POL00029097

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

15X DecNovember 2017



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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Contents

Commented [A1]: To be updated on stable version.

1	Executive Summary	2
2	Management Summary	11
3	Background	2928
3	Scope and Approach	32
4	Work Performed	38
5	General Assumptions and Limitations	7979
Appendix 1		8080
Appendix 2		8383
Appendix 3		8484
Appendix 3a		8585
Appendix 4		8888
Appendix 4a		9090
Appendix 5		9191
Appendix 6		122122
Appendix 6a		124124
Appendix 7		128127
Appendix 8		136135
Statement of Responsibility		152143

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

1. Executive Summary

1.1 Horizon Online Core Summary

1.1.1 In assessing the Horizon Online system, our work has focused on a broad suite of controls which, in collaboration, work to assure the integrity of transactional data is maintained from branch to audit store. The controls respond to the fundamental risks of data integrity which are:

1.1.1.1 *Completeness* – All data is transmitted from source to destination in its entirety.

1.1.1.2 *Accuracy* – Data is accurately transmitted from source to destination without change.

1.1.1.3 *Validity* – The data is valid and has not been doctored or changed such that it is no longer representative of the information the original data was recorded to capture, or has been created spuriously and not linked to a real life data generating event.

1.1.2 The system controls across the areas of the Horizon Online system we have examined are robust at the point our work was conducted with minimal exceptions noted from our testing. They are appropriate to a system the size and scale of Horizon, and the distributed EPOS (electronic point of sale) function it performs; have been designed to meet a high standard of control; and have been assessed similarly in the reports of other independent assurance organisations such as Ernst and Young (Service Auditor Report), although not specifically in the context of responding to these allegations.

1.1.3 We have focused on the core data flow within Horizon Online, from the Counter in branch to the Audit Store where case data is extracted from because it is this data flow which leads to the initial capture of case relevant data, and its subsequent long term storage prior to its download to allow investigation in response to the legal cases. This data flow is subject to industry standard cryptographic controls. These controls are automated, inherent system controls, which are applied by the system to each and every transaction processed by the Counter. As such they represent the most reliable control type possible over data integrity – they are hardcoded into the system, and no manual intervention is required for them to operate; as a consequence of being inherent to the technology they have been in operation throughout the life of Horizon Online

1.1.4 Working together, the Digital Signature (1.3.3.1 (d)), and JSN (1.3.3.1 (c)) controls respond to the fundamental data integrity risks of Completeness, Accuracy and Validity, and make it extremely unlikely that the record of transactions contained within the Audit Store is not representative of the transactions input by staff in branch. Whilst it is possible (as with all large scale computer systems), that glitches and coding errors in the system have resulted in errors in the recording of transactions to occur, the probability of such errors occurring in a manner which has adversely affected certain branches materially, whilst causing other branches to suffer no errors at all/minimal issues, would, based on the controls in place, in our view be remote. The testing we have performed over these controls was designed and executed to assess their operation, in responding to these fundamental risks. Noting the assumptions and limitations detailed in section 1.5, this testing has not resulted in any matters being identified that would call into question the integrity of the core data flow within Horizon Online from the Counter in branch to the Audit Store.

1.1.5 An exception in the cryptographic controls (1.4.2.10) which would theoretically allow a malicious actor to undermine them and potentially change data has been identified. However, it is limited to a third party (Fujitsu), and would be technically very challenging to achieve. It would require significant motivation fFor one of the limited set of Fujitsu staff members to exploit this vulnerability~~(for whom personal gain would almost certainlikely require collusion with Post Office staff or Postmasters) would require a significant motivation~~ given the technical challenges and risks of tripping monitoring controls and, although, ~~Further it is not understood how they would benefit personally without collusion occurring as~~ we have not performed procedures in this area, it would almost certainly require collusion with Post Office staff or Postmasters. Although our investigations have not been exhaustive, they have been extensive, and we have seen no evidence of malicious misuse of the system.

Commented [A2]: Please remind me why we can't go further than likely

MAMW: I've strengthened the wording pending approval from Andy.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

1.2 The Allegations

1.2.1 Post Office/their advisors have informed us that the Claimants in the Group Litigation have asserted that Post Office / Fujitsu has the ability to add / delete / change transactions recorded by branches without the consent / knowledge of a Postmaster and that this may have been the cause of discrepancies in some of the Claimants' branch accounts. We understand that the allegation has been formulated in several different ways:-

1.2.1.1 Post Office / Fujitsu have the ability to log on remotely to a Horizon terminal in a branch so to conduct transactions.

1.2.1.2 Post Office / Fujitsu have the ability to conduct transactions (either remotely or locally) under another user's ID.

1.2.1.3 Post Office / Fujitsu have the ability to insert transactions into a branch's accounts without either a Postmaster's (a) knowledge or (b) consent.

1.2.1.4 Post Office / Fujitsu have the ability to amend or delete transactions entered by branch staff on Horizon (and can do so in a way that is hidden from Postmasters).

1.2.2 More generally, we are informed that the Claimants also allege that Horizon makes errors in accurately recording the transactions input by Postmasters.

1.2.3 The Claimants we have been told, also make a variety of other allegations, principally relating to Horizon providing a poor user experience or having insufficient safeguards against user error. These allegations are beyond our scope of work.

1.3 Overview of Horizon and Our Approach

1.3.1 Horizon is the core operational and Electronic Point of Sales platform for the Post Office network. Although the system has been in use for over 15 years, it is important to note that in 2010 there was a migration from the system commonly referred to as "Legacy Horizon" to the online variant that is operated today ("HNG-X" or "Horizon Online"). We have been informed by Fujitsu that the key difference between the two variants is the way in which data is stored; local versus central. Below is an overview of Horizon Online.

1.3.2 A diagram showing the high level flow of data from transaction origination through to the Audit Store is set out in the 'Background' section 3 below. In summary:-

1.3.2.1 Transactions conducted on Horizon terminals in branches are bundled into virtual baskets (i.e. one basket of transactions per customer) and securely transferred over the internet to the Branch Database (**BRDB**). The BRDB is hosted on a central server farm operated by Fujitsu (there is more than one BRDB server for resilience, and a set of gateway servers collectively termed the Branch Access Layer (BAL) are also used).

