction, immediately subsequent to the migration to Horizon HNG-X. The remainder relate to switching a flag on Stock Units (SU are a Counter concept to allocate transactions to a particular 'sub-branch' area to enable users to process transactions on that stock unit (following communications failure Stock Units occasionally become locked to editing).

Our work has highlighted a number of fundamental controls which are designed within the system to control the use of Balancing Transactions and to ensure that the use of Balancing Transactions is recorded. Key principles/items identified include:

i) Balancing Transactions are the only transactions that do not either originate at Branch, or have to be acknowledged / accepted by branch. As such the use of Balancing Transactions is very rare.

ii) Any writes by Fujitsu Support to BRDB must be audited. The mechanism for inserting a correction record must ensure that the auditing of that action is atomic with the insert of the record.

iii) Fujitsu Support with access to post Balancing Transactions cannot amend the related audit files.

iv) Fujitsu Support will have privileges of only inserting balancing / correcting transactions to relevant tables in the database. They will not have any privileges to update or delete records in the database.

v) There are various inherent system controls around Balancing Transactions, notably that each Balancing Transaction must only contain 1 transaction (single SQL statement) and the balancing transaction module can only be ran by limited appropriate personnel.

In assessing the risk posed by Balancing Transactions we have also enquired as to additional 'privileged account' transactions which could also be used to post transactions centrally without the knowledge of Branch staff. These enquiries have highlighted two additional areas of consideration against this risk:

a. Global Users of the Horizon System – These are users that can log on at any HNG-X Branch, and are used for a number of purposes including global user administration.

b. Other 'Superusers' – At various layers of the Horizon infrastructure there exist accounts with privileged access rights which could be used to modify or insert data relevant to transactions at branches should they not be adequately controlled. For example a superuser account on the Oracle DB forming the nucleus of the Branch Database could insert transactions directly onto the backend (effectively Balancing Transactions are a specialised 'legitimised' way of using such Oracle access).

POL00400064

A number of key controls were noted to operate on Horizon to mitigate these broader 'superuser' risks:

vi) Global Users are subject to two fundamental controls reducing their risks. The first is that they cannot post transactions in a branch unless they are physically present at that branch. The second is that the Global Admins can only create users and there is therefore a Segregation of Duties between users who can create users, and users who can post transactions.

vii) Superuser activity is monitored via log files which are transferred to the Audit Store following aggregation by the Event Management System which collects log files from across the Horizon estate. Regardless of this control, for transactions related to the Counter and Kiosks any attempt to insert transactions into the database by an individual with the privileged access rights to do so, would be identifiable due to the Digital Signature process applied to Message Journals from the Counter. To circumvent this a 'superuser' would require the relevant access rights to the key management infrastructure which controls the Digital Signature processes, and therefore the segregation of duties between such infrastructure and the remaining Branch infrastructure is a key control.

Alongside the inherent system controls around balancing transactions, and the completeness and accuracy of the audit log of Balancing Transactions available for our review, there are various data analytics procedures which can be performed:

vii) As discussed above Fujitsu highlighted that while the Balancing Transaction module has been used approximately 200 times in the past 7.5 years, only 1 of these uses has been a 'complex' Balancing Transaction. Analytical procedures could be performed to validate the number and nature of Balancing Transactions which have been performed in:

a. The Case Data available

b. The BRSS most recent 6 months data available

c. The full period of data available – (7.5 years)

Sample (or full population) testing could then be performed to validate that for all Balancing Transaction records (except the 1 known Balancing Transaction, for which the branch was aware of) no transactional postings were made using Balancing Transactions.

POL00400064

2.3.2 Summary Table of Phase 0 Procedures and Conclusions

POL Instruction	Procedures Performed	What we have discovered
POL consider instructing a suitably qualified party to carry out an analysis of the relevant transaction logs for branches within the Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.	Identified relevant business processes and areas of interest. Review of existing technical documentation and identification of key inherent system controls, and support in interpreting the transactional data. Workshops with Systems Architects (Fujitsu) in order to understand how to interpret the technical documentation and the availability of Audit Store data. A walkthrough on-screen as to how the system works.	There are a sequence of inherent system controls within Horizon which ensure Balancing Transactions have certain standard characteristics, use of them is controlled, and usage is recorded in the Audit Store. Other privileged access rights which would lead to similar risks of central posting of transactions with sub postmaster knowledge, such as Global Users, and 'superuser' accounts on the Horizon infrastructure, are also subject to key controls, most notably the segregation of duties between the key infrastructure for digital signatures and the infrastructure supporting the processing of Branch transactions. The strategy to be adopted across our analytical procedures will be to Investigate a sample / full population of all Balancing Transaction records found to validate the branch was aware of their usage / no transactional postings were made in the balancing transaction.

POL00400064

2.3.3 Phase 1 Procedures

POL instructed procedures. (Scope Area 2)

Procedures
Controls
1. Validate inherent system controls around balancing transactions (See Appendix 3 for detail of controls 1a – 1c):
2. Any writes by Fujitsu support staff to BRDB must be audited. The mechanism for inserting a correction record must ensure thatthe auditing of that action performed is atomic.
3. Fujitsu support staff cannot amend audit files for Balancing Transactions.
4. Fujitsu support staff will have privileges of only inserting balancing / correcting transactions to relevant tables in the database. SSC will not have any privileges to update or delete records in the database.
5. Validate broader population of Balancing Transaction controls identified. (See Appendix 3a for detail of controls 2a – 2n)
6. Validation there is a Segregation of Duties between BRDB Administration and Key Management Software Administration.
7. Validate inherent system controls around Global Users, notably that Global users with a Role of ADMIN cannot log onto to anyBranch other than Global (Including Remote access controls to branch infrastructure (e.g. Counter)).
Data
8. Review case data for Balancing Transactions to validate population of Balancing Transactions relative to total transaction vdumes (Balancing transactions should be inherently rare, and only deployed in response to actual loss/bugs in code.)
9. Review full population (already extracted by Fujitsu - 7.5 years) of balancing transactions (sample vs full population depending on feasibility) to validate the branch was aware of their usage / no transactional postings were made in the balancing transaction.
Substantive
10. Review source code on screen at Fujitsu headquarters which supports the key inherent control operation around Balancing Transactions.
11. Review of Transaction Correction source code on screen at Fujitsu headquarters to validate that Transaction Corrections must be accepted by Branches, in order to validate Balancing Transactions are the only transactions Branches would not have to accept
12. Review the 9 Balancing Transaction Templates to validate balancing transactions would, if the template wasfollowed, logically perform as expected.
13. Walkthrough of a Transaction Correction being raised by SCC, and the notification / acceptance of it by a branch.

