POL00400125

Deloitte.

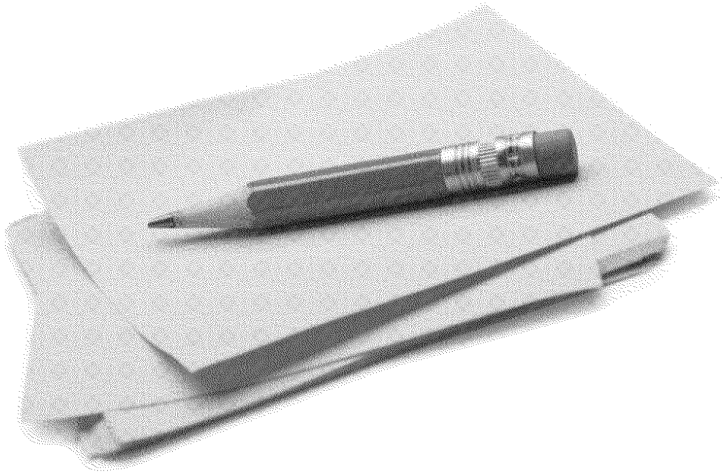
PRIVATE AND CONFIDENTIAL – SUBJECT TO LEGAL PRIVILEGE

'Bramble' – Draft Report

Draft for discussion

THIS IS A DRAFT DISCUSSION DOCUMENT AND REPRESENTS A WORK IN PROGRESS AND MAY CONTAIN PRELIMINARY RESULTS OR CONCLUSIONS INCOMPLETE INFORMATION OR INFORMATION WHICH IS SUBJECT TO CHANGE

31 October 2016



POL00400125

Contents

POL00400125

1 Executive Summary

All results highlighted within this report are provisional as our QA processes remain ongoing due to outstanding evidence from Fujitsu and as a result our findings may change as the work performed is finalised.

1.1 Background

Post Office Limited (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"). The 'Allegations' span a period of over 15 years, some pre date 2000 and others relate to 2016. In response to the commencement of litigation proceedings, Deloitte has been instructed to plan and execute proceduresand respond to three scope areas supporting POLs ability to understand how Horizon (HNG-X) has been operated to prevent incorrect system operation that could have resulted in Sub-postmaster detriment.

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

(i) *Scope Area 1* - 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* - 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* - 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.

Against each of these three scope areas the main body of this 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 undertake in response to the planning activities; and

(iv) Results of these testing procedures.

1.2 Summary of Results

A summary of key controls tested and results are set out below. A full set of agreed procedures tested and associated results has been included in Section 3 of this report. These should be reviewed in tandem with the assumptions and limitations that have been included in Section 5.

POL00400125

1.2.1 Scope Area 1

Scope Area 1: *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.*

We have performed testing of key inherent system controls, together with review ofsome of the source code which supports the correct operation of the system in relation to 'bugs' (error, flaw, failure or fault in a system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways) which may have given rise to or contributed to the allegations under investigation. These are controls which in our scoping discussion with POL and Fujitsu have been determined to be fundamental to protecting the integrity of transaction data within thesystem.

The key controls identified were:

- All transactions on the Horizon Counter balance to zero – *No Relevant Exceptions Noted.*
- Transactions are atomically (either in entirety, or not at all) written to the Branch Database – *No Relevant Exceptions Noted.*
- Digital Signature controls are applied to the Message Journal during initiation of transfer to Branch Database, ensuring the integrity of data. – *No Relevant Exceptions Noted.*
- Access to mechanisms for managing the digital signatures are segregated from database administration responsibilities (via system access rights restrictions), meaning that even if such access rights be abused the digital signature that is included with every Counter and Kiosk transaction could not be spoofed.– *Relevant Exceptions Noted.*

  The exception noted was

  - *'A number of users have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'*
- Transaction Acceptance (in relation to interface file receipt for non-Counter originated interface files) is required by Sub Postmaster's in order to be accepted into branch accounting records. – *No Relevant Exceptions Noted.*
- Recovery processes are in place for transactions in the event of connectivity failure. – *Relevant Exceptions Noted.*

  The exceptions noted were:

  - *'For one of the transaction recovery scenarios tested (whereby a user session is automatically logged out after a period of inactivity – 59 minutes after the session screen being locked), it was noted that Post Office business rules are in place for Horizon to automatically commit unprocessed transactions to the branch database tables. This would have the effect of committing any unprocessed transactions within a basket to the branch database. However 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.'*
  - *'Where a new product is created, the recovery script could theoretically be coded to do nothing, meaning no recovery of transactions would occur in the event of connection failure - no rollbacks or roll-forwards would happen in this case.'*

  The first exception could lead to an increased risk that Sub-postmasters are unaware of transactions being posted in a power failure, although they are notified by receipt that this has occurred. The second exception could lead to the risk of inappropriate/inaccurate resolution to a recovery situation.

The above controls were tested at a recent point in time, as they are system controls. Given this limitation the following procedures were undertaken over change control, as changes to the system are subject to the change control process in place over the Horizon system:

POL00400125

- A review of sources of assurance around change control was performed and it was noted that three ISAE3402 reports were performed covering the period April-December in 2012, 2013 and 2014 by professional services firm Ernst & Young LLP. The scope of the report was seen to include 'Fujitsu's system of IT Infrastructure Services supporting POL's POLSAP and HNG-X applications'. Within each reports' scope was a control objective relating to change management, and in each report reviewed no deviations were noted against this objective, or any related controls.
- Further it was identified through change documentation review, and discussion with Fujitsu SMEs that various controls tested had specifically changed, either since inception of HNG-X (replacing Riposte) in 2010, or changed during the lifespan of Riposte. Please see Appendix 5 for a full list of controls tested and a view on whether the controls have been consistent.

  In summary the major change affecting the operation of controls in relation to this scope area is the creation of the Branch Database (BRDB) to replace individual branch databases (2010). This change fundamentally altered the operation of many controls tested. Whilst Fujitsu have attempted to give a view on controls in operation in the Riposte system, much of the knowledge of this system has leftthe business.

Whilst not causing an exception to one of the controls covered by the scope of our work the following exception relating to General IT Controls over Horizon was noted:

- *One Fujitsu user has access to both development and live environments of HNG-X, contravening typically expected segregation between environments in a change control process.*

Fujitsu stated that:

"*Whilst we appreciate that there is lack of segregation of duties here for Gerald between Live and Development, it is felt that there is a strong business need for this access for Gerald. He provides 4th line/final line support for the audit service and is in regular weekly contact with the Security audit team to assist them in resolving queries with the audit service. He is the lead designer/developer and system owner.*

Additionally there are compensating controls in place such as CCTV, and the auditing (performed by Fujitsu) we have in place (and the technical controls around not being able to change audit items for 7 years) acts as a safeguard against anyone with access trying to change anything in an unauthorised way."

In addition to the system controls noted above, the following analytics procedures were performed to support this scope area:

- Review of the case data available (relevant to allegations) for transactions indicating items of risk from a system functionality perspective. The analytical procedures outlined in Appendix 6 were undertaken, and a number of items of interest were noted, see Appendix 6a for details and summary of findings. One finding of note is that 'there were 59 (0.0019%) session ids from a total of 3,074,830 which were out of balance based on the transactional data received. Those 59 session ids out of balance related to 16 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-x in 2010.

  POL investigators have been handed this information for further investigation. In short, whilst various characteristics were noted that could be indicative of risk within the system, further manual investigation will be required by POL's investigators to conclude. This has been discussed with POL management during the course of our work.

1.2.2 Scope Area 2

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.

POL00400125

In performing our procedures against this scope area, we have worked with POL and Fujitsu to identify other methods of posting transactions which impact a branch accounts, without knowledge of the sub-postmaster which in the context of the allegations is the more generic risk illustrated by Balancing Transactions. This highlighted other areas of risk, such as:

- 'Global Users' – being central users who can access branches remotely for support purposes. Critically such users are not able to post transactions remotely, but only when physically in the branch.
- Database and Operating System Users with sufficient privileges to post transactions directly to the database from outside of Horizon, thereby bypassing the system controls to manage activity.