1.3.2.2 Camelot, Paystation, and Post & Go transactions are conducted on their own separate terminals (hence they are often referred to as "**Non-Counter transactions**") and accepted into the BRDB by way of Transaction Acknowledgments (**TAs**) on a daily basis.

1.3.2.3 The BRDB holds the live version of the transaction data used in day to day operations. Fujitsu also hosts other centralised data services to support reporting activities which are drawn from summarised data on BRDB

1.3.2.4 From the BRDB, transaction data is fed into various other Post Office systems that then connect to various third party systems.

1.3.2.5 The transaction records in the BRDB are also transferred to the Audit Store via the Audit Server. The Audit Store is not involved in the live operation of a branch or Post Office's business. It is the long term repository of transaction data. In the event of a challenge to the integrity of any transaction data, the Audit Store is considered to be the master record. In usual circumstances, it holds that data for 7 years but this has been extended to 10 years owing to the Group Litigation, and this is now reviewed on an annual basis.

1.3.3 There are a number controls in place to protect the integrity of transaction data within Horizon (i.e. from branch terminal to Audit Store):-

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

1.3.3.1 Counter transactions:-

(a) must balance to zero (e.g. the value of payment taken or given by the branch equals the value of goods and services provided);

(b) are atomically written (i.e. entirely or not at all) to the BRDB so that there can be no partial transactions; and

(c) are each given a unique Journal Sequence Number (JSN) of 1 greater than the previous transaction so that the completeness (density) of the flow of transactions from a particular branch can be checked when data is extracted from the Audit Store.

(d) are signed by a digital signature, which in accordance with commonly adopted cryptography techniques, is used to secure the integrity of transactional data once it has been initiated at the counter and allows all transactions to be checked for subsequent interference once they have left the counter.

1.3.3.2 Non-Counter transactions:-

(a) must be accepted into the BRDB by branch staff by way of a TA in order to affect the branch accounts. Branch staff can obtain reports from the Camelot, Paystation and Post & Go terminals and compare those reports to the TAs that they are asked to accept; and

(b) are digitally signed and subject to JSN fingerprinting by the Counter after being accepted and those digitally signed files can be compared against raw data files that are interfaced into the Audit Store in order to verify completeness when data is extracted from the Audit Store (i.e. once they have been accepted by the Postmaster non-counter transactions are subject to the same data integrity controls as counter transactions).

1.3.4 Due to the nature of the allegations and the investigations that they have necessitated, we have carried out work in phases and, within each phase, scope areas. The main body of this report contains a summary of the work that we have been asked to do, and then designed, in each phase and scope area and that shows how the overall project has expanded and developed. However, the purpose of this Executive Summary is to outline our overall findings and apply them to the allegations set out in section 1 above. We also provide a summary of the procedures performed and the findings of each stage of the work.

1.3.5 In broad terms, we have performed five methods of investigation:-

1.3.5.1 reviewing Horizon technical documentation provided by Fujitsu;

1.3.5.2 asking questions of key Fujitsu staff;

1.3.5.3 reviewing transaction and event data generated by Horizon;

1.3.5.4 testing controls, such as walking through some of the Horizon processes on screen with Fujitsu; and

1.3.5.5 analysis of Horizon's source code.

1.4 Our Findings

1.4.1 As the way data was handled by Horizon changed materially in 2010 with the introduction of Horizon Online, legacy Horizon and Horizon Online need to be addressed separately.

1.4.2 Horizon Online

1.4.2.1 When branch staff lookup transaction records, the terminal in branch contacts the BRDB to retrieve the necessary information. Given that branch accounts (as seen and operated in branch by Postmasters) draw on data from the BRDB, additions, edits or deletions in the BRDB could impact upon branch accounts.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

1.4.2.2 The integrity of transaction data (as recorded in branch and then communicated via the BRDB to the Audit Store) is protected in the following ways-

(a) Counter transactions (i.e. those transactions that originate in branch due to the actions of branch staff) are given a unique number of 1 greater than the previous transaction so that the data can be checked for missing or duplicate transactions.

(b) Counter transactions are also digitally signed (i.e. a unique "hash" is applied to each message) so that the accuracy and validity of the transaction data can also be checked.

(c) Non-counter transactions (i.e. those generated by TAs that originate from Post Office) must be accepted by branch staff before they enter into the BRDB. Once accepted, the TA is digitally signed by the Counter and sent to the BRDB and then on to the Audit Store.

(d) The original non-counter transactions raw data file is also sent direct to the Audit Store and the digitally signed file from the BRDB can be compared to the raw date file to check its integrity (this has been represented by Fujitsu to be the case but not tested during the course of our work).

(e) When data is sent from the BRDB to the Audit Store via the Audit Server it is sealed (while in the Audit Server) and a database of sealed files is maintained so that when data is subsequently retrieved from the Audit Store, its integrity can be checked. The mechanism to do this (MD5 hashing algorithm) was previously a well adopted industry standard mechanism. Although this is now a technically obsolete (in that for encryption purposes it can be cracked relatively easily) significant technical expertise would still be required to exploit this vulnerability.

(f) Indirectly the integrity of the transaction data is protected by the interface of BRDB data on a regular basis to downstream systems (some of these feeds for a number of products are in real time), and therefore interception and adjustment of data would have to concurrently update BRDB and downstream data sources to remain in alignment and prevent being subsequently spotted.

1.4.2.3 Setting aside the "remote access" issues discussed below, in our view:

(a) controls are in place to support the integrity of the processing of data from the Counter into BRDB and the Audit Store. The level and design of the controls is proportionate to a system of the size, scale, usage and data sensitivity, of Horizon;

(b) it is very unlikely that the data input by branch staff and as recorded in the BRDB and the Audit Store would be incomplete or inaccurate.