POL00400064

Phase 1 Procedures Performed at Interim Reporting Date

It should be noted this work is still going through our 'internal review process' and as such the below statements are subject to change. Any change in conclusionswill be communicated immediately and also included in the final report.

Procedures	Conclusions
Controls	
1. Validate inherent system controls around balancing transactions (See Appendix 3 for detail of controls 1a – 1c):	1. No Issues Noted
2. Any writes by Fujitsu support staff to BRDB must be audited. The mechanism for inserting a correction record must ensure that the auditing of that action performed must be atomic.	2. No Issues Noted
3. Fujitsu support staff cannot amend audit files for Balancing Transactions.	3. No Issues Noted
4. Fujitsu support staff will have privileges of only inserting balancing / correcting transactions to relevant tables in the database. SSC will not have any privileges to update or delete records in the database.	4. No Issues Noted
Data	
8. Review case data for Balancing Transactions to validate population of Balancing Transactions relative to total transaction volumes (Balancing transactions should be inherently rare, and only deployed in response to actual loss/bugs in code).	8. For the analytics performed, some potential exceptions were noted. These are being discussed with POL and further investigation will be needed to validate the impact of the exceptions to the overall assessment.

POL00400064

2.4 Scope Area 3

Scope Area 3: POL instruct a suitably qualified party to carry out a full review of the controls over the user and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed audit store throughout the lifetime of the Horizon system, insofar as possible.

2.4.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 1.3.1 above.

For this specific scope area our procedures centred on understanding the specific controls and processes around protecting the integrity of data from inception to Branch Database, and subsequently to the Audit Store. Our work highlighted a number of core concepts relevant to understanding the related risks and controls during this data flow:

i) In essence the data journey can be divided into a number of distinct phases:

   a. Transaction initiation within either the Counter, Kiosk, or 'third party interface source', and subsequent interface to the Branch Database.

   b. Archival from the Branch Database to the Audit Server.

   c. Sealing of Audit Tracks via MD5 Message Digest and Archive to the Audit Store itself (Now based on Eternis technology).

   d. Subsequent Retrieval of Tracks, validation via the ARQ (Audit Track Retrieval) process, and Investigator validation on the received data.

   e. Non-Branch Transaction Data Records of Relevance

a. Transaction Initiation within either the Counter, Kiosk or 'third party interface source'

ii) For Counter and SSK (Kiosk) initiated transaction data, the JSN remains a core element of control for the Audit Store process as it validates the origination and completeness of data for a particular Counter and is independent of the MD5 message digest elements.

iii) Given the wealth of 'data at rest' (stored in a directory/database awaiting onward processing) and 'data in transit', security controls over access to 'data at rest' and interface controls over monitoring completeness and accuracy of 'data in transit' are both pertinent. However the JSN concept provides assurance regardless given interruptions in the sequence, or mis-match between signature value and message content, would highlight downstream risks of data corruption.

iv) The other interfaces pertinent to our understanding have been represented by Fujitsu systems architects to be:

   a. Logistic Feeder Service

   b. Post and Go (discontinued in 2015, but relevant prior to that date)

   c. Near Real Time (NRT) feeds

   d. Paystation

   e. Camelot

v) For non-Counter and Kiosk interfaces to the Branch Database completeness is provided by the interface file header and footer record, with accuracy and validity provided by manual inspection by Branch staff themselves via the Transaction Acknowledgements process.

vi) For many of these interfaces the Post Office Data Gateway (PODG) provides the point of entry to POL infrastructure.

POL00400064

b. Archival from the Branch Database to the Audit Server

vii) Archival from the Branch Database of data take place to the Audit Server (which is the gateway to the Audit Store infrastructure) in accordance to an automated routine which is central to the operation of the Horizon system. If archival did not take place then very quickly the system would run out of available capacity. Two intermediate directories are used to hold records prior to transfer to the Audit Server.

viii) As referenced above both 'data at rest' and 'data in transit' controls are therefore relevant to this stage of the process.

c. Sealing of Audit Tracks via MD5 Message Digest and Archive to the Audit Store itself

ix) The Audit Track Gatherer (ATG) is a routine which is permanently scanning for new Audit files on the upstream infrastructure (including the Branch Database) which are then copied to the Audit Server, sealed by the Audit Track Sealer (ATS), using the MD5 message digest algorithm, copied to the Audit Store Eternis architecture itself, and then purged from the Audit Server when copied across.

x) The Audit Server maintains a database of sealed files and their seal values, for later interrogation when locating files, and validating their integrity has not been violated.

xi) Therefore once again both 'data at rest' and 'data in transit' controls are relevant to this stage of the process.

xii) Once on the Eternis hardware which has now replaced the EMC Centera hardware solution, the data is subject to a number of controls around access, deletion and amendment, all of which are designed to maintain the integrity of the audit trail during storage. Both EMC Centera (historical solution) and Eternis (current solution) are specialised hardware solutions for the storage of audit trail data intended to be used forensically.

xiii) Previously there was a seven year limit to the retention of data in the Audit Store, after which it was purged by the system in line with Retention requirements. Given recent history this policy has recently been changed to indefinite retention of all Audit Store data. As a result all transactions should be available for as long as the Audit Store continues to exist from 04/10/2007, and therefore a complete audit trail of all transactions ever posted on Horizon HNG-X should exist (given the migration date).

d. Subsequent Retrieval of Tracks, validation via the ARQ (Audit Track Retrieval) process, and Investigator validation on the received data itself

xiv) Extraction of the data from the Audit Store is via a defined process known as the ARQ process. A specialised Audit Desktop estate is utilised to interrogate the Audit Server database, retrieve relevant sealed files, process the data, and burn to CD (or email as a data file), whereby it is made available to POL investigative staff. Per Fujitsu POL is permitted to make 1,500 ARQ requests during the course of a Financial Year. Extracting 7 years' worth of data for a branch would attract 84 (12*7) ARQ requests as data is typically provided on a month by month basis.

xv) There are a number of logical access controls operating over this process, including role based access mechanisms, a strict 'segregation of duties' from POL staff and audit logs over the process.

xvi) Upon receipt of the data files POL investigators carry out a number of additional checks themselves in order to validate the data integrity.

e. Non-Branch Transaction Data Records of Relevance

xvii) Alongside the Branch Database data flowing into the Audit Store there are a number of other relevant data sources:

xviii) Interface files received from third party systems which are then processed into the Branch database, are also sent directly to the Audit Store as raw files, allowing potential future reconciliation between the two data sources.