These areas have been brought into scope.

In summary across each of these areas, including Balancing Transactions, controls were noted to be operating effectively. In particular, based on the procedures we have performed:

- Logical Access rights to these sensitive functions had been appropriately restricted. – *No Relevant Exceptions Noted.*
- Any writes by the Shared Service Centre (SSC) to the Branch Database (BRDB) must be audited. The mechanism for inserting a correction record must ensure that the auditing of that action performed must be atomic. – *No Relevant Exceptions Noted.*
- Access to these mechanisms is segregated from key management responsibilities (via system access rights restrictions), meaning that should such access rights be abused the digital signature that is included with every Counter and Kiosk transaction could not be spoofed. – *Relevant Exceptions Noted.*

  The exception noted was:

  - *'A number of users have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'*
- It was also noted via a control walkthrough that any Transaction Corrections created by POL Finance must be accepted by a Postmaster at branch prior to affecting branch accounts. – *No Relevant Exceptions Noted.*
- Inherent system controls around Global Users were tested, notably that Global users with a Role of ADMIN cannot log onto any Branch other than Global (including Remote access controls to branch infrastructure (e.g. Counter)). – *No Relevant Exceptions Noted.*
- 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. – *Relevant exception noted.*

  The exception noted was:

  - *'The control wording is not accurate. A small number of users are granted extended privileges which enable them to update / delete records. However the control is operating in line with management's expectations. Access to the privileged role is restricted to users explicitly authorised for this access. User actions are audit logged, and not proactively reviewed.'*

The above controls were tested at a recent point in time, as they are system controls. Given the limitations around this the following procedures were undertaken over change control, as changes to the system are subject to the change control process in place over the Horizon system:

- A review of sources of assurance around change control was performed and it was noted that three ISAE3402 reports were performed covering the period April-December in 2012, 2013 and 2014 by professional services firm Ernst & Young. The scope of the report was seen to include 'Fujitsu's system of IT Infrastructure Services supporting POL's POLSAP and HNG-X applications'. Within each reports scope was a control objective relating to change management, and in each report reviewed no deviations were noted against this objective, or any related controls.

POL00400125

- Further it was identified through change documentation review, and discussion with Fujitsu SMEs that various controls tested had specifically changed, either since inception of HNG-X (replacing Riposte) in 2010, or changed during the lifespan of Riposte. Please see Appendix 5 for a full list of controls tested and a view on whether the controls have been consistent.

  In summary the major change affecting the operation of controls tested is the creation of the BRDB to replace individual branch databases (2010). This change fundamentally altered the operation of many controls tested. It is not known whether balancing transactions existed in Riposte, as much of the knowledge of this system has left the business.

An exception was noted relating to a core General IT Control exception around Segregation of Duties, please see page 4 above where this issue is described in detail.

In addition to the system controls noted above, the following analytics procedures were performed to support this scope area:

- All available audit data over the use of Balancing Transactions was inspected (12/03/2010 – 28/05/2016) and it was noted that only 1 'true' Balancing Transaction was inserted, it did not relate to a branch involved in the allegations, and the branch was made aware of the transaction prior to insertion. Other uses of the tool used to insert Balancing Transactions were noted, however they did not affect transactional data and related to the update of a specific flag (SU) to enable continued processing.

1.2.3 Scope Area 3

Scope Area 3: 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.

In performing our procedures against this scope area, we have worked with POL and Fujitsu to identify how baskets of transactions flow from creation at the counter, through the sealed audit store (See Background section for a high level overview).

Further we have tested controls over the accuracy, completeness and validity of the flow of data into the audit store, which is used as the master data point for audit purposes. We highlight the following key controls during scoping as being fundamental to ensuring the accuracy, completeness and validity of this data flow:

- The flow of data from counter to audit store was mapped at a detailed level (See Section 1 for high level overview). Security controls over data at rest (when held in an intermediate location), and completeness and accuracy controls over data in transit (transfer of data from one holding location to another) including exception monitoring were tested. – *No Relevant Exceptions Noted.*
- Security controls over access to the audit servers, and audit store were tested, specifically that there are separate roles and a clear segregation between audit server administration staff, who administer the architecture, and Fujitsu service audit staff, who have access to retrieve data from the audit store via an audit workstation. – *No Relevant Exceptions Noted.*
- Access to mechanisms for managing the digital signatures are segregated from database administration responsibilities (via system access rights restrictions), meaning that even if such access rights be abused the digital signature that is included with every Counter and Kiosk transaction could not be spoofed. – *Relevant Exceptions Noted.*

  The exception noted was:

  - *'A number of users have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital*

POL00400125

signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'

- The ATS (Audit Track Scheduler) collects files for sealing and records a log of its activities to the ATD (Audit Track Database). In sealing a file the seal is generated using a MD5 hash algorithm. Once a file has had a seal calculated the file is written to Centera and details are stored in the Audit Track Seal Database. – *No Relevant Exceptions Noted.*
- Audit tracks and seals are copied 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 the imported seal file. Assuming they match, the file is then written to the remote Audit archive. If the seals do not match, the Audit track and seal file are moved to a holding area and an event is raised. Manual investigation is necessary to investigate the cause of the discrepancy (which could be indicative of tampering with the data in between the two Audit servers). – *No Relevant Exceptions Noted.*
- Audit tracks that are gathered at one data centre are replicated to the Audit server at the remote data centre. – *No Relevant Exceptions Noted.*
- As Audit tracks are retrieved from the archive, their seals are 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. The digital signature check is also applied at this point to ensure data integrity. – *No Relevant Exceptions Noted.*
- The remote directories from which the Audit Server gathers Audit Tracks is configured so that only the Audit Server (or an administrator who has been explicitly given permission) is able to delete files in the directory. – *No Relevant Exceptions Noted.*
- All users (including administrators) of the Audit Workstation and Audit Server log onto systems using two factor authentication in conjunction with the HNG-X Active Directory system. Each user is uniquely identifiable. – *No Relevant Exceptions Noted.*
- The following operating system level events on the Audit Server are 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 (incl. software configuration and account details)
    - System start up and shut down
    - Change of user rights

Relevant Exceptions Noted:

- *'Review of the audit settings for the Audit Server noted that the audit policy change which relates to change of user rights was set to log success events only, with failure not enabled.'*

The above controls were tested at a recent point in time, as they are system controls. Given the limitations around this the following procedures were undertaken over change control, as changes to the system are subject to the change control process in place over the Horizon system:

- A review of sources of assurance around change control was performed and it was noted that three ISAE3402 reports were performed covering the period April-December in 2012, 2013 and 2014 by professional services firm Ernst & Young. The scope of the report was seen to include 'Fujitsu's system of IT Infrastructure Services supporting POL's POLSAP and HNG-X applications'. Within each reports scope was a control objective relating to change management, and in each report reviewed no deviations were noted against this objective, or any related controls.
- Further it was identified through change documentation review, and discussion with Fujitsu SMEs that various controls tested had specifically changed, either since inception of HNG-X (replacing Riposte) in 2010, or

POL00400125

changed during the lifespan of Riposte. Please see Appendix 5 for a full list of controls tested and a view on whether the controls have been consistent.

In summary it is understood controls relating to the audit server and store have been relatively consistent throughout the lifetime of Riposte and Horizon. It should be noted that whilst Fujitsu have attempted to give a view on controls in operation in the Riposte system, much of the knowledge of this system has left the business.

An exception was noted relating to a core General IT Control exception around Segregation of Duties, please see page 4 above where this issue is described in detail.

In addition to the system controls noted above, the following procedures were performed to support this scope area:

- The process of Journal-Sequence-Numbering (each transaction is given a unique ID of 1 greater than the previous transaction), whereby completeness checks are performed over these JSNs, is an optional setting within the system (which assures the completeness of messages from the counter in the audit store). Testing supported that this control has been enabled since 2010 and not turned off since inception in 2010.

1.3 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 system (HNG-X) operating at the time of our review, and Finance controls testing will cover controls in place at the time of our review. 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 have commented on the evidence that supports the view that the control was operating in the relevant period where we were 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 limited the volume of data that is able to be retrieved and interrogated. Also any controls testing is subject to the availability of evidence.