(c) in the event that data was incomplete or inaccurately recorded, the controls in Horizon provide tools that can be used to effectively identify such issues;

(d) therefore a suitably skilled and qualified person could review the raw data from the Audit Store to determine whether any data was incomplete or inaccurate (as a result of one of the actions set out at 1.2), and when data is extracted from the Audit Store a number of checks are performed to validate the completeness and accuracy of the data (none of which have been flagged to us as failing by Post Office or Fujitsu in the extraction of data relevant to this case).

1.4.2.4 In response to the allegations referred to in section 1 above, we would highlight that our testing supports the following assertions (subject to the limitations in Section 1.5 below):

(a) Neither Post Office nor Fujitsu have the ability to log on remotely to a Horizon terminal in a branch so to conduct transactions.

(b) Neither Post Office nor Fujitsu users nor administrators have the ability to conduct transactions (either remotely or locally) under another user 's ID (unless that user shares their password but this would be a breach of operational procedure). As with the majority of computer systems there are ~~a~~ some ~~small number of~~ generic accounts (service accounts, or other accounts named so not specifically assigned to a specific user)~~, which are in breach of this principle~~.

Commented [A3]: How many?

MAMW: Difficult to quantify in this case. We have seen specific examples but cannot provide population estimates with the data we have,

MU – IF WE CANNOT QUNATIFY, HOW DO WE KNOW IT IS ONLY A SMALL NUMBER? WE NEED TO PROVIDE SOME ADDED DETAIL HERE

JG Can we say that transactions entered using these generic accounts are clearly identifiable in the transaction logs?

Commented [A4]: If such generic accounts are common, what principle is being breached? Suggest that this wording is deleted.

MAMW: Wording updated as discussed.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

(c) Neither Post Office nor Fujitsu have the ability to inject additional transactions into a branch's accounts, through normal systems functionality, without either a Postmaster's (a) knowledge or (b) consent (however see 1.4.2.5 below).

(d) This is with one exception for a small group of Fujitsu Privileged Users (30 users) who may do so via Balancing Transactions (BTs):

(i) BTs do not require formal acceptance through the Horizon terminal by branch staff (unlike transaction corrections and transaction acknowledgements) and so can be pushed into the branch accounts by Fujitsu.

(ii) A population of BTs since the inception of Horizon HNG-X was extracted from the Audit Store and a review of this highlighted that there had only been one usage of BTs for general data correction in this period (at a branch not associated with the allegations). BTs are used more routinely (although still infrequently – 1,643 instances during the period of approximately 6 years) to update a flag which can become locked in the wrong binary setting (1, 0), preventing updates to stock units within a branch.

1.4.2.5 Fujitsu (but not Post Office) has the ability to amend or delete transactions entered by branch staff on Horizon via Privileged Users outside of specific functionality of the Horizon application – this is addressed below in the next section.

1.4.2.6 A limited number of authorised Fujitsu personnel (19 at the Operating System layer and 26 at the database layer, at the time of testing - ~~June~~May 2016) have sufficient privileges to theoretically add / delete / change data in the BRDB (**Privileged Users**). However, see paragraph 1.4.2.10 below regarding the segregation of access conditions. These users may also have access to other systems, such as the Audit Store, however in the current circumstances access to the BRDB is the most important as it is the BRDB that generates the branch accounts and is the source of the data ultimately used to hold Postmasters liable for shortfalls.

1.4.2.7 Post Office personnel do not have this Privileged User access and Fujitsu and Post Office have asserted that they have never had such access, however there is no historic record of all the Privileged Users that there have ever been, so this cannot be verified.

1.4.2.8 Changes to a branch's transaction data in the BRDB by Privileged Users would be visible to branch staff. The amended transaction would show up in transaction reports produced in branch but would not be flagged as a change by a Privileged User and to the best of our knowledge would appear like a normal transaction generated in branch. (although~~Also~~ see paragraph 1.4.2.14 below around database logging of the actions of Pprivileged Uusers).

1.4.2.9 We would expect a system such as Horizon to have this type of Privileged User access as it will be used to undertake maintenance on the system or to implement updates. Such access comes with a risk of it being misused, either by accident or maliciously. It is impossible to eliminate this risk entirely (within Horizon or any other IT system) and so systems generally have controls over the use of Privileged access so as to reduce the risk or misuse or to make it detectable.

1.4.2.10 A key control in Horizon is the segregation of access permissions between Privileged Users who can access the BRDB and those users who may access the Key Management Server (**KMS**). The KMS holds the digital keys that underpin the controls listed in paragraph 1.4.2.2. Segregation of Privileged Users from KMS users means that a Privileged User cannot get around the controls in paragraph 1.4.2.2 and therefore cannot cover up any changes they make in the BRDB (Controls 1.4.2.2 b, c, d and e are of particular importance). If a proper segregation of duties is in place, any changes by a single Privileged User to the BRDB would be detectable in line with paragraphs 1.4.2.2 b, c, d and e above. This does not eliminate the risk of misuse entirely as there could be a conspiracy between a Privileged user and a KMS user.

1.4.2.11 Through our enquiries, we have identified that 25 current Privileged Users have access to the KMS such that they could theoretically cover up changes they make to the BRDB data. This is a failure by Fujitsu to implement its own segregation of duties policy. We are unable to determine how long this vulnerability has existed as records of historic users are not kept, and as far as we are aware it has not been fixed by Fujitsu.

Commented [A5]: Can Privileged Users add transactions/data? See 1.4.2.4(c) above.

MAMW: Amended the wording above.

JG - if Priv Users can add transactions, how would they disguise them? Wouldn't there be no space in the JSN to slot an additional transaction in?

MAMW – Could add them with the most recent legitimate JSN reference.

Commented [A6]: There would be no visible difference at all?

MAMW:

I don't think so -Not in reports. Database logs would potentially highlight this as we discuss elsewhere.

MU – CAN WE PLEASE INCLUDE WHETHER OR NOT IT WOULD APPEAR IN THE DATABASE LOGS AND WHERE IN THE REPORT THIS IS DISCUSSED IN MORE DETAIL?

MAMW: Added,

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

1.4.2.12 Despite this vulnerability, there are a number of other factors to consider in determining the likelihood that actions by a Privileged User would be the cause of shortfalls in a branch.