POL00400064

xix) The Event Management System captures System Audit Logs from across the Horizon estate, and processes these to the Audit Store.

Given the above understanding of the process gained from our work to date, our approach to assurance against this scope area is largely based upon controls assurance, in combination with some limited analytics procedures to support completeness, security and integrity of the data throughout the relevant data flows.

POL00400064

2.4.2 Summary Table of Phase 0 Procedures and Conclusions

POL Instruction	Procedures Performed	What we have discovered
POL instruct a suitably qualified party to carry out a full review of the controls over the user and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed audit store throughout the lifetime of the Horizon system, insofar as possible.	Identified relevant business processes and areas of interest. Review of existing technical documentation and identification of key inherent system controls, and support in interpreting the transactional data. Workshops with Systems Architects (Fujitsu) in order to understand technical documentation. A walkthrough on-screen as to how the system works. Walkthrough of Audit Store specific controls in order to determine relevance and accuracy for inclusion within the scope of our work.	The Branch Database is a key point in the data journey at which all Branch relevant data whether generated by the Counter or by a third party data source external to Horizon will interface to. There are a number of intermediate points at which data is at rest during the flow of data to the Audit Store, and understanding the Security controls over such data will support the integrity of data flowing into the Audit Store. Regardless of the opportunity or otherwise for interception and tampering of data pre its arrival in the Audit Store, for key data originating from the Counter and the Kiosks, the digital signatures should highlight any tampering with data prior to its usage within the Cases. The Case data provided can be reviewed with a view to re-performing the key integrity checks performed by investigators, over the completeness and accuracy of the data. The Audit Store controls should have remained relatively constant over the period of allegations when considering those relating to infrastructure downstream of the Branch Database. This is due to the HNG-X project which has influenced a number of other key control areas, leaving the Audit Store architecture relatively untouched.

POL00400064

2.4.3 Phase 1 Procedures

POL instructed procedures. (Scope Area 3)

Procedures
Controls 1. Validate Audit Store controls identified (See Appendix 4 for detail of controls 1a – 1o). 2. Digital Signature controls applied to Message Journal during initiation of transfer to Branch Database. 3. Additional Audit Store Controls identified (See Appendix 4a for detail of controls 3a – 3f). 4. Identification of Audit Store Data Flows at a Detailed Level, including security controls over data at rest, and completeness, accuracy and validity controls over data in transit. **Data** N/A **Substantive** 5. Review source code on screen at Fujitsu headquarters which supports the key inherent control operation around digitally signing transactions posted from the Counter to the Branch Database. 6. Identification of changes relevant to the Audit Store from review of historical documentation, and validation that the AuditStore has remained broadly consistent over time from a controls perspective for the period relevant to the allegations.

POL00400064

Phase 1 Procedures Performed at Interim Reporting Date

It should be noted this work is still going through our 'internal review process' and as such the below statements are subject to change. Any change in conclusions will be communicated immediately and also included in the final report.

Procedures	Conclusions
Controls	
1. Validate Audit Store controls identified (See Appendix 4 for detail of controls 1a – 1o)	1. No Issues Noted
2. Digital Signature controls applied to Message Journal during initiation of transfer to Branch Database.	**2.** No Issues Noted

POL00400064

2.5 Scope Area 4

Scope Area 4: POL commission forensic accountants to review the unmatched balances on POL's general suspense account to explain the relationship (or lack thereof) with branch discrepancies and the extent to which those balances can be attributed to and repaid to specific branches.

2.5.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 1.3.1 above. Specifically for this scope area;

i) POL operate a large network of branches in the UK and offer customers a broad range of products. Whilst the overwhelming majority of transactions are processed successfully a minority of transactions are, inevitably, not processed as expected.

ii) It is important to note that these transactions not processed as expected need not necessarily end up in suspense, despite having been processed according to policy. Our work has taken a holistic view of transactions not processed as expected as it is possible that differences are transferred to suspense despite this not being the 'business as usual' process.

iii) POL use SAP to operate their general Ledger. Within POL chart of accounts in SAP a number of suspense accounts are operated and these are managed by the Finance Service Centre based in Chesterfield.

iv) The suspense accounts that POL have made us aware of during our discussions are listed below. We cannot guarantee this is a complete list of suspense accounts as we have not met with all product owners and knowledge of the existence of suspense accounts is spread out amongst product owners in the business.

   a. Customer Creditor - intended to relate to differences between end consumers in Post Office branches and POL.

   b. Client Creditor - intended to relate to differences between Post Office clients (such as Bank of Ireland, Santander etc.) and POL.

   c. Paystation Creditor - similar to Client Creditor but is used specifically for the Paystation product

   d. Branch Creditor - intended to relate to differences between Post Office branches and POL. Despite it being intended to relate to branches it has not been subject to the same level of detailed retrospective review as Client Creditor by the Finance Service Centre.

   e. Current Agents Customer Creditor - account was only used in 2012 and has a small balance.

   f. ATM Surplus - POL have told us that this account was created post August 2013 for the purpose of branches declaring surpluses in their ATM identified through balancing the ATM.

v) POL's archiving policy in SAP means that the Finance Service Centre is unable to view all suspense transactions in SAP.

vi) These suspense accounts are on the balance sheet and are defined according to their nature, for example whether transactions are expected to relate to branch, customer or client. Not all suspense transactions relate to branch and the naming of an account is no guarantee that the nature of the transaction is consistent with the account name.

vii) If a suspense transaction does relate to a branch then it can either be adverse or favourable for the sub postmaster.

POL00400064

Controls

viii) Workshops with the Finance Service Centre were held to identify controls common to the suspense account process overall, irrespective of product. A number of controls have been identified which we are informed are common across all suspense accounts and products:

a. If a suspense amount is allocated to a branch, the mechanism for this is via a Transaction Correction and the branch must acknowledge and accept this on screen or query it with the Finance Service Centre. Acknowledgement of transaction corrections can be delayed until the end of the month but must be accepted in order to allow roll over between trading periods. Fujitsu have highlighted that a branch can theoretically continue to trade for a protracted period beyond month end before rolling over (i.e. could delay rolling over if they were unhappy with a dispute resolution), but eventually this would cause performance issues.

b. The Finance Service Centre performs probity checks of suspense accounts to review movements to the accounts. These checks are signed off by management in the Finance Service Centre. Suspense amounts are released to P&L after three years and only after exhaustive investigation. This process of releasing amounts takes place on a quarterly basis.

c. Access to post to suspense accounts is restricted to appropriate people.

d. The Post Office chart of accounts in POLSAP includes matching accounts on the balance sheet. Whilst these are not suspense accounts, this provides management with visibility over differences (or lack thereof) between cash taken and client settlement.

ix) POL performed a retrospective review of the Client Creditor suspense account in early 2015 to investigate whether transactions relate to branch. POL have plans to perform similar retrospective views on the other suspense accounts in the new financial year.

x) Separate workshops have been held for ATMs, Green Giros and Epay. The three products were chosen based on time available and our assessment of risk. Further details on our risk assessment are included below. Our objective was to understand what the product was, the end-to-end business process for the product, and how processing issues are resolved. We did not review any other products, or their related processes.