Finally our work performed for Phase 0 and proposed/tested procedures for Phase 1 are specifically limited to the three 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 three scope areas as above.

Please see Section 5 for a full list of assumptions and inherent limitations.

POL00400125

2 Background

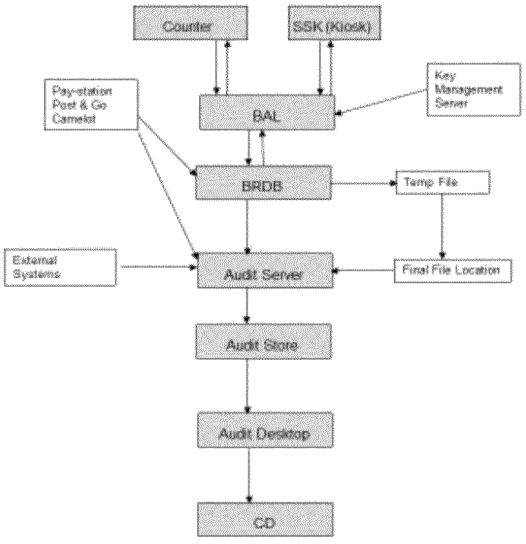
The Horizon system was developed by Fujitsu and is the core operational and Electronic Point of Sales (EPOS) platform for the Post Office network. Whilst formal benchmarking data is not available, it is considered by interviewed stakeholders to be one of the largest computer systems in existence in terms 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 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 and 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 data for the branches, with a Counter application held locally within the branch which connects to the branch database as necessary. 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:

Indicative Data Flow Overview



System	Description and 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 in real time.
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 from POL, Fujitsu audit staff can use the Audit Desktop to query the audit store to extract specified data. Upon extraction from Audit Store – Audit Desktop, the integrity of the data is confirmed via the digital signature and seal check.
CD	A CD is produced with the requested Audit Data.

POL00400125

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 data flows at the Branch database and the chain of subsequent data movements.

In considering these diverse data feeds a key concept is those which use a public key infrastructure (Counter) 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).

2.1 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.

The table below shows how each potential risk relates to POL's scope areas:

	Requested Scope Areas		
	1 - 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 - 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 - 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.
R1	✓		
R2		✓	
R3		✓	
R4		✓	✓

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.

POL00400125

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

POL00400125

3 Scope and Approach

3.1 Scope of Work

We have structured our work around the three 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.

3.2 Summary of Approach and Work Performed

The work was performed in two phases. Phase 0 was 'Discovery' and Phase 1 was 'Testing'.

3.2.1 Phase 0 - Discovery

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

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

- Review of relevant technical documentation as 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 inAppendix 1.
- Workshops with Finance staff in Chesterfield on 14th and 23rd March, and 18th April 2016.
- Workshop with Fujitsu staff in Bracknell on 14th April 2016.
- Workshop with Case Handlers in Chesterfield on 8th April 2016

POL00400125

The aim of these procedures was:

- To enhance Deloitte's previous understanding of the *key concepts, processes, risks and controls associated with the Horizon system*, relevant to the three scope areas highlighted above (see 2.1).
- 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).
- 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 three scope areas highlighted above (see 1.3.4). We identified three core procedure types which were then utilised during Phase 1:
  - 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.
  - 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.
  - 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.

3.2.2 Phase 1 - Testing

Deloitte conducted the following procedures:

- Onsite review and visit to Fujitsu to test controls between May 2016 and September 2016.
- Review of case data provided by POL case handlers and tested for characteristics which could illustrate the Horizon system has not operated as expected.
- Review of relevant technical documentation as 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.

POL00400125

4 Work Performed

4.1 Summary of Work Performed

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) A tabular format of the procedures performed in Phase 0, and the key learnings relevant to our planning.

iii) The procedures which have been performed in Phase 1 as per POL instruction, and the findings obtained from the performance of those procedures.

4.2 Scope Area 1

Scope Area 1: *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.*

4.2.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 2.2.1 and 2.2.2. 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 has, since 2012 been assessed on a regular basis, via Service Auditor Reports (ISAE3402 produced by EY). Further sources of assurance is provided by regular 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.

POL00400125

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 process used depend on the nature of the connectivity issue. Recovery scripts designed by POL are an integral part of this process.

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 should 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 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.

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).

POL00400125

4.2.2 Summary Table of Phase 0 Procedures and Conclusions

POL Instruction	Procedures Performed	What we have discovered
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.

POL00400125

4.2.3 Phase 1 Procedures

Performed Procedures

Procedures	Findings
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 and 6 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: 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.	**Controls** 1a. No issues noted 1b. No issues noted 1c. Issue noted. '*A number of users have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'* 1d. No issues noted 1e. issue noted. *'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*

POL00400125

Procedures	Findings
	automatically been committed by Horizon to provide greater visibility to Post Masters that a recovery session had been initiated.' 2. Issue noted. See Appendix 5 for details of which controls have been subject to change. It was noted one user has access to both development and live environments of HNG-X. Fujitsu stated that; *"Whilst we appreciate that there is lack of segregation of duties here for Gerald between Live and Development, it is felt that there is a strong business need for this access for Gerald. He provides 4th line/final line support for the audit service and is in regular weekly contact with the Security audit team to assist them in resolving queries with the audit service. He is the lead designer/developer and system owner.* *Additionally there are compensating controls in place such as CCTV, and the auditing we have in place (and the technical controls around not being able to change audit items for 7 years) acts as a safeguard against anyone with access trying to change anything in an unauthorised way."* **Data** 3. Review of the case data available (relevant to allegations) for transactions indicating items of risk from a system functionality perspective. The analytical procedures outlined in Appendix 6 were undertaken, and a number of items of interest were noted, see Appendix 6a for details and summary of findings. One finding of note is that 'there were 59 (0.0019%) session ids from a total of 3,074,830 which were out of balance based on the transactional data received. Those 59 session ids out of balance related to 16 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-X in 2010.

POL00400125

Procedures	Findings
	POL investigators have been handed this information for further investigation. In short, whilst various characteristics were noted that could be indicative of risk within the system, further manual investigation will be required by POL's investigators to conclude. This has been discussed with POL management during the course of our work. 4. No issues noted. 1 Balancing Transaction identified (in the period where data was available for review 12/03/2010 – 28/05/2016) which did not relate to a branch involved in the allegations and was appropriately approved and governed. **Substantive** 5a. No issues noted 5b. No issues noted 5c. No issues noted 5d. No issues noted 5e Post Office have the ability to create their own APADC transactions. So they can create a product, and a transaction and then also specify the recovery script which would be initiated when any of the recovery scenarios kick in. This could, theoretically cause an issue where a new product is created, and the recovery script is then coded to do nothing. So if the cashier sold that product for the customer, and then in the event of the connection going down and the recovery process kicking in - no rollbacks or roll-forwards would happen in this case. Our testing has shown no evidence which would suggest this has happened, although we have not specifically performed procedures to verify this.

POL00400125

4.3 Scope Area 2

Scope Area 2: 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.

4.3.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 2.2.1 and 2.2.2 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 (substantive procedures performed support management representation there has been only 1 true Balancing Transaction since 2010).

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 HNG-X system, 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 (record created and stored in audit store). 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 run by limited appropriate personnel.

POL00400125

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 modfy 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).

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 anyattempt 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.

POL00400125

4.3.2 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 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.	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. These controls have been tested at a point in time. 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.