1.4.2.13 First, Horizon has functionality (in the form of transaction corrections and balancing transactions) to resolve the significant majority of imaginable operational errors in branch or technical errors in Horizon. There is therefore little need to use privileged access to manipulate transaction data to resolve an error – such use would be a last resort, and outside of mandated process (Balancing Transactions in particular are a deliberately engineered process to support the exceptional corrective processing that less controlled privileged access would typically be used for).

1.4.2.14 Based on assertions from Fujitsu, there is a key split in dates around the audit trail of privileged user usage in July 2015:

(a) Pre July 2015 - only Privileged User log on and log off's were logged. However these are expected to be of a low volume, and would always (if valid 'accesses') be approved by a documented access request form.

(b) Post July 2015 – Fuller transaction audit logging was enabled by Fujitsu. ~~a~~A reviewer could always see the last action by a Privileged User, if a Privileged User deleted their actions, it would always leave a footprint of the deletion of logs. They could theoretically remove what they have done, but they cannot remove that they have done something.

1.4.2.15 Fujitsu have advised us during the course of testing that turning off audit logs completely would 'break' the application, causing it to crash and become un-functional. We have performed no further testing to validate this assertion. A 'Delete' record on the audit trail is likely to be highly unusual and easy to spot, and should facilitate further testing should it be required.

1.4.2.16 Second, subject to the circumstances described in paragraph 1.4.2.17 immediately below, any change to a branch's transactions in the BRDB by a Privileged User would be visible to Post Office, Fujitsu and branch staff through the reports available from the system. Further, Fujitsu has the data and, has informed us, the expertise, to identify that the root cause of the change was the actions of a Privileged User via interrogation of the audit trails maintained on such activity, and a likely lack of coherency between amended data and the records of that data within other systems. This means that should a Privileged User have materially changed a branch's transaction data via unauthorised mechanisms, it is likely that it would be spotted and resolved; any unauthorised Privileged User change, regardless of materiality, would be identified by control 1.4.2.3(d) if transactions were checked.

1.4.2.17 Third, there is a theoretical risk of a Privileged User maliciously changing a branch's data and successfully covering up that fact that those changes were made by the Privileged User (due to Fujitsu's failure to segregate duties) but in our view this is an unlikely risk to crystallise because the steps that would need to be taken for this to be successful are complex. A high level of technical expertise would be needed to do this, it would almost certainly require the writing of a bespoke computer programme, the circumvention of several other control measures and deployment of the fraud in a relatively small window of opportunity. We believe it would take significant planning to execute this successfully. In summary:

(i) There are a limited number of users (25 at the time of testing – June 2016) who could theoretically, due to a segregation of duties breach between database administration and the key management server, amend the Message Log for one or more Counters in one or more branches and make the transaction/s amended, look legitimate when it is retrieved from the Audit Store (through spoofing of the digital signature).

(ii) However to do this would require an existing systems administrator with a large amount of technical expertise and systems knowledge, it would almost certainly require a program to be installed onto the Horizon online system, and a release process would have to be bypassed in order for this to be installed maliciously (and avoid file integrity checking controls operated by Fujitsu).

(iii) There is also a time restriction of under 24 hours where the amendment of the message log would have to complete by (likely to be a much smaller time window of

Commented [A7]: How many?

MAMW: Added

MU- FOR ALL OF THESE QUESTIONS THAT HAVE SINCE BEEN QUANTIFIED – DO THESE NUMBERS REPRESENT THENUMBER OF USERS THAT CURRENTLY HAVE THIS ACCESS OR THE NUMBER OF USERS THAT HAVE HAD THIS ACCESS OVER THE LIFETIME OF HORIZON?

Agree - need to provide dates to future proof the report.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

opportunity for the majority of transaction types where there is real-time or near real-time processing ~~, such as~~ (for example a number of postal transactions generate a 'Track and Trace' message as they are carried out in the branch and t~~.~~ These messages are sent to Royal Mail/Parcelforce in near real time~~[insert example]~~). This is because such real-time or near real-time processing would copy data to other data sources and as a result expose data which had been edited post such transfer, through lack of coherency between differing data sources.

Commented [A8]: Please add an example

MAMW: TO DISCUSS WITH LEWIS

(iv) Further since July 2015 there will always be a record of a Privileged User amending transactions in this way due to audit logging always logging DELETE actions (even if a Privileged User deleted their actions this action would be logged). Pre-July 2015 there will be logs of Privileged User log and log offs to the Horizon system databases, Privileged User log on / offs should be inherently rare, and would (if legitimate accesses) always be accompanied by a request for access and appropriate approvals.

(b) In light of the above, it seems unlikely that a Privileged User would have the motivation to do this besides being involved in some form of fraudulent collusion, and their motivations for doing so given the impacts would be to a branches accounts or Post Office's P&L are not easy to theorise.

1.4.3 Legacy Horizon

1.4.3.1 The old Horizon system was named 'Riposte'. This was a third party provided product which provided a similar functionality and service as the current Horizon system, but with a number of important distinctions, in the context of the allegations made in Section 1 of this Executive Summary above:

(a) On the Riposte system the data was held locally on a Branch Server and then replicated to a cluster of central servers overnight. On HNG-X a key principle is branch data is only held centrally (on the BRDB).

(b) A CRC (Cyclic Redundancy Check) function provided functionality similar to the digital signature in that it provided a checksum capability. A checksum applies a predetermined algorithm to a set of data, to produce an output. When transmitted or held with the data the checksum algorithm can be reapplied to validate whether the dataset is complete and accurate. Unlike the digital signature applied by Horizon to Counter transactions, this is not cryptographically secure, and technically competent people can generate CRCs simply (i.e. it is at greater risk of tampering).

(c) Once data was received from a branch server by the centralised server farm, it would be duplicated to all nodes in the farm (they were four clusters), meaning that challenges in terms of altering the data would likely still exist (as data would now be different between different nodes), causing a data integrity issue which would be likely to generate system errors and be noticed if only one location was updated.