ATMs

xi) ATMs are the automatic telling machines which are installed at post office branches to allow customers to check their balances, withdraw cash and perform other banking services.

xii) We chose to have further discussions on ATMs because they have a high volume of cash of transactions and the process involves significant cash handling both of which increase the risk of fraud or error.

<u>Responsibilities – ATM operation and cash ownership</u>

xiii) The majority of ATMs are operated by Bank of Ireland with cash supplied by POL. However a limited number of ATMs exist where:

a. POL provide the cash and the ATM is provided by another party such as Hanco. This can either be at a branch or offsite such as in a hospital; or

b. The Branch provides the cash and the ATM is provided by another party such as Hanco. POL do not have any involvement in cash settlement where the branch provides its own cash.

xiv) For the most part ATMs are funded with POL cash and operated by Bank of Ireland and therefore POL should be reimbursed for this cash by Bank of Ireland. At 4:30 PM daily Link does a sweep of the ATMs in the network to understand the cash position to support the settlement process.

POL00400064

Balancing of ATMs

xv) We are informed that sub postmasters should balance their ATM at least once per week according to documented policy. This involves obtaining a printed report from the ATM showing how much cash has been loaded, withdrawn, retracted successfully and stuck and comparing it to a physical count of cash by responsible person at the branch.

xvi) Discrepancies could have a number of root causes. The impact of a discrepancy, adverse or favourable, could either be taken by the sub postmaster, POL or Bank of Ireland depending on the specifics. Of particular note are two scenarios, both of which POL have told us do not involve transactions going into suspense:

a. Small disputes - any disputes less than £15 between a customer and the bank is made good by the bank. This results in POL obtaining surplus which is recorded and stored to be set off against other customer disputes. We are informed this is an industry standard rather than a specific POL policy.

b. Retract fraud - POL made a change to their business processes in August 2013 when they became aware of retract fraud at ATMs in their branch network. Retract fraud involves an unscrupulous customer instructing the ATM to withdraw cash and only taking a portion of that cash dispensed. The remaining cash is then retracted into the ATM. The funds are debited in full on the customer's bank statement. The customer then makes contact with their bank to claim that cash was never received and the bank refunds the customer the full amount and deducts this amount from the next settlement run with POL. Customer has fraudulently profited by the portion of cash taken from the ATM and this shows as a discrepancy when the ATM is balanced. Before August 2013 the branch is made responsible for the amount via transaction correction. Since this date POL have been monitoring for retracts and either taking the impact of the loss instead of the sub postmaster or challenging this with Bank of Ireland.

Daily cash declaration process

xvii) As part of an overarching cash declaration process that also includes cash in the branch counter, sub postmasters should manually key in Horizon the amount of cash in the ATM on a daily basis. This is not based on a physical count of cash but the transactions recorded by the ATM during the day.

xviii) POL obtain a feed from bank of Ireland at 5 AM the following day which is loaded into the accounts. Discrepancies between the manually keyed amount and Bank of Ireland feed are investigated by the Finance Service Centre and resolved.

xix) Example root causes include the amount keyed by the responsible person branch is incorrect due to a keying error and the responsible person in the branch has not yet keyed any amount for the day. Items not resolved in 12 weeks of transferred to suspense.

xx) In particular POL have made us aware of differences between ATM reports run by sub postmasters and electronic feeds from Hanco which POL consider to be a possible cause of ATM items in the Client Creditor suspense account.

Green Giros

xxi) Green Giros are pieces of paper issued to qualifying members of the public for Social Security benefits. Green Giros are redeemed for cash on presentation in the branch. The Government, under EU competition rules, put up the contract to administer Green Giros up for tender in 2007. It subsequently awarded the contract to a rival operator and as a result the Green Giros service is no longer offered by POL.

xxii) We chose to have further discussions on Green Giros because POL made us aware of a possible issue. In February/March 2015 the Finance Service Centre performed a retrospective review of suspense transactions on the Client Creditor account to determine the nature of suspense transactions and in particular whether they relate to branch. As part of our discussions POL informed us that a

POL00400064

limited number of Green Giro transactions were identified which did relate to branch but were too old to be allocated to the branch and were also rejected by the branch when offered by the Finance Service Centre.

Cashing the Green Giro

xxiii) The customer presents the person in the branch with the Green Giro. Amounts over £449.49 will not be cashed and those over £100 will only be cashed on presentation of acceptable ID. If the Green Giro is acceptable it will be cashed and the amount will be keyed in Horizon. No other details are captured in Horizon. The Green Giro is retained by the branch and is sent to Santander and Alliance & Leicester in a pouch by post on a daily basis.

Settlement

xxiv) POL has provided its customer with cash from the counter and therefore needs to be reimbursed. Alliance & Leicester and Santander are responsible for settling these amounts with Post Office on behalf of the government. They settle Green Giros with POL on a daily basis based on electronic data from Horizon.

"Truing up"

xxv) Alliance & Leicester and Santander operate a Thursday to Wednesday cash accounting week which is used as the basis of truing up settlement once physical Green Giros have been received from the branch. Any 'unders' or 'overs' at branch level are posted as an adjustment to the next settlement run. There could be a number of root causes for differences, including:

a. The pouch containing the physical Green Giros has not been posted by the branch.

b. The physical Green Giro has been placed in the wrong pouch, for example for a different product at the same bank

c. The pouch has been sent but has not been received by the bank

d. The Green Giro amount has been keyed into Horizon incorrectly by the responsible person at the branch

e. The Green Giro is fraudulent and this has been detected by the bank. For example it is a duplicate has been claimed twice inappropriately or the amount has been fraudulently altered on the slip.

f. The amount is above £100 and there is no evidence that ID was checked by the sub postmaster.

g. The amount is not above £100 but the bank has inappropriately flagged that no ID has been checked in error, despite this not being a requirement.

h. There is no Horizon transaction but the bank has received a physical slip. For example this could be caused by the responsible person at the branch not keying the transaction or the transaction being keyed but not making its way to the branch database in error.

xxvi) The adjustments made to settlement by the banks in a given week usually relate to physical Giros as old as 3 to 6 months. This service level is less timely than, for example, bank account deposits and withdrawals which typically take 3 to 5 weeks.