POL00400125

4.3.3 Phase 1 Procedures

Performed Procedures

Procedures	Findings
Controls 1. Validate inherent system controls around Balancing Transactions (See Appendix 3 for detail of controls A – 1). 2. Validate 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 is atomic. 3. Validate Fujitsu support staff cannot amend audit files for Balancing Transactions. 4. Validate Fujitsu support staff only have privileges for only inserting balancing / correcting transactions to relevant tables in the database. Confirm SSC do 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 A – N) 6. Validate 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 any Branch 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 volumes (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.	**Controls** 1. No issues noted 2. No issues noted 3. No issues noted 4. *'Through discussion with Fujitsu management it was noted that the control wording is not accurate. A small number of users are granted extended privileges which enable them to update / delete records. However in mitigation this access is appropriately restricted to authorised users. Users do not have the ability to bypass this role restriction by running SUDO command. User actions are audit logged and not proactively reviewed, and all instances of users being granted the APPSUPP role are also captured in audit logs.'* 5. Issues noted for control 2A and 2C. 2a finding noted – '*Through discussion with Fujitsu management it was noted that the control wording is not accurate. A small number of users are granted extended privileges which enable them to update / delete records. However in mitigation this access is appropriately restricted to authorised users. Users do not have the ability to bypass this role restriction by running SUDO command. User actions are audit logged and not proactively reviewed, and all instances of users being granted the APPSUPP role are also captured in audit logs.'* 2c finding noted – *'The technical document <DESAPPLLD0142> is inaccurate. The user OPS$SUPPORTTOOLUSER does require update access to the table BRDB_BRANCH_INFO, however the document does not reflect this.'* This is a documentation finding only. 6. Issue noted: '*A number of users have access to mechanisms for managing the digital signatures and have database administration*

POL00400125

Procedures	Findings
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 was followed, logically perform as expected. 13. Walkthrough a Transaction Correction being raised by SCC, and the notification / acceptance of it by a branch.	*responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'* 7. No issues noted **Data** 8. Review of the case data available (relevant to allegations) for transactions indicating items of risk from a system functionality perspective. The analytical procedures outlined in Appendix 6 were undertaken, and a number of items of interest were noted, see Appendix 6a for details and summary of findings. One finding of note is that 'there were 59 (0.0019%) session ids from a total of 3,074,830 which were out of balance based on the transactional data received. Those 59 session ids out of balance related to 16 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-X in 2010. POL investigators have been handed this information for further investigation. In short, whilst various characteristics were noted that could be indicative of risk within the system, further manual investigation will be required by POL's investigators to conclude. This has been discussed with POL management during the course of our work. 9. No issues noted. 1 Balancing Transaction identified (in the period where data was available for review 12/03/2010 – 28/05/2016) which did not relate to a branch involved in the allegations and was appropriately approved and governed. **Substantive** 10. No issues noted 11. No issues noted

POL00400125

Procedures	Findings
	12. No issues noted 13. No issues noted

POL00400125

4.4 Scope Area 3

Scope Area 3: 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.

4.4.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 2.2.1 and 2.2.2 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:

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'

i) 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.

ii) 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.

iii) 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

iv) 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.

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

POL00400125

B. Archival from the Branch Database to the Audit Server

i) 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.

ii) 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

i) 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.

ii) 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.

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

iv) 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.

v) 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

i) 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.

ii) 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.

iii) 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

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

ii) 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.

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

POL00400125

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.

POL00400125

4.4.2 Summary Table of Phase 0 Procedures and Conclusions

POL Instruction	Procedures Performed	What we have discovered
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.

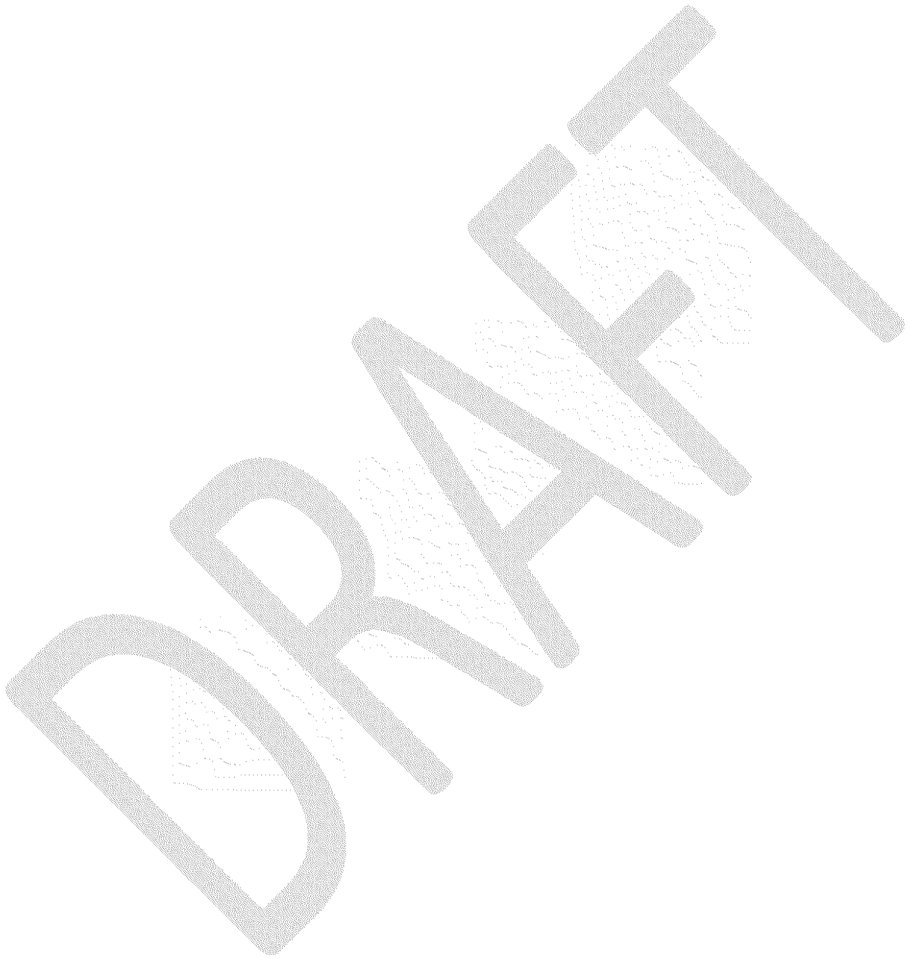
POL00400125

4.4.3 Phase 1 Procedures

Performed Procedures

Procedures	Findings
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 Audit Store has remained broadly consistent over time from a controls perspective for the period relevant to the allegations.	**Controls** 1. No issues noted 2. Issue noted: '*A number of users have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'* 3. No Issues Noted except for control 3A. 3A finding - *'Review of the audit settings for the Audit Server noted that the audit policy change which relates to change of user rights was set to log success events only, with failure not enabled.'* 4. No issues noted **Data** N/A **Substantive** 5. No issues noted 6. See Appendix 5 for details of which controls have been subject to change.

POL00400125



POL00400125

5 Assumptions and Limitations

5.1 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;
7. We have not validated or commented on the quality of the Assurance Work[2] supplied to us.

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.

We have performed work on control in place and operating at the time of the review, and not those operating at the time of the allegations. Other evidence has been obtained, where available, to provide evidence as to whether the control was likely to have operated at the time of the allegations.

[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.

[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.

POL00400125

Appendix 1

Documents Reviewed

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 and 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 and 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
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

POL00400125

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 and Solutions Designer
Gareth Seemungal	Fujitsu - Senior Software and Solutions Designer

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.

POL00400125

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 a correction record must ensure that the auditing of that action performed must be atomic.

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 code where 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.

POL00400125

Ref	Control Description
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 • 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 is enforced 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

POL00400125

Ref	Control Description
	• 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 is completed, 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 $BRDB_SH directory so that access to the script and the associated components can be restricted to authorised users. The shell script calls the PL/SQL package PKG_BRDB_TXN_CORRECTION.
L	PL/SQL package PKG_BRDB_TXN_CORRECTION, which resides within the Branch Database and is owned by Oracle user OPS$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 columnson 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.

POL00400125

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 secured to 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 the imported seal file. Assuming they match, the file is then written to the remote Audit archive. If the seals do not match, the Audit track and 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 Centera and details will be stored in the Audit Track Seal Database via I-ATS-5.
D	Access to the Audit Track files for gathering shall 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 start and 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

POL00400125

Ref	Control Description
	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 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 HNG-X 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.

POL00400125

Appendix 5

Change Control – list of controls and their change dates.