(d) Riposte was a third party provided system, meaning that neither Fujitsu nor POL would have been likely to have ready access to the source code of the application. Access to source code is an imperative requirement to being able to change the underlying code or functionality of the application, and the fact that POL or Fujitsu would have been likely to require an approach to the vendor in order to do so, would inherently lower the risk of malicious changes to the application from Privileged Users (although not necessarily the amendment of transactions data within the system).

(e) The Audit Store technology was largely identical to the instance supporting Horizon HNG-X at the point of adoption (including the audit server).

(f) Fujitsu have stated that due to (b), (c) and (d) above an application would need to be inserted onto a Branch server to manipulate transactions prior to them being distributed to the datacentre, and that whilst there is a theoretical possibility this could be achieved, it is considered by Fujitsu to be a 'remote possibility'.

1.4.3.2 Our assessment of Riposte was largely dependent on interview with Fujitsu SMEs and review of the available technical documentation. Given the time that has elapsed and lack

POL00029097

of a system to perform direct controls testing or substantive procedures thereon further testing over this system was limited.

1.4.3.3 We did perform some analysis of the baskets generated by Riposte, which initially identified 0.0015% of transactions had errors, but subsequently demonstrated these were false positives as set out in section 2.2.1 (i.e. they were not actually errors).

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

1.5 List of Assumptions and Limitations

1.5.1 Where we have reviewed technical documentation we are reliant on the accuracy of the information contained within.

1.5.2 Where we have interviewed with Fujitsu and POL SMEs we are reliant on the accuracy of the information provided by these individuals.

1.5.3 Where these sources of information (Appendix 1 and the broader procedures illustrated throughout this report) have not highlighted system functionality which is a potential risk in the context of the allegations described above, we will not have performed procedures over this system functionality.

1.5.4 Our work has utilised sample testing to support the operation of controls and substantive procedures. Whilst sample testing is a useful tool for assessing an overall population, there is a possibility that our samples and the conclusions we have derived from them are not representative of the overall population. Samples selected to support the controls testing were aligned to Deloitte's standard methodology for sample selection, based upon the frequency of operation of the control.

Commented [A9]: Need a statement justifying the sample sizes selected by Deloitte.

MAMW: Added for controls testing.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2. Management Summary

2.1 Background and Scope

Post Office Limited (Post Office) continues to respond to allegations that the "Horizon" IT system used to record transactions in Post Office 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 the present day. In response to the commencement of litigation proceedings, Deloitte was originally instructed to plan and execute procedures and respond to three scope areas supporting Post Office's ability to understand how Horizon (HNG-X) has been operated to prevent incorrect system operation that could have resulted in Postmaster detriment.

After the completion of the initial procedures (Phase 0 and Phase 1) over the three scope areas, it was identified that further investigations would be required following the identification of exceptions in key controls tested by Deloitte and identification of key areas of risk. As such, Deloitte was instructed to provide responses to specific questions to aid Post Office's ability to understand a number of areas within Horizon (HNG-X), namely:

1. The usage of Privileged Users and the configuration of audit logs (specifically over the actions of Privileged Users, including audit logs over Riposte); and
2. The control environment over ~~Non Counter~~Non-Counter Transactions.

All procedures performed throughout the various phases of work have been designed to assess the level of relevant risks surrounding financial loss to Postmasters or levels of reliance that can be placed on data used by case handlers.

It should be noted that this report is to be considered a 'living' document, and in its current format represents the final format following the completion of Phases 0 – 4. Future updates may be required if additional work is scoped in at a future date.

2.1.1 Phase 0 and Phase 1

The scope areas over which Deloitte was originally instructed to perform procedures are as follows:

1. *Scope Area 1* - To carry out an analysis of the relevant transaction logs for branches within the Complaint Review & Mediation Scheme (the "Scheme") to confirm, insofar as is 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 (see 2.2.1).
2. *Scope Area 2* - To carry out a full review of the use of Balancing Transactions throughout the lifetime of the Horizon system and, insofar as is possible, to independently confirm from Horizon system records the number and circumstance of their use (see 2.2.2).
3. *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 is possible (see 2.2.3).

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

1. Background and context in relation to this engagement;
2. The approach Deloitte have taken to planning the procedures;
3. The testing procedures Post Office has, upon Deloitte's recommendation and with agreement of Post Office and their advisors, requested Deloitte undertake in response to the planning activities; and
4. Results of these testing procedures.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.1.2 Phase 2

This additional phase of work constituted 'Phase 2', the 'Further Investigations Phase', whereby Deloitte performed procedures it recommended and agreed with Post Office and their advisors in response to certain findings or outcomes of 'Phase 0' and 'Phase 1' against the three scope areas examined during that phase.

The three additional scope areas were:

1. *Additional Scope Area 1* – To perform an investigation of Privileged User Audit Logs from Branch Database, the controls over them, and corresponding data extract and interrogation options (see 2.2.4).
2. *Additional Scope Area 2* – To perform an investigation of analytics test results 1: 'Identify Gaps in Audit Logs Sequencing', and 6: 'Identify branches which are out of balance based on transactional data available' (see 2.2.5).
3. *Additional Scope Area 3* – To perform an investigation of controls over the integrity of non-counter initiated transactions, e.g. Paystation (see 2.2.6).

2.1.3 Phase 3

This additional phase of work constituted 'Phase 3', the '~~Non Counter~~Non-Counter Transactions Phase' whereby Deloitte performed procedures it recommended and agreed with Post Office and their advisors in relation to Non-Counter transactions to provide an assessment against the following questions:

1. Are there any gaps in the controls around Non-Counter transactions that could call into question the Integrity of the data generated in relation to these transactions? (see 2.2.7)
2. If there are gaps (see 2.2.8):
    a. Could they be the cause of discrepancies in branch accounts (or could they mean that errors in Horizon would not be revealed and those errors could then be the cause of discrepancies in branch accounts); and
    b. What is the risk of those gaps (or resulting discrepancies) materialising?