Epay

xxvii) Epay a product which is delivered using the Paystation hardware managed by Ingenico. Epay allows customers in the branch to top up mobile phones. This can either be achieved by topping up a card held by the customer or by purchasing a paper receipt with a unique code that is redeemable by dialling the mobile phone operator's top up number.

xxviii) We chose to discuss Epay transactions because it was one of four products which POL identified as being a significant contributor of the suspense balance in written correspondence with Second Sight in 2015. We chose this product at random from the four products.

POL00400064

Interface with Horizon

xxix) There is a regular batch file interface between each Paystation terminal and the centralised Horizon branch database. Transactions are grouped into batch files up to a maximum value of £600. This maximum limits the exposure of lost transactions. In the event the Paystation is unavailable, e.g. due to loss of power, transactions will continue to transfer data when and if the Paystation is restored. Each group of transactions has a batch control total so that Ingenico and Horizon can verify the completeness of the batch.

Correction process

xxx) Paystation operators are able to reverse committed transactions within a 10 minute period if they are identified as erroneous.

xxxi) A correction process exists for the event that Paystation is permanently unavailable and committed transactions have occurred which have not reached Horizon in error. Corrections are made only at the request of the branch via an Ingenico incident management report hardcopy form. All corrections must be confirmed post implementation by the operator through a transaction acknowledgment.

Daily reconciliation process

xxxii) Sub postmasters must confirm Epay amounts on Horizon reconcile to their physical receipts on a daily basis.

POL00400064

2.5.2 Summary Table of Phase 0 Procedures and Conclusions

POL Instruction	Procedures Performed	What we have discovered
POL commission forensic accountants to review the unmatched balances on POL's general suspense account to explain the relationship (or lack thereof) with branch discrepancies and the extent to which those balances can be attributed to and repaid to specific branches.	Workshop to understand suspense process and controls common to all products. Workshop to understand Epay process and interaction with suspense accounts. Workshop to understand ATM process and interaction with suspense accounts. Workshop to understand Green Giro process and interaction with suspense accounts. Workshop with Case Handlers to understand available Case Data. Review of suspense account process documentation, where available. Review of letter from POL to Second Sight regarding purpose of client creditors suspense account and POL assessment as to whether relevant to branch. Review breakdown of suspense account transactions from SAP, excluding those archived.	The majority of transactions processed by POL are done so successfully, without issues. Transactions not processed as expected need not necessarily end up in suspense, despite having been processed according to policy. During our enquiries it has been represented to us there are numerous examples where human error by a variety of parties in a business process could result in a transaction not being processed as expected. Perhaps unsurprisingly for a high volume business, the Finance Service Centre team has seen the majority of these types of human error actually occur. In discussing the sample of products we have also been made aware of various attempted or actual frauds against POL by a variety of parties. From a data and systems perspective we see the key risks as Horizon counter transactions not making their way successfully to the centralised branch database, or central transaction amendment processes by privileged Fujitsu. However, no actual instances of data transfer issues have been brought to our attention from our discussions with POL to date, and we highlight within the other scope areas of this document the control environment relevant to the Horizon system responding to these risks. Suspense account transactions are, by their nature, difficult to understand the root cause of. POL performed a detailed review of open transactions in the Client Creditor suspense account in 2015 and were unable to fully conclude on the nature of all suspense transactions despite investing significant time and liaising with the right people in the business.

POL00400064

2.5.3 Phase 1 Procedures

POL instructed procedures. (Scope Area 4)

Procedure's
Controls 1. Validate monthly probity checks take place on all suspense accounts. 2. Validate POL release of suspense accounts takes place on a quarterly basis according to documented policy. 3. Validate sub-postmasters must accept transaction corrections (TC) before they are accepted into the branch accounts. **Data** 4. Using audit log data available to case handlers, validate what percentage of transaction corrections are accepted in the final 2 days of a trading period (month) or in the following month i.e. delayed rollover. 5. Profile Account Balances - Perform general profiling on line items and account balances for the suspense account items, to observe anything which appears to be unusual, which would be followed up with POL finance. Investigation of Items and Attempt to Attribute to Branches to Confirm that the Branch Cannot be Identified - For the suspense accounts which are currently known about being: - Customer Creditor - intended to relate to differences between end consumers in Post Office branches and POL. - Client Creditor - intended to relate to differences between Post Office clients (such as Bank of Ireland, Santander etc.) and POL. - Paystation Creditor - similar to Client Creditor but is used specifically for the Paystation product - Branch Creditor (aka Local Suspense - intended to relate to differences between Post Office branches and POL. Despite it being intended to relate to branches it has not been subject to the same level of detailed retrospective review as Client Creditor by the Finance Service Centre. - Current Agents Customer Creditor - account was only used in 2012 and has a small balance. - ATM Surplus - POL have told us that this account was created post August 2013 for the purpose of branches declaring surpluses in their ATM identified through balancing the ATM.

POL00400064

Procedure's
Select a sample of items for investigation (subject to judgemental sampling, with sample sizes being dictated by the number of line items within each account) and pass to POL Finance for analysis and attempts to allocate to a branch. Items selected to be those which based on the data available appear to be connected to the three currently selected Product types (ePay, ATMs and Green Giros). Deloitte to then review the POL analysis and through meetings and workshops discuss and challenge the conclusions. In addition we will use TB information provided during the course of the work in order to try and validate the completeness of the population of suspense accounts we have been asked to focus on. **Substantive** N/A

Phase 1 Procedures Performed at Interim Reporting Date
It should be noted this work is still going through our 'internal review process' and as such the below statements are subject to change. Any change in conclusions will be communicated immediately and also included in the final report.

Procedure's	Conclusions
Controls 3. Validate sub-postmasters must accept transaction corrections (TC) before they are accepted into the branch accounts.	3. No Issues Noted

Note no procedures have been performed specifically for Scope Area 4 to date. The one procedure listed is a crossover procedure that was performed during testing of other scope areas.

POL00400064

3. Assumptions and Limitations

3.1 Assumptions and Limitations

Our work has been subject to the following exclusions:

1. We have not verified or tested any information or assertions provided directly by you, or directly or indirectly by third parties;
2. For scope areas 1, 2 and 3, only matters relating to Horizon Features and Audit Store within the Horizon processing environment have been considered during our workshops and discussions;
3. We have not provided a legal or any other opinion as to the completeness and accuracy of processing of Horizon at any point throughout the work;
4. We have not had direct contact with any third parties other than named contacts that you have provided to us (Appendix 1);
5. We have not reviewed any contractual provisions in place between you and third parties;
6. Our work was limited by gaps existing in the information available, relating to both the granularity of information and the existence of the Horizon Features[1] over the entire timeline of operation of Horizon and suspense account process documentation. The effect of which is that there are in gaps within what we are able to comment upon over this timeline;

[1] "Horizon Features" is a term we have introduced to represent those features of the Horizon processing environment, including IT management and business use controls, which provide that:

- Movements in Branch ledgers have the full ownership and visibility of sub-postmasters; and
- Audit trails kept by the system are complete and accurate.