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
1	1a	All transactions on counter must balance to zero.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied in Riposte.
1	1b	All controls of transactions to the branch database are atomically written and committed.	No	-	-	-	No	In Riposte this control is of less importance given each Branch operated its own database. There is no visibility of an reconciliation controls in place between local and central databases in Riposte.
1	1c	A Digital Signature is applied to Message Journal during initiation of transfer to Branch Database.	No	-	-	-	Yes	Digital Signature did not exist in Riposte. However a CRC check was applied, which whilst Fujitsu assert that this is less complex than the digital signature check, and it is noted that this check has not been tested in detail, if operating correctly the check would notify Fujitsu on retrieval of audit data from the audit store if any amendments to data had been made.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
1	1d	Any non-Counter originated interface files (POLSAP or third party sources) must be Transaction Accepted by the Branch.	Yes	R13 and R13.05	Release notes obtained and reviewed. Seen to document various management reviews / approvals and testing steps.	The changes introduced are assumed to be 'Win in Mails'. As part of this initiative an extra file is received from Paystation and used to trigger Track and Trace messages (to Royal Mail). Items on hand are updated reflecting postal items delivered to and from the branch but there is no financial impact on the branch from this. The transactions impacting the financial state of the branch are received in the same file as previously - i.e. via Transaction Acceptance.	N/A - see change to left	N/A - see change to left
1	1e	In the event of connectivity failure there is a transaction recovery process which is initiated.	No	-	-	-	Yes	As each branch operated its own database, transaction recovery processes were of less importance in Riposte.
1	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).	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
1	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.	No	-	-	-	Yes	Source code was reviewed at a point in time. The Digital Signature did not exist in Riposte. However a CRC check was applied, which whilst Fujitsu assert that this is less complex than the digital signature check, and it is noted that this check has not been tested in detail, if operating correctly the check would notify Fujitsu on retrieval of audit data from the audit store if any amendments to data had been made.
1	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.	N/A (this procedure)	N/A (this procedure)	N/A (this procedure)	N/A (this procedure)	N/A (this procedure)	N/A (this procedure)
1	4	Review of population of balancing transactions (to validate population of Balancing Transactions relative to total transaction volumes)	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure
1	-	Review source code on screen at Fujitsu headquarters which supports the key inherent control operation around:	No	-	-	-		Source code was reviewed at a point in time. Please refer to 1.1-1.5.
1	5a	Refer to control 1.1						

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
1	5b	Refer to control 1.2						
1	5c	Refer to control 1.3						
1	5d	Refer to control 1.4						
1	5e	Refer to control 1.5						
2	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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	3	Fujitsu support staff cannot amend audit files for Balancing Transactions.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	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	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		deployed in response to actual loss/bugs in code.)						
2	10	Review source code on screen at Fujitsu headquarters which supports the key inherent control operation around Balancing Transactions.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	6	Validation there is a Segregation of Duties between BRDB Administration and Key Management Software Administration.	No	-	-	-	No	The Digital Signature did not exist in Riposte. However a CRC check was applied, which whilst Fujitsu assert that this is less complex than the digital signature check, and it is noted that this check has not been tested in detail, if operating correctly the check would notify Fujitsu on retrieval of audit data from the audit store if any amendments to data had been made.
2	7	Validate inherent system control around Global Users, that Global users with a Role of ADMIN cannot log onto to any Branch other than Global (Including Remote access controls to branch infrastructure (e.g. Counter)).	No	-	-	-	Yes	Fujitsu represented that no such equivalent role or ability to remote access onto counters existed in Riposte.
2	9	Review a sample of the full population (already extracted by Fujitsu - 7.5 years) of balancing transactions to	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		validate the branch was aware of their usage / no transactional postings were made in the balancing transaction.						
2	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.	No	-	-	-	N/A	Source code reviewed at a point in time.
2	12	Review the 9 Balancing Transaction Templates to validate balancing transactions would, if the template was followed, logically perform as expected.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	13	Walkthrough of a Transaction Correction being raised by SCC, and the notification / acceptance of it by a branch.	Yes	Release 5.5	Release notes obtained and reviewed. Seen to document various management reviews / approvals and testing steps.	The mechanisms for producing TAs changed at Release 5.5 as a result of introducing Client File Delivery.	See Left	See Left

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
2	1a	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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5a	All inserts will be audited in the table BRDB_TXN_CORR_TOOL_JOURNAL.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5b	The PL/SQL package PKG_BRDB_TXN_CORRECTION will be owned by Oracle user "OPS$SUPPORTTOOLUSER".	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5c	The PL/SQL package PKG_BRDB_TXN_CORRECTION will execute with the permissions of the OPS$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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
2	5d	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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5e	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:	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2		<transaction_file_name>_<CCYYMMDDHHMISS>.log						

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
2		Access to these 2 directories is appropriately restricted.						
2	1b	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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5f	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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5g	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 code where 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.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

2	5i	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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
2	1c	Any writes by the SSC to BRDB must be audited. The mechanism for inserting a correction 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.	No	-	-	-	No	As each branch operated its own database, BRDB did not exist in Riposte.
2	5j	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 is completed, an Operational exception should be raised to indicate the count of missing sequence numbers. Duplicate records	No	-	-	-	No	JSN check in its current format did not exist in Riposte. However Fujitsu assert that a data density check was applied.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		are not possible due to the primary key on this table.						
2	5k	Unix shell script BRDBX015.sh which is in the /app/brdb/trans/support/brdbx015 directory. It is deliberately kept separate from the standard $BRDB_SH directory so that access to the script and the associated components can be restricted to authorised users. The shell script calls the PL/SQL package PKG_BRDB_TXN_CORRECTION.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5l	PL/SQL package PKG_BRDB_TXN_CORRECTION, which resides within the Branch Database and is owned by Oracle user OPS$SUPPORTTOOLUSER. The PL/SQL package is the component that validates, creates and audits the balancing transaction.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2	5m	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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		BRDB_OPERATIONAL_EXCEPTIONS.						
2	5n	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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		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						

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		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.						
2	5o	Balancing transaction audit files (BRDBC033), unlike the files produced by BRDBC002, are not compressed, but are still encrypted.	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
2	5h	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 • 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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		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 …'.						

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		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						

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		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 is enforced for that field. Note that if the parameter does not exist, then no values are enforced in the SQL.						

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
2	7	Validate inherent system controls around Global Users, notably that Global users with a Role of ADMIN cannot log onto to any Branch other than Global (Including Remote access controls to branch infrastructure (e.g. Counter)).	No	-	-	-	Yes	Fujitsu represented that no such equivalent role or ability to remote access onto counters existed in Riposte.
3	1a	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 secured to 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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	2	Digital Signature controls applied to Message Journal during initiation of transfer to Branch Database.	No	-	-	-	Yes	Digital Signature did not exist in Riposte. However a CRC check was applied, which whilst Fujitsu assert that this is less complex than the digital signature check, and it is noted that this check has not been tested in detail, if operating correctly the check would notify Fujitsu on retrieval of audit data from the audit store

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
								if any amendments to data had been made.
3	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	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.	No	-	-	-	Yes	Source code reviewed at a point in time. Digital signature check in its current form originated in HNG-X
3	6	Identification of changes relevant to the Audit Store from review of historical documentation, and validation that the Audit Store has remained broadly consistent over time from a controls perspective for the period relevant to the allegations.	Yes	R10.20 (Refresh of Eternis Storage infrastructure)	Release notes obtained and reviewed. Seen to document various management reviews / approvals and testing steps.	Agree that the system changed to the extent that it is now implemented on different hardware. A crucial point is that the audit data was not changed and the digital signatures created in the branches at the time that transactions were carried out were persisted and	N/A - see change to left	N/A - see change to left