2.1.4 Phase 4

This additional phase of work constituted 'Phase 4', whereby Deloitte performed procedures it recommended and agreed with Post Office and their advisors in relation to the Fujitsu Report 'Database Security in Horizon Online', specifically:

1. Deloitte review of Fujitsu Report in conjunction with initial comments raised (see 2.2.9).
2. Workshop with appropriate Fujitsu resource (see 2.2.10) to:
    c. Answer any outstanding comments / questions on the report.
    d. Produce a detailed commentary on what steps would need to be taken to replace the message log, as per ~~section 2.2~~Section 2 of the Fujitsu report (reproduced in Appendix 9).

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2 Summary of Results

A summary of the key controls tested and the results of that testing are set out below for all Phases (1-4 – Note Phase 0 was a planning phase to determine the procedures needed for Phase 1 and so did not produce testing results in its own right, hence it is not referenced below). A full set of agreed procedures tested and associated results has been included in Section 4 of this report. These should be reviewed in tandem with the assumptions and limitations that have been included in Section 5 and at the end of this Management Summary.

2.2.1 Phase 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 is 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 a review of some of the source code which supports the correct operation of the system in relation to 'bugs' (an 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, it is alleged, could have caused shortfalls in branch accounts. These are controls which in our scoping discussion with Post Office and Fujitsu have been determined to be fundamental to protecting the integrity of transaction data within the system.

The key controls identified were:

1. All transactions on the Horizon Counter balance to zero – *No Relevant Exceptions Noted.*
2. Transactions are atomically (either in entirety, or not at all) written to the Branch Database – *No Relevant Exceptions Noted.*
3. 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.*
4. 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 (at the point our testing was conducted – June 2016):

   - *'25 IT users (i.e. non-Branch staff) have access to mechanisms for managing the digital signatures (i.e. access to the key management server and related technologies) 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 (see section 2.2.10)'*
5. Transaction Acceptance (in relation to interface file receipt for non-counter originated interface files) is required by Postmaster's in order to be accepted into branch accounting records. – *No Relevant Exceptions Noted.*
6. Recovery processes are in place for transactions in the event of connectivity failure. – *Relevant Exceptions Noted.*

   The exceptions noted were (at the point our testing was conducted):
   - *'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 (as would be enforced by the system) 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.'*

Commented [A10]: Currently, as at X date or over X number of years?

MAMW:

Added that it is at the point of testing.

JG - I think we need a specific date

MU – DO WE KNOW / IS IT POSSIBLE TO ASERTAIN THE NUMBER OF USERS WHO HAVE HAD ACCESS SINCE THE INTRODUCTION OF HORIZON?

MAMW: No – I think we make that point elsewhere as well.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

The first exception could lead to an increased risk that Postmasters are unaware of transactions being posted in a power failure, although they are notified by receipt that this has occurred.

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:

1. 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 Post Office'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.
2. 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 left the 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 (note: this is a separate point to the segregation of duties issue).*

  As a result they would have the technical knowledge and access rights to make changes to Horizon HNG-X which were not sanctioned by management – this ability could theoretically be used to subvert the controls over Horizon, or system functionality, for personal gain or other malicious outcomes.

  Fujitsu stated that:

  "*Whilst we appreciate that there is lack of segregation of duties here for the <specified user> between Live and Development, it is felt that there is a strong business need for this access for <specified user>. 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:

1. 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 originally noted (see Appendix 6a for details and summary of initial findings). One such initial finding of note was that 'there were 48 (0.0015%) session ids from a total of 3,124,140 which were out of balance based on the transactional data received. Those 48 session ids out of balance related to 18 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-X in 2010. As explained in section 4.5.2 below, further sample testing work was undertaken on the 48 items and it was established that none of the items originally noted were issues when looking at fresh extracts of the system data – the original extracts provided were out of as they had not been extracted correctly.

Commented [A11]: Is this the segregation of duties control exception?

MAMW: No this is a different issue. No changes made to the report.

Added a note to make this clear.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.2 Phase 1 - Scope Area 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 is possible, to independently confirm from Horizon system records the number and circumstance of their use.*

In performing our procedures against this scope area, we worked with Post Office and Fujitsu to identify other methods of posting transactions which impact a branch accounts, without knowledge of the Postmaster which in the context of the allegations present similar risks to that of Balancing Transactions. This highlighted other areas of potential risk, such as:

1. 'Global Users' – being central users who can access branches remotely for support purposes (by remotely this means accessing a branch terminal without being physically present in the branch). Critically we have been informed by Fujitsu and have verified as far as possible, that such users are not able to post transactions remotely (i.e. view only access), but they can only make edits when physically in the branch.
2. 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 were 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:

1. Logical Access rights to these sensitive functions had been appropriately restricted. – *No Relevant Exceptions Noted.*
2. 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.*
3. 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 (at the point our testing was conducted – June 2016) was:

   - *'25 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.'*
4. It was also noted via a control walkthrough that any Transaction Corrections created by Post Office Finance must be accepted by a Postmaster at branch prior to affecting branch accounts. – *No Relevant Exceptions Noted.*
5. 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.*
6. 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. 26[1] users (at the time of testing – May 2016) are granted extended privileges which enable them to update / delete records. However the control is operating in*

[1] This number, 26, is different to the previous figure of 25 quoted around privileged users with access to both BRDB and the Key Management Server (thus contravening expected segregation of duties), as it relates purely to SSC users with privileged access rights, contravening the above control wording.

Commented [A12]: This feels like a higher standard than we did. I presume we just attempted it and it demonstrated it could not be done. We probably did not try and use every possible way of doing it.

MU – THANKS – SO THESE USERS HAVE A LEVEL OF ACCESS BELOW AND DIFFERENT TO PRIVILEGED USERS?

MAMW – That is correct and I think interpretable as such by the current text.

Commented [A13]: Currently or over the lifetime of Horizon being in place?

MAMW: Updated.

Again, I think we need to give a date

Commented [A14]: How can this number be greater than the 25 on the previous page?

Further, are we saying that privileged users cannot only insert transactions but also delete and edit existing transactions?

MAMW:

This is valid as a totally separate point. One is referring to the breach of the segregation between system administration for BRDB and the key management server. The paragraph where you have raised this comment is talking about people with SSC access who have update delete access to the database. They are separate points.