7. We have not validated or commented on the quality of the Assurance Work[2] supplied to us.

[2] Since its implementation in branches, POL has commissioned or has received a number of pieces of work relating to the Horizon processing environment, to provide comfort over its integrity. This work, referred to in our report as the "Assurance Work", provides documented assertions relating to aspects of the design and operation of the Horizon processing environment. The Assurance Work includes IT project documents; operational policies and procedures; internal and external investigations and reviews; independent audits; and emails confirming otherwise verbal assertions.

Our work was also based on the assumption that the documents provided and assertions made are a complete and accurate representation of the Horizon design, audit store process and suspense account process. We therefore cannot comment as to whether other processes would need consideration in the context of the Matters.

POL00400064

Appendix 1

Documents Reviewed (detail)

Document Ref	Document Title
DES/APP/HLD/0047	HNG-X Counter Application High Level Design
DES/APP/HLD/0020	Branch Database High Level Design
DES/APP/HLD/0030	Audit Data Collection & Storage High Level Design
DES/APP/HLD/0029	Audit Data Retrieval High Level Design
ARC/SOL/ARC/0006	HNG-X Architecture - Global Users
DEV/APP/LLD/0065	BRDBC002 – BRDB Message Journal Auditing LLD
DEV/APP/LLD/0014	Host Branch Database Audit Archive Purge Low Level Design
DEV/APP/LLD/0142	Host BRDB Transaction Correction Tool Low Level Design
DES/APP/SPG/0001	Host branch database support guide
DEV/APP/LLD/0199	Schema definition for branch database, standby branch database and branch support system
DES/APP/HLD/0035	Exceptions and logging frameworks high level design.
DES/APP/IFS/0002	HNG-X:RDDS to Branch Database - Counters & HBS Reference Data and Memo Submission Interface Specification
DES/APP/IFS/0012	BAL Service Interface Specification
DES/APP/HLD/0083	HNG-X Counter Subsystem : Recovery Management
DES/APP/HLD/0021	Branch Database Scheduling High Level Design
DES/APP/IFS/0007	Branch Database to Legacy Host Interface Specification
DES/APP/IFS/0001	HNG-X: RDMC / RDDS to Branch Database Application Interface Specification
DES/APP/HLD/0049	HNG-X Generic Reports Data Extract HLD
DES/APP/HLD/0057	HNG-X Counter Infrastructure: Service and Process Control High Level Design
ARC/SOL/ARC/0001	HNG-X Solution Architecture Outline
DEV/APP/LLD/0071	Audit Data Retrieval Low Level Design
POLSAP/DES/APP/STG/0001	POLSAP Archiving Strategy

Documents Reviewed (high level)

Document Ref	Document Title
DEV/INF/ION/0001	Archive Server Configuration
DES/SEC/HLD/0003	HNG-X KEY MANAGEMENT HIGH LEVEL DESIGN
DES/APP/HLD0041	HNG-X Counter Applications: Business Logic Subsystem High Level Design
DES/APP/IFS/0018	XML Message Audit between Counter or HBS and BAL/OSR
DES/APP/HLD/0012	DVLA Internal Web Service High Level Design
ARC/SEC/ARC/0003	HNG-X Technical Security Architecture
DEV/APP/LLD/0204	Host BRDB Update Outstanding Recovery Transaction Tool Low Level Design
DES/APP/HLD/0070	Host Applications Monitoring High Level Design
DEV/APP/LLD/0151	HNGX BRDB HOST: BRANCH SUPPORT DATABASE LOW LEVEL DESIGN

POL00400064

Individuals Interviewed

Name	Job Title
Patrick Bourke	POL – 'Bramble' Project Manager
Mark Underwood	POL – 'Bramble' Project Manager
Rodric Williams	POL – POL Legal
Rod Ismay	POL - Head of Finance Service Centre
Lorraine Garvey	POL - Enquiries Manager
Sarah Haywood	POL - Finance Team Leader
Tracy Middleton	POL - Finance Team Leader
Michael Harvey	Fujitsu -Head of Commercial
Pete Newsome	Fujitsu - Business Change Manager
Torstein Godeseth	Fujitsu - Chief Architect
Steve Bansal	Fujitsu - Senior Service Delivery Manager
Alan Holmes	Fujitsu - Customer Solution Architect
Gerald Barnes	Fujitsu -Senior Software & Solutions Designer
Gareth Seemungal	Fujitsu - Senior Software & Solutions Designer

POL00400064

Appendix 2

Scope area 1 – Potential Analytics Procedures

Ref	Analytics Procedure
A	**Completeness Test -** Identify gaps in audit log sequencing
B	**Completeness Test -** Identify gaps in transaction times during working hours
C	**Completeness Test -** Identify two user logon events in sequence without the expected logoff event in between, an indicator of a connectivity issue
D	**Completeness Test -** Identify recovery transactions
E	**Accuracy Test -** Identify zero valued transactions
F	**Accuracy Test -** Identify branches which are out of balance based on transactional data available (should not be possible based on inherent system controls).
G	**Integrity Test -** Identify transactions posted by non-branch users without subsequent branch acknowledgement.
H	**Integrity Test -** Identify balancing transactions.

POL00400064

Appendix 3

Scope area 2 – Balancing Transactions Controls

Ref	Control Description
A	SSC will have privileges of only inserting balancing / correcting transactions to relevant tables in the database. SSC will not have any privileges to update or delete records in the database.
B	If the process fails (e.g. transaction file is found to be invalid), then the transaction file will not be moved and an error message will be written to standard output.
C	Any writes by the SSC to BRDB must be audited. The mechanism for inserting acorrection record must ensure that the auditing of that action performed must be atomic. There also needs a level of obfuscation to ensure that the audit mechanism is robust.