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
						demonstrate that the data in the audit trail has not been tampered with.		
3	1b	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 the imported seal file. Assuming they match, the file is then written to the remote Audit archive. If the seals do not match, the Audit track and seal file are moved to a holding area and an event is raised. Manual investigation is necessary to investigate the cause of the discrepancy.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1c	There will be a single instance of the ATS that concurrently accepts files for sealing/seal checking from ATG and ATR and notifies	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
		sealed files to the ATD and into the Sealer Database for subsequent use by the Audit Track Extractor.						Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3		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.						
3		Once a file has had a seal calculated the file will be written to Centera and details will be stored in the Audit Track Seal Database via I-ATS-5.						
3	1d	Access to the Audit Track files for gathering shall 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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3	1e	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	3a	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	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3	1f	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1g	All Audit Server and Audit Workstation and Centera hardware shall be held in physically secure areas where physical access to the systems is controlled.	Yes	R10.10 and R10.20 (Refresh of Eternis Storage infrastructure)	Release notes obtained and reviewed. Seen to document various management reviews / approvals and testing steps.	Agree that the system changed to the extent that it is now implemented on different hardware. Operational processes were not changed.	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1h	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. The Fujitsu Services Audit Staff role shall not have any write, modify or delete access to the Audit Archive.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3	1i		No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	3b	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	3c	POL staff will not be given direct access to the Audit Workstation to safeguard other parts of the HNG-X system. Instead nominated Fujitsu Services personnel will supply audit information as requested by Post Office.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1j	The following integrity checks will be applied to the data:					-	-
3		• Completeness of data – contiguous message sequence numbers	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3		• Integrity of individual messages					No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3		o For Riposte data the message CRC should be checked					No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3		o For HNG-X data the message signature will be verified					Yes	For Riposte CRC control above was in place.
3		Separate Riposte and HNG-X summaries of the results of the integrity checks are generated. They should detail:					No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3		• Summary of the message sequence runs broken down by counter Id. This should include start and end date/times and start and end message sequence numbers. Any gaps in the message sequence runs must be highlighted.					No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3		• Summary of messages that have failed individual message integrity checks					No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3		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.					No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1k	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3	1l	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 named AUDIT_USER will be created with the rights required to utilise the workstation applications. Authorised users will be added to this group.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	3d	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1m	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Scope Area	Control Ref.	Control/Procedure description	Evidence reviewed indicates control has changed since HNG-X (2010)?	Details of the change (Inc. change reference)	Appropriately approved and tested?	Fujitsu assertion on whether control has changed since HNG-X	Pre HNG-X change to Fujitsu / Deloitte knowledge?	If Yes - detail of process in place before change
3	1n	Audit workstations and Atalla NSPs are located in secure areas. Only authorised users are given physical access to these areas.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3	1o	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.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.
3		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						
3	3e	Baskets are stored for a defined period of time. The configuration of this parameter and the audit trail around changes to it need to inspected in order to provide assurance over the maintenance time period for audit purposes.	No	-	-	-	No	Whilst it has not been corroborated by review of technical documentation / testing it is expected this control applied pre HNG-X. Fujitsu attested that controls surrounding the audit store have remained largely unchanged.

POL00400125

Appendix 6

Case Data Analytics Overview

The below analytical procedures were performed on 'Case Data'. 'Case data' refers to transactional data provided by POL, which had been extracted by Fujitsu from the audit store, and relates specifically to the branches involved in the 'allegations'. The data extracted is in 1 month periods relating specifically to the period of the allegations for each specific branch.

Scope Area	POL Instruction	Proposal	Relevant Analytics Procedures	Analytic
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.	Review case data for transactions indicating items of risk from a system functionality perspective (e.g. recovery transactions are present in the case data).	1, 2, 3, 4, 4a, 5, 6, 6a, 7

Tab Index	Description
Analytic 1	Identify gaps in audit log sequencing
Analytic 2	Identify gaps in transaction times during working hours
Analytic 3	Identify two user logon events in sequence without the expected logoff event in between; an indicator of a connectivity issue
Analytic 4	Identify recovery transactions
Analytic 4a	Identify recovery transactions that indicate a connectivity issue
Analytic 5	Count of zero valued transactions summarised by product
Analytic 6	Identify branches which are out of balance based on transactional data available (should not be possible based on inherent system controls).
Analytic 6 Group and Session id	Identify branches which are out of balance based on transactional data available (should not be possible based on inherent system controls).
Analytic 7	Identify transactions posted by non-branch users without subsequent branch acknowledgement.

POL00400125

Appendix 6a

Case Data Summary Findings

POL investigators have been handed this information for further investigation. In short, whilst various characteristics werenoted that could be indicative of risk within the system, further manual investigation will be required by POL's investigators to conclude. This has been discussed with POL management during the course of our work.

Procedure	Comments	Summary
Analytic 1: Identify gaps in audit log sequencing	In order to identify gaps in audit log sequencing, the transactions data was sorted into ascending order on session id and txn id, and any gaps in the sequence at both the session and txn level were identified.	There were 212,372 (1.60%) gaps in audit log sequencing from a total of 13,307,999 transactions
Analytic 2: Identify gaps in transaction times during working hours	In order to identify gaps in transaction times during working hours, the transaction data was ordered by branch, date and time. Gaps that were significantly higher than the average gaps in transaction times were identified, only transactions with the same date were compared. Transactions with a stock unit of ATM, LOT, OOH or BUR were excluded.	There were 46,528 (0.35%) gaps in transaction times that were more than 20 times higher than the average transaction gap of all stores with the same number of positions from a total of 13,307,999 transactions
Analytic 3 : Identify two user logon events in sequence without the expected logoff event in between, an indicator of a connectivity issue	In order to identify two user logon events in sequence without the expected logoff event in between, an indicator of a connectivity issue the events data was ordered by date and time and logon events (event code 12 or "EPOSSTransaction.Ti of Logon Completed") not followed directly by a log off event (event code 13, 27 and 102 or "EPOSSTransaction.Ti of Logoff Completed") were identified.	There were a total of 1,064 (0.93%) logon events in sequence without the expected logoff between; from a total of 114,491 log on/off events.
Analytic 4: Identify recovery transactions	In order to identify recovery transactions the eventDetailMsg column of the Events data was searched for words like 'successfully recovered' but not like 'No recovery required.'	There were 30 (0.00057%) recovery transactions identified from a total of 5,289,369 transactions in the events data
Analytic 4a: Identify recovery transactions that indicate a connectivity issue	In order to identify connectivity issues of none recovery transactions the eventDetailMsg column of the Events data was searched for words like 'could not recover' and 'No recovery required.'	There were 258 'no recovery' transactions that indicate a connectivity issue from a total of 5,289,369 transactions in the events data
Analytic 5: Identify zero valued transactions	In order to Identify zero valued transactions, all transactions with a sale value of 0, a quantity not equal to zero and a mode of either 1 or SC for 'Serve	There was a total 1,314,761 (9.88%) zero valued transactions with a quantity not equal to zero from a total of

POL00400125

Procedure	Comments	Summary
	Customer' were identified and a summary per item is produced.	13,307,999. These transactions were against a total of 814 products
Analytic 6: Identify branches which are out of balance based on transactional data available (should not be possible based on inherent system controls).	In order to identify branches which were out of balance based on transactional data available (which should not be possible based on inherent system controls), the transactions data was summarised by branch (Group) and session id and those session ids that do not sum to zero were identified, and are ordered by balance descending.	There were 59 (0.0019%) session ids from a total of 3,074,830 which were out of balance based on the transactional data received. Those 59 session ids out of balance related to 16 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-x in 2010.
Analytic 7: Identify transactions posted by non-branch users without subsequent branch acknowledgement.	In order to identify transactions posted by non-branch users without subsequent branch acknowledgement, any users whose id did not take the usual format (6 digits - 1st letter of forename followed by 1st and 2nd letters of surname and numeric 001) were identified. A user id of *PS98 are Paystation transactions and were ignored here, a user id beginning with a * are identified as global users	There were 17 (3.03%) users (*DSI02, *JBA03, *TAK01, *PJO07, *BMA01, *JCA01, *RCR01, *DCU02, *JHO05, *RLY01, *DWA01, *MWE01, *STU03, *GDR01, *NST01, *PJO02 and *GMU01) from a total of 561 users classified as non-branch users who posted transactions

POL00400125

Appendix 7

Clarification questions

The below clarification questions and associated answers attempt to provide clarity on queries arising from the content of this report.

Key questions

1. From the perspective of the Group Action, we are trying to understand:
    a) Whether Fujitsu can edit or delete transactions recorded by branches in a way that could impact on the branch's overall accounting position?