JG - please make the distinction clear in the report

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

line with management's expectations. Access to the privileged role is restricted to users explicitly authorised for this access. User actions are audit logged, but not proactively reviewed.' (Note: This has been raised as an exception as it is stating that 26 users within SSC also have backend database access allowing them to directly insert transactions).

Commented [A15]: FOOTNOTE ON THE 26 WHEN FIRST APPEARS

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:

1. 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 Post Office'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.
2. 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 the controls tested is the creation of the BRDB to replace individual Branch Databases (2010). This change fundamentally altered the operation of many of the 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 section 2.2.1 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:

1. 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. The insertion was four new lines of SQL transactions each for a value of £4000. Other uses of the tool used to insert Balancing Transactions were noted, however they do not affect transactional data and relate to the update of a specific flag (SU) to enable continued processing.
2. Additional context around the usage of this tool was obtained from ticket review:
    a. The original TFS helpdesk ticket was obtained which is the legacy system used by Post Oeffice where branch incidents are recorded. The TFS ticket 2091569 was reviewed and it was noted that this had been raised by Anthony Vasse (Service Desk) on 02/03/2010 and transferred to Cheryl Card (SSC Product Specialist). Within the incident ticket it was noted that the after investigation the clerk had incorrectly doubled a transfer of stock of £4000.00 to £8000.00; therefore creating an incorrect loss to the branch of £4000.00. It was noted this issue was required to be fixed by 17/03/2010 as the branch was due to roll into the next transaction period; therefore meaning that the branch required a fix to ensure the accounts were correctly recorded. An update was provided by Cheryl Card on 11/03/2010 confirming that the issue had been resolved using the transaction tool to insert transactions into the BRDB_RX_REP_SESSION and BRDB_RX_EPOSS_TRANSACTIONS tables to reverse the incorrect £4000.00 charge. The ticket confirmed that the Post Master had been advised to print a balance snapshot of the accounts before and after the transaction correction took place to ensure the transaction had been reversed correctly. A subsequent update was provided confirming that the balances had been correctly fixed. The ticket was subsequently closed on 04/04/2010.

    b. Evidence was obtained of the Peak Incident ticket raised in relation to this balancing transaction performed. Incident ticket 'PC0195561' was raised by Lorraine Elliot (Service Desk) on 15/04/2010 in relation to a Post Master attempting to transfer £4000.00 when the system crashed resulting in the post master being issued with 2 x £4000.00 receipts.

Commented [A16]: Can we include some further detail e.g. the amount of £ involved, date etc.

MAMW: Done.

MU: THANKS – CAN WE ADD ADDITIONAL CONTEXT INFORMATION E.G. WHY IT WAS NECESSARY

MAMW: Additional context added both here and in the main body of the report.

Formatted

Formatted: Indent: Left: 2.54 cm, No bullets or numbering

Formatted

Formatted: Indent: Left: 2.54 cm, No bullets or numbering

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

c. An OCP ticket was also raised which is the solution management system used by Fujitsu which tracks issues and resolutions. From this OCP reference 25882 it could be seen that the branch had performed a transfer out of stock for the value of £4000.00 but due to a system error this had incorrectly doubled in value creating an imbalance of £4000. Therefore, a balancing transaction of £4000.00 was required to correct the loss using the transaction correction tool. This was approved by Emma Langfield (Post Office) on 10/03/2010 at 15:33. From this OCP ticket, it could be seen that this incident was raised by Cheryl Card (SSC Product Specialist) on 10/03/2010 who subsequently performed the work and inserted the balancing transaction.

1.

Formatted

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.3 Phase 1 - 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 is possible.*

In performing our procedures against this scope area, we worked with Post Office and Fujitsu to identify how baskets of transactions flow from creation at the counter, through the sealed audit store (See Section 3, Background, for a high level overview).

Further, we tested controls over the accuracy, completeness and validity of the flow of data into the audit store, which is used as the master data source for audit purposes (and hence the primary source of data in relation to these cases). We identified the following key controls during scoping as being fundamental to ensuring the accuracy, completeness and validity of this data flow:

1. 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*.
2. 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*.
3. 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 (at the time of testing – June 2016) was:

   - *'25 IT 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.'*
4. 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*.
5. 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*.
6. Audit tracks that are gathered at one data centre are replicated to the Audit server at the remote data centre. – *No Relevant Exceptions Noted*.
7. 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* (reader should be mindful of the more general limitations of the MD5 algorithm as highlighted within the executive summary).
8. 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*.

Formatted: Font: (Default) Times New Roman, 12 pt, English (United Kingdom)

Commented [A17]: Currently or over the lifetime of Horizon?

MAMW:

Updated again (at the time of testing).

JG - when was testing?

MAMW: Added the month – June 2016.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

9. 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.*
10. The following operating system level events on the Audit Server are audited via the System Management event monitoring facilities:
    a. Log on/Log off (including unsuccessful log on attempts)
    b. File Creation, Deletion and Modification (on selected files)
    c. Modifications to system configuration (incl. software configuration and account details)
    d. System start up and shut down
    e. 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.' (i.e. a failed attempt to update audit policy would not be reported on).*

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:

1. 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 Post Office'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.
2. 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.
3. 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 Section 2.2.1 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:

1. 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. This was determined via interrogation of the supporting logfilelog file settings.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.4 Phase 2 - Scope Area 1

Scope Area 1: *Investigation of Privileged User Audit Logs from Branch Database, the controls over them, and corresponding data extract and interrogation options.*

In performing our procedures against this scope area, we held a workshop with Post Office and Fujitsu in which the approach was decided for future phases, and centred on a report produced by Fujitsu on how Privileged User access is controlled by Fujitsu.

The key facts determined at this stage of the investigation (to be illuminated further by the production of the Fujitsu report) were that:

1. Regardless of access rights to amend and delete audit logs, the digital signature controls should still allow for the detection of data which had been modified, deleted or inserted subsequent to receipt from the Counter (subject to the next point).
2. There are a limited number of users (~~26~~25 at the time of testing – June 2016~~)~~ who could theoretically, due to a segregation of duties breach between database administration and the key management server, amend the Message Log for one or more Counters in one or more branches and make the transaction/s amended, look legitimate when it is retrieved from the audit store (through spoofing of the digital signature).
3. However to do this would require an existing systems administrator with a large amount of technical expertise and systems knowledge, it would require a program to be installed onto the Horizon online system, and a release process would have to be bypassed in order for this to be installed maliciously (and avoid file integrity checking controls operated by Fujitsu).