Appendix 3a

Scope area 2 – Balancing Transactions Controls (Broader population)

Ref	Control Description
A	All inserts will be audited in the table BRDB_TXN_CORR_TOOL_JOURNAL.
B	The PL/SQL package PKG_BRDB_TXN_CORRECTION will be owned by Oracle user "OPS$SUPPORTTOOLUSER".
C	The PL/SQL package PKG_BRDB_TXN_CORRECTION will execute with the permissions of the OPS$SUPPORTTOOLUSER account and can only insert rows into the transaction tables as controlled by an entry in BRDB_SYSTEM_PARAMETERS. The account will not have update or delete privileges.
D	Each of the transaction tables that are allowed to have balancing transactions inserted on them has an associated template file. Each file contains a template of an INSERT statement for that table, in the required format, and listing all of the columns on the table. Users should create their own transaction file based upon the relevant template file, substituting the values they require into the SQL. Note that some of the column values specified in the template should not be changed – these are annotated with comments as appropriate.
E	When execution is complete the file is then moved to directory '/app/brdb/trans/support/brdbx015/output' and the log file is created in directory '/app/brdb/trans/support/brdbx015/log'. Log file will be named using the following convention: <transaction_file_name>_<CCYYMMDDHHMISS>.log Access to these 2 directories is appropriately restricted.
F	It is expected that only a small number of skilled staff will run this tool and that they will have detailed guidance as to when and how to use the tool (For example by restriction of staff to "OPS$SUPPORTTOOLUSER").
G	From the Unix command prompt, execute the following ./BRDBX015.sh MyTransactionFile.sql 2001 where the first parameter is the transaction file name and the second parameter is the branch codewhere the balancing transaction is going to be applied. Note that the branch code must exist in the database, and must not be for a closed branch. If this is not the case, then an error message will be shown and the run aborted.
H	The correction tool places a number of constraints on the contents of the transaction file. These are necessary in order to provide a defined baseline upon which it can base its operation. If any of the constraints are violated then validation will detect it and abort the run with a meaningful error message. The constraints are as follows: • The transaction file must be less than 32K in size • The transaction file must only contain Unix-style end of line markers (EOL), not DOS format end of line markers (CR/EOL) • The transaction file can only contain a single SQL statement. If more than one balancing transaction is required then more than one transaction file must be created, each of which is executed with a separate run of the tool

POL00400064

Ref	Control Description
	• If the transaction file contains an introductory comment, then it must be a '/* …… */' style comment, not a '-- ……' style comment • The closing '*/' of the introductory comment must have a trailing space (i.e. '….. */ ') • The run symbol at the end of the SQL must be a ';' , not '/', and must have a trailing space (i.e. '…..; ') • The SQL must be a valid SQL statement according to the normal Oracle SQL parsing rules (e.g. valid syntax, objects accessible etc) • The SQL must begin with 'INSERT INTO OPS$BRDB.' and be of the form 'INSERT INTO ….. SELECT ….. FROM dual, (SELECT ….. FROM …. WHERE …..)'. • The table name must be one of the tables named in the BRDB_TXN_CORRECTION_ALLOWED_TABLES1 or BRDB_TXN_CORRECTION_ALLOWED_TABLES2 configuration parameters • All of the columns that exist on the table in question must be explicitly named. It is not necessary for every listed column to be on a separate line, but this is advisable for readability. • The values to be inserted must be provided by the 'SELECT … FROM dual …'. Each value must be on a separate line. Trailing comments are allowed, but must be a '-- …..' style comment. Any such comment must not include any commas. All columns must have values provided for them (even if that value is NULL). • Certain columns are common between a subset of the transaction tables. In some cases, these columns should be set to the same value no matter what table is in use. With the exception of the bind variables listed earlier, the value that the SQL will try to insert is under the control of the user (i.e. it is determined by the value specified in the SQL). However, the tool can be configured to validate that the value specified in the SQL matches that expected. In order to do this, set the BRDB_TXN_CORRECTION_ENFORCED_VALUES configuration parameter to include the field and the required value. The parameter is populated as a comma-delimited list of name/value pairs, where the name is the name of the column name, and the value is the value to be enforced. As released, this configuration parameter is set to: NODE_ID=99,APP_SERVER_NODE_NAME=999,BRANCH_USER=:bind_SSC_user,BRDB_INSTANCE_NAME=:bind_instance_name which, for example. ensures that if a 'node_id' column exists on the transaction table, it's value is specified as 99. If there is no 'node_id' on the transaction table, then no value isenforced for that field. Note that if the parameter does not exist, then no values are enforced in the SQL.
I	The SQL statement being executed will be logged in the table BRDB_TXN_CORR_JOURNAL. The format of the data to be written to the column JOURNAL_XML is: "<?xml version="1.0" encoding="UTF-8"?> <Support_Insert> <Unix_User>Unix User Name</Unix_User> <Oracle_User>Oracle User Name</Oracle_User> <Sql>SQL Statement</Sql> </Support_Insert>" where : • Unix User Name is the Unix user name under which the user logged in • Oracle User Name is Oracle user that is carrying out the actual insert i.e. SUPPORTTOOLUSER • SQL Statement is the final (i.e. after substituting actual values for bind variables) SQL that is executed to insert the balancing transaction
J	As records are being written to the audit files, the process must optionally be able to monitor if the set of Journal Sequence-Numbers for a node in a Branch is dense. The check should only be performed when the value of mandatory System-Parameter 'JOURNAL_SEQ_DENSE_SET_CHECK_ENABLED' is "TRUE". When a missing journal entry is encountered, a message should be written on standard output along the lines of "…records between sequence numbers M and N are missing…". Once the list of auditable messages for a node iscompleted, an Operational exception should be raised to indicate the count of missing sequence numbers. Duplicate records are not possible due to the primary key on this table.
K	Unix shell script BRDBX015.sh which is in the /app/brdb/trans/support/brdbx015 directory. It is deliberately kept separate from the standard $BRDB_SH directory so that access to the script and the associated components can be restricted to authorised users. The shell script calls the PL/SQL package PKG_BRDB_TXN_CORRECTION.