    Yes – Transactions can be deleted at database layer (BRDB) by DBA's.

    Before audit store access locked down, transactions could be deleted at audit store level (and still can be once a transaction has been in the audit store for 7 years), but this would not affect a branches overall accounting position unless there was a query that resulted in the extraction of data. If data was extracted from the audit store and records had been tampered with or removed, this would be flagged upon extraction by the process to report on data integrity, so it would be transparent that the data has been edited. It should be noted the warning that the data integrity check failed can be ignored by the operator.

    b) How difficult it would be to do (a)?

    Access to do (a) is restricted to appropriate personnel by Fujitsu. For users who have DBA access on the BRDB, this could be done.

    However if the edit/delete of the transaction was not done before the data had been 'collected' by the Audit Server (typically every 15 minutes), then this would not affect the record of data in the Audit Store. The audit store is the location where data is retrieved from in the event of a dispute.

    Further if the edit/delete of the transaction was performed prior to the data being 'collected' by the Audit Server, whilst it would be reflected in the audit store data, upon retrieval of branch data from the audit store, if a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data.

    c) Whether (a) is possible without leaving a "footprint" that is visible to either (i) postmaster or (ii) Post Office / FJ.

    i) Amendment / deletion of transactions would not be overtly notified to the Postmaster, however if the amendment / deletion happened at the BRDB, this would affect the declarations made by Postmasters (encouraged to do so on a daily basis) and also declarations are required to be done in order to rollover into the next accounting period (typically 4-5 weeks). The monthly Branch Trading Statement which a Postmaster must sign off on in order to roll into the next accounting period would also be impacted by a change of this nature which would capture summarised totals of transactional data, which could be reconciled by branch back to the granular transaction log reports. All of the mentioned reports are mechanisms by which the Postmaster would be made aware of any such changes.

    Amendment / deletion of data in the audit store has no effect on branch accounting and would only impact a branch (Postmaster be made aware) if data was retrieved from the audit store. Further if upon retrieval of branch data from the audit store a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data.

    ii) Branch Database privileged Oracle user operations are audited by Oracle to the SYS.AUD$ table. This table is extracted into audit files every night by a batch job into a directory from which the audit archiving system extracts the data. The audit data is currently stored for 10 years. This table can be extracted from the Audit Store by Fujitsu.

POL00400125

Any amendment / deletion of data in the audit store would be visible to Fujitsu only when data is retrieved. Upon retrieval of branch data from the audit store a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data.

As per the exception noted on page 3, there is a small theoretical risk of a user 'spoofing' the digital signature, arising from a failure in SOD controls relating to the digital signature.

d) Whether (a) has ever actually happened?

Audit logs of super-user access in the BRDB exist. Fujitsu have confirmed where amendment / deletion of live database tables would be identifiable from this log.

Our work has not included obtaining logs for the relevant time period and performing analytics over them to identify any instances where this has happened, and investigate if so. Such procedures should be theoretically possible however.

2. The key points we need to understand are whether (i) Balancing Transactions and (ii) changes by Super-users can effect branch accounts from the perspective of the postmaster, in particular:

a) Are these changes visible to the postmaster?

There is no system setting which would flag to the Postmaster when a change had been made by a super user.

The Transaction Log report gives the Postmaster a way of identifying Balancing Transactions, as transactions that have been inserted can be identified as the associated user would be displayed as "SUPPORTTOOLUSER99" (i.e. not a member of staff at the Branch)

b) Can these generate a shortfall in the branch accounts?

If used in a certain way, BTs or a super-user change could theoretically cause a shortfall in branch accounts.

c) How would this impact on the making of daily cash declarations?

Daily cash declarations are a real time report generated by a branch (counter) which queries the BRDB live database; therefore any balancing transaction inserted into the BRDB or change of transactional BRDB data by a super user, would automatically impact the daily cash rec report (impact dependent on nature of BT / change).

d) How would this impact on "monthly" branch trading balances?

The monthly Branch Trading Statement, which a Postmaster must sign off on in order to roll into the next accounting period would also be impacted by a change of this nature.

The monthly branch trading statement, reports on data live from the BRDB, and aggregated data from the BRDB, therefore any balancing transaction inserted into the BRDB or change of transactional BRDB data by a super user, would automatically impact the daily cash rec report (impact dependent on nature of BT / change).

Specific questions on the Interim Report

3. Diagram on Page 8:

a) Transfer of data from BAL to BRDB - Does this happen daily? If so when during the day? Is it overnight?

BAL is a compilation of servers used for the transfer of data from Counter to BRDB, this processing is done in a near real time manner. As such transfer of data from BAL to BRDB is instantaneous once a basket is complete.

i) Given the daily polling of data from which source does the Counter pull data when the postmaster conducts an end of day cash declaration? (The above suggests the data must be pulled from BAL as all other sources would not be up to date in real time?)

POL00400125

BRDB. A request from counter is raised (via the BAL) to BRDB using pre-defined SQL scripts at the BRDB layer to generate this cash declaration report/process. When a cash declaration is raised by a branch a message transfer is sent via the BAL which communicates with the BRDB to query the live transaction tables using a pre-defined SQL script

b) Transaction corrections generated by POL: Where does a Transaction Correction fit on this diagram?

Transaction Corrections are inserted directly into BRDB by a defined data transfer process.

c) The diagram suggests that data is held in the Audit Server for 5 days but para (iii)(b) on page 14 suggests that data is held in the BRDB for 5 days? Are both statements correct or is one a typo?

Most data is held in BRDB for approximately 5 days, (depending on specific type of data). Certain values are also aggregated and the aggregated data held for up to 60 days to allow for real time reports, and the monthly branch trading statement, ran by the counter to include this data if required.

Most data is held on the Audit Server for approximately 5 days, (depending on specific type of data).

4. Page 10:

a) Point F – says POL finance staff can "*input / amend*" a transaction – We know they can input a transaction but can they "amend" a transaction? If so, how?

This refers to a Transaction Correction (TC). A TC could, depending on the detail of the TC, have the effect of 'amending' an existing transaction. A TC must be accepted at the counter before impacting branch accounting.

5. Page 19:

a) What is meant by the phrase "*predominantly limited to HNG-X due to previous Audit Store retention limitations*"?

Wording removed to avoid ambiguity.

b) What is meant by the phrase: "*Any writes by Fujitsu Support to BRDB must be audited*"?

Branch Database privileged Oracle user operations (Fujitsu Support) are audited by Oracle to the SYS.AUD$ table.

c) At point "iv" – what is the difference between "Correcting" and "updating"? We did not think FJ could "correct", only "insert"? [This point also comes up at Page 13, 1st column of table].

A BT could, depending on the detail of the BT, have the effect of 'amending' an existing transaction. A BT can only insert, and not update or delete existing records. The possibility of a superuser amending existing transactions does exist as highlighted above in question 1.

6. BTs in relation to the SU issue:

a) Please can you explain the situation with using Balancing Transactions to solve the SU problem?

The usage of the BT tool for this purpose is not a 'true' BT as no data (transactions) is/are injected into the database. However the same tool which allows a BT to be posted, is used to perform this procedure.

The procedure is performed to update the transaction recovery table of a Stock Unit (SU) in the rare instance when the recovery flag for a transaction gets into an inconsistent state, and needs to be manually updated, to show that the transaction has been recovered by the branch.

This procedure is managed by an MSC (change request) process prior to the updates taking place.

b) Other than the one use of a BT to solve a bug, are you sure that all other uses of BTs relate to the SU issue?

For the period data was available for and therefore reviewed (12/03/2010 – 28/05/2016).

All other uses of the tool in this period updated the specific table BRDB_RX_RECOVERY_TRANSACTIONS' (SU issue) and did not contain INSERT statements.

c) Will the branch be aware of the SU issue?

POL00400125

The Branch would not be notified of the tool being used for this purpose, however this process is generally initiated by the branch when the branch is struggling to perform this task manually using the counter.

d) Can the SU issue ever cause a discrepancy in the branch accounts?

The usage of the tool to update the transaction recovery table of an SU does not insert / remove / amend transactions.