POL00400064

Ref	Control Description
L	PL/SQL package PKG_BRDB_TXN_CORRECTION, which resides within the Branch Database and is owned by Oracle user OPS$SUPPORTTOOLUSER. The PL/SQL package is the component that validates, creates and audits the balancing transaction.
M	If an Oracle node/instance failure occurs, the utility will fail with an error code of 99. For all other failures, it will fail with an error code of 1 and log an operational exception in BRDB_OPERATIONAL_EXCEPTIONS.
N	The SQL in the transaction file is validated as follows. Any validation failures are displayed to standard output and logged to the log file. • Check that the file does not contain any carriage returns, indicating DOS format EOL markers • Check that the SQL in the transaction file parses according to the standard Oracle rules (e.g. syntax, privileges etc). This is done using the standard Oracle DBMS_SQL.PARSE procedure. • Check that there is only a single SQL statement in the transaction file. Note that in most cases, this will be detected by the previous parsing step. However, the fact that the parsing does this is not described in the Oracle documentation, so it may be changed in future releases of Oracle. Therefore, this validation provides security if the behaviour of the Oracle procedure is changed at a later date. • Check that the SQL begins with 'INSERT INTO OPS$BRDB.' • Check that the table named in the SQL is one of the tables listed in the two BRDB_TXN_CORRECTION_ALLOWED_TABLES<n> configuration parameters. Note that as long as the privileges are set up correctly (i.e. OPS$SUPPORTTOOLUSER only has insert privileges on the allowed tables), any attempt to insert a balancing transaction on a non-allowed table will cause the previous parsing step to fail (because the user would not have the necessary privileges). Therefore, this validation provides security in case the privileges are not correctly set up. • Check that all the columns named in the SQL exist on the table, and that all the columns on the table are named in the SQL • Check that the values to be inserted are provided by a SELECT … FROM dual, (SELECT … FROM … WHERE) i.e. not a VALUES • Check that if any of the name/value pairs that are listed in the BRDB_TXN_CORRECTION_ENFORCED_VALUES configuration parameter are present on the table, they are set to the listed value.
O	Balancing transaction audit files (BRDBC033), unlike the files produced by BRDBC002, are not compressed, but are still encrypted.

POL00400064

Appendix 4

Scope area 3 – Audit Store Controls Listing

Ref	Control Description
A	Audit tracks that are gathered at one data centre are replicated to the Audit server at the remote data centre. This replication process is managed by the Audit Track Sealer. As Audit tracks are securedto the Audit archive, they are moved to an export area awaiting transfer to the remote campus. A second file, containing the calculated seal value for the audit track is also stored in the export area.
B	Audit tracks and seals are copied, using robocopy, to the equivalent import area on the remote audit server as part of Audit server overnight schedule. On arrival, the sealer on the remote audit server recalculates the seal value of the imported audit track and compares it with the original value in theimported seal file. Assuming they match, the file is then written to the remote Audit archive. If the seals do not match, the Audit trackand seal file are moved to a holding area and an event is raised. Manual investigation is necessary to investigate the cause of the discrepancy.
C	There will be a single instance of the ATS that concurrently accepts files for sealing/seal checking from ATG and ATR and notifies sealed files to the ATD and into the Sealer Database for subsequent use by the Audit Track Extractor. The ATS shall collect files for sealing via I-ATS-4 and shall write a log of its activities to the ATD via I-ATS-2. In sealing a file the seal shall be generated using a secure hash algorithm, the MD5 algorithm has been selected. Once a file has had a seal calculated the file will be written to Centeraand details will be stored in the Audit Track Seal Database via I-ATS-5.
D	Access to the Audit Track files for gatheringshall be via Samba (for Unix systems) or NTFS (for Windows systems). Access to the sub directory shall be limited to the application generating the Audit Track and the Audit Track Gatherer. Audit track files should be written in write-append mode.
E	All users (including administrators) of the Audit Workstation and Audit Server shall log onto systems using two factor authentication in conjunction with the HNG-X Active Directory system. Each user shall be uniquely identifiable.
F	The remote directories from which the Audit Server gathers Audit Tracks will be configured so that only the Audit Server (or an administrator who has been explicitly given permission) is able to delete files in the directory.
G	All Audit Server and Audit Workstation and Centera hardware shall be held in physically secure areas where physical access to the systems is controlled.
H	There shall be separate roles for: • Audit Server (inc. Audit Workstation) Administration • Fujitsu Services Audit Staff The roles shall be mutually exclusive, i.e. no one individual shall be given access rights of more than one role.
I	The Fujitsu Services Audit Staff role shall not have any write, modify or delete access to the Audit Archive.
J	The following integrity checks will be applied to the data • Completeness of data – contiguous message sequence numbers • Integrity of individual messages ○ For Riposte data the message CRC should be checked ○ For HNG-X data the message signature will be verified Separate Riposte and HNG-X summaries of the results of the integrity checks are generated. They should detail: • Summary of the message sequence runs broken down by counter Id. This should include startand end date/times and start and end message sequence numbers. Any gaps in the message sequence runs must be highlighted. • Summary of messages that have failed individual message integrity checks Any failure of the data integrity checks will not prevent subsequent execution of the query. The audit workstation user will be warned of the failure via the server process status notification mechanism.
K	As Audit tracks are retrieved from the archive, they are seal checked (by re-application of the MD5 message digest function) to ensure that the source data has not been tampered with while it was stored in the archive.
L	Only authorised users may access the Audit workstation applications. Authorised users are required to log on to the workstation using two factor authentication and the HNG-X Identity Management system. An Active Directory group

POL00400064

Ref	Control Description
	named AUDIT_USER will be created with the rights required to utilise the workstation applications. Authorised users will be added to this group.
M	All retrievals of audit data are performed using the Audit Extractor Client, and all such user actions are themselves audited. It is not possible for users to access the archive by any other means.
N	Audit workstations and Atalla NSPs are located in secure areas. Only authorised users are given physical access to these areas.
O	All auditable messages logged during a calendar day will be made available to the audit system in uncompressed form as a part of Branch Database batch overnight processing. The message journal is implemented in the form of a single Oracle table named BRDB_RX_MESSAGE_JOURNAL. Uniqueness is controlled at the level of a Branch counter using a dense sequence known as the Journal Sequence-Number

Appendix 4a

Scope area 3 – Audit Store Controls Listing (broader population)

Ref	Control Description
A	The following operating system level events on the Audit Server will be audited via the System Management event monitoring facilities: • Log on/Log off (including unsuccessful log on attempts) • File Creation, Deletion and Modification (on selected files) • Modifications to system configuration (inc software configuration and account details) • System start up and shut down • Recovery actions • Exception conditions • Change of user rights
B	The Audit Server Administrator role shall have full access to manage all of the Audit Server and Audit Workstation file stores and shall be granted the necessary Windows privileges.
C	POL staff will not be given direct access to the Audit Workstation to safeguard other parts of the HNGX system. Instead nominated Fujitsu Services personnel will supply audit information as requested by Post Office.
D	User Log/On events are included in the Windows event log. Users are allocated to a specific role which enables them to access the Audit databases.
E	Baskets are stored for a defined period of time. The configuration of this parameterand the audit trail around changes to it need to inspected in order to provide assurance over the maintenance time period for audit purposes.
F	POL controls around processing of received data from Fujitsu following a successful ARQ including validation checks.

POL00400064

Appendix 5

Glossary

XXX