7. BT audit files:

a) What do the "*audit files*" in relation to BTs track and show?

All usages of the tool used for inserting BTs. The logs show the actual SQL commands used to insert the BT, and contain all fields updated and their respective values (quantities and product ids). There are also user timestamps which identify the user who inserted the BT.

b) How far back do the audit files go?

The audit files commence at 12/03/2010

8. FJ access to conduct a BT

a) How many staff at FJ have permission to inject a BT?

31 (of these 31, 26 also have direct access to the live BRDB database and therefore could theoretically make changes to transaction tables as described in (10b) below.

b) What is the process followed by FJ for using a BT?

The process followed by FJ is:

An error is recognised by the branch and they raise a request/call to SSC.

A TFS/Peak Incident service desk tool is then used to record incidents raised by Post masters (TFS has subsequently been retired and incidents all 1st and 2nd line branch incidents are now recorded in Peak Incident Management).

This issue will then be investigated by SSC. If a BT is required then this is passed to Fujitsu for further work and solution management.

If a BT is required this is recorded on the Peak Incident ticket.

Approvals are then sought by senior members of POL before this is executed which is captured within the ticket request.

c) What operational controls are there around the use of BTs at FJ?

A branch would initiate the process described in (b) above for a BT to be executed.

Senior approvals are required by POL before this process can be completed.

Use of BT tool is audited and any transactions inserted would be recognised by branch through transactional log reports.

The BT tool is restricted to a limited number of Fujitsu personnel who are independent to the Peak incident process.

d) What is the process followed at POL for implanting / authorising a BT (if this is out of scope, please say and we will pick up direct with POL)?

Out of scope. Agreed POL will answer.

9. BT visibility

a) Would a BT shows in the branch accounts from a postmaster's perspective?

i) What report would a postmaster need to run?

POL00400125

A Postmaster is not notified if a Balancing Transaction is inserted into the live transaction tables.

There are various real time reports a Postmaster can run which would be affected by something of this nature (notably the Transaction Log report, which is able to display transactions that have been posted over the last 60 days.). Transactions in this report would be identifiable by the user code "SUPPORTTOOLUSER99" (i.e. not a member of staff at the Branch).

Further any Balancing Transaction impacting a branch's transactional data would impact declarations made by Postmasters (encouraged to do so on a daily basis) and also declarations are required to be done in order to rollover into the next accounting period (typically 4-5 weeks). The monthly Branch Trading Statement which a Postmaster must sign off on in order to roll into the next accounting period would also be impacted by a change of this nature which would capture summarised totals of transactional data, which could be reconciled by branch back to the granular transaction log reports. All of the mentioned reports are mechanisms by which the Postmaster would be made aware of a Balancing Transaction. The reporting functionality of counters was described by Fujitsu and this understanding was corroborated by review of technical documentation, no walkthroughs were performed of this process.

ii) How would it be identifiable from other transactions?

Transactions in the Transaction Log report would be identifiable by the user code "SUPPORTTOOLUSER99" (i.e. not a member of staff at the Branch).

b) Can a BT by back-dated (i.e. injected into the branch accounts at an historic date)?

Whether the Balancing Transaction would be successful or not is not known by Fujitsu as it has never been attempted.

POL and Deloitte are awaiting Fujitsu to provide an estimated cost / time for this walkthrough to be performed (Cost and time required made up primarily from creating a suitably isolated test environment in order to perform the walkthrough in).

Fujitsu have stated *'the answer has to be yes in the sense that if the fix involves inserting a record with an associated date then the date would be chosen as part of the design to fix the problem. The choice of date would have to be made carefully as transactions will only be harvested from the Branch Database for processing by back-end systems if it meets the correct selection criteria – hence the need to test any proposed fix. . The issue is simply that we would have to invent a scenario from scratch and then check that out. I don't see that such an exercise would add value given that we have already carried out a walkthrough of the tool.'*

c) Were BTs (or something similar) possible in Old Horizon? [See attached note from FJ]

Fujitsu have advised they have attempted to make contact to retired staff on the matter but are unable to provide a definitive answer on processes in place pre HNG-X relating to Balancing Transactions, only that the transaction correction tool used to inject BTs that has been used since HNG-X implementation in 2010, was not used.

i) What controls were there around these?

Due to the response on the prevous question from Fujitsu we cannot comment on these controls.

ii) Were they logged?

Due to the response on the prevous question from Fujitsu we cannot comment on these controls.

POL00400125

10. Super-users

a) Can Super-users only access the BRDB or can they access other servers (ie. audit server, audit store)?

Super-users could theoretically access data at any other point in the flow of data from Counter – Audit Store. This flow of data has been mapped by Deloitte and access rights at each point tested.

i) In Deloitte's Board Briefing Paper dated 4 June 2014, on page 2, it notes: *"It is possible for Fujitsu staff with suitably authorised privileged access to delete data from the Audit Store."* Has this issues been addressed / will it be addressed?

Yes, once data is in the audit store it cannot be amended / deleted for 7 years, as described in (1a) above.

ii) Would deleting data from the audit store have any effect on branch accounting?

No, unless data was retrieved from the audit store which would only happen in the case of a query being raised / investigation. It would only impact usage of this historical data for any purposes when subsequently extracted from the audit store.

All postmaster reporting functionality is generated from the live BRDB transactional tables (and tables which aggregate this data and store it for up to 60 days). Any amendment / deletion of data in the audit store therefore has no effect on branch accounting and would only impact a branch if data was retrieved from the audit store. Further if upon retrieval of branch data from the audit store a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data. As per the exception noted on page 3, there is a small theoretical risk of a user 'spoofing' the digital signature, arising from a failure in SOD controls relating to the digital signature.

b) If a Super-user edits data in the BRDB, how might this affect the branch accounts from the perspective of the postmaster?

i) Where does the edited data flow to?

The edited data would remain in the BRDB transactional tables assuming that it was entered in the correct logic.

The data in this table would then follow the normal data flow processes (i.e. BRDB > audit server > audit store, BRDB > POLSAP, BRDB > Counter reporting etc.) if this transaction had not already been picked up by the mechanisms which transfer transactional tables downstream (eg. Audit track gatherer which runs every 15 minutes.)

ii) Could the edited data cause a loss in a branch's accounts?

Yes, from a branch reporting perspective any change to data in the BRDB would affect the real time reports ran on the counter, which are used for branch accounting, specifically the monthly Branch Trading Statement which a Postmaster must sign off on in order to roll into the next accounting period.

However if a branches data was retrieved from the audit store, any amendment to transactional data would cause the 'digital signature' integrity check to fail, and Fujitsu would be notified of this failure upon retrieval of the audit data. As per the exception noted on page 3, there is a small theoretical risk of a user 'spoofing' the digital signature, arising from a failure in SOD controls relating to the digital signature.

iii) Will the edited data be visible to the postmaster?

A Postmaster is not specifically notified if a change had been made by a 'super-user'.

Any changes to transactional data would impact declarations made by Postmasters (encouraged to do so on a daily basis) and also declarations are required to be done in order to rollover into the next accounting period (typically 4-5 weeks). The monthly Branch Trading Statement which a Postmaster must sign off on in order to roll into the next accounting period would also be impacted by a change of this nature which would capture summarised totals of transactional data, which could be reconciled by branch back to the granular transaction log reports. All of the mentioned reports are mechanisms by which the Postmaster would be made aware of any such changes.

iv) Would the edited data be visible to POL / FJ?

POL00400125

Yes, as the data amendments would impact transactional records in the BRDB, and subsequently this data would flow through to the audit store. POL / FJ would be able to identify this through review of audit logs as described in 1C above.

POL00400125

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented.

Deloitte LLP
London
October 2016

Other than as stated below, this document is confidential and prepared solely for your information and that of other beneficiaries of our advice listed in our engagement letter. Therefore you should not, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or otherdocument, or make them available or communicate them to any other party. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). In any event, no other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom member firm of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see **www.deloitte.co.uk/about** for a detailed description of the legal structure of DTTL and its member firms.

Member of Deloitte Touche Tohmatsu Limited