Given the above findings, Fujitsu were requested to prepare a paper outlining the steps a Privileged User would need to take to subvert the digital signature controls, and this has been documented within our write up of Phase 4 (see below).

Commented [A18]: How many

MAMW: Added.

Commented [A19]: I'm lost again - it would help if the wording around the numbers was consistent

MAMW: Updated. Typo.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.5 Phase 2 - Scope Area 2

Scope Area 2: *Investigation of analytics test results 1: 'Identify Gaps in Audit Logs Sequencing', and 6: 'Identify branches which are out of balance based on transactional data available'.*

We performed further investigations over certain analytics test results from Phase 1. Analytic 1 – '*Identify gaps in audit log sequencing*' and Analytic 6 '*Identify branches which are out of balance based on transactional data available (should not be possible based on inherent system controls)*'. These further procedures highlighted in each case that there was a reason for each of the results and they were not therefore indicative of a problem with the operation of the Horizon system.

The original challenges highlighted were:

1. *Analytic 1* – 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 13,666,238 transactions.
2. *Analytic 6* - 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. The data used was filtered for transaction mode 'SC' only. There were 48 (0.0015%) session ids from a total of 3,124,140 which were out of balance based on the transactional data received. Those 48 session ids out of balance related to 18 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-X in 2010.

The results after responding to the challenges in the original analytic were:

1. *Analytic 1* –The analytic logic was revised following discussion with Fujitsu and following this revision there were no gaps in audit log sequencing.
2. *Analytic 6* – There was a logic error in the production of the extracts originally provided by Fujitsu. A sample of 15 items which were errored in the original data was investigated to confirm they were fixed when looking at the revised data provided by Fujitsu and confirmed the root cause was issues with the data extraction rather than the underlying data within the system.

Given the original discrepancies in these analytics were resolved, no further work against this area was recommended or required.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.6 Phase 2 - Scope Area 3

Scope Area 3: *Investigation of controls over the integrity of non-counter initiated transactions, e.g. Paystation.*

Following our work for Phase 1, we understood that non-counter transactions were not subject to the same level of controls as counter transactions for the following three non-counter sources:

1. Camelot (*Current*)
2. Paystation (*Current*)
3. Post and Go (*Historic*)

A key area of focus in the operation of these controls is the ability of the Postmaster to validate that the data being received from these external data sources is correct, and this was incorporated within the procedures that we suggested for inclusion and testing in Phase 3. In addition, a diagram highlighting the understanding gained of the data flows, and the related controls understood from technical documentation has been included within Appendix 8.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.7 Phase 3 - Question 1

Question 1: *Are there any gaps in the controls around non-counter transactions that could call into question the integrity of the data generated in relation to these transactions?*

This piece of work investigated any risk of data relating to ~~non counter~~non-counter transactions not being complete / accurate and being at risk of interference. It can be split into two parts:-

1. the controls applicable to data in respect of non-counter transactions before it is accepted into Horizon by branch staff; and
2. the controls applicable to data in respect of non-counter transactions after it is accepted into Horizon by branch staff.

Our procedures centred on:-

1. understanding data flows and controls over the current reconciliation process and how Transaction Acknowledgements are utilised;
2. testing key reconciliation controls between key data sources within the data flow;
3. performing detailed walkthroughs of the Transaction Acceptance process to confirm the granularity of the information Postmasters are provided with; and
4. performing an analytics pilot to assess the feasibility of performing a reconciliation between raw data files received by PODG (Post Office Data Gateway – the interface hub utilised by Post Office for receipt of external data files from Third Parties).

The first key area of interest from a controls perspective in relation to the completeness and accuracy of the flow of data is around the sending, processing by, and subsequent receipt of data from third parties. The primary control in relation to this is the requirement for Postmasters to accept 'Transaction Acknowledgements' in relation to such data before it is accepted into their accounts, but the formalisation of the processes and controls ensuring Postmasters reconcile their financial positions before accepting transactions has not been enforced. We have reviewed supporting documentation, primarily from the Horizon Online Help, which Post Office has informed us is available to branch staff which describe a number of reports which are available to assist Postmasters to reconcile data received from third parties. We have not validated this.

Originally it was theorised there was a second key area of interest, being that no digital signature is applied to ~~non counter~~non-counter transactions, potentially opening up this category of transactions to greater risk of interference subsequent to processing into the BRDB (as the digital signature is the primary control preventing downstream editing of transactions once they have been processed by the Counter). However, further discussion with Fujitsu established that when the BRDB receives ~~non counter~~non-counter transaction data, it pushes it down to the counter for acceptance by the Postmaster, at which point the Counter digitally signs the acknowledgement of the transaction and therefore in theory a reconciliation between these digitally signed TAs and the raw data files received from the third parties (which are interfaced into the Audit Store) should also be possible mitigating this risk. Note however that this means the data is digitally signed only from the point it is accepted by the Postmasters, and not prior to that point, making visibility and reconciliation of the data back to source by the Postmaster at the point of acceptance even more important.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.8 Phase 3 - Question 2

Question 2: *If there are gaps:*

a) Could they be the cause of discrepancies in branch accounts (or could they mean that errors in Horizon would not be revealed and those errors could then be the cause of discrepancies in branch accounts); and

b) What is the risk of those gaps (or resulting discrepancies) materialising?

In theory, if a third party incorrectly reflected the data they had received from a non-counter system, and this incorrect total was then downloaded into the Branch accounts, then in the absence of formal controls to reconcile data transmitted to the third party, back to data received, this could cause discrepancies in the branch accounts. However, Postmasters are able to challenge any transactions that they do not recognise / agree with through the aforementioned Transaction Acknowledgement process.

Without a full investigation of the controls at the third parties, and any other mitigating controls which may exist, it is difficult to quantify the risk exposure. However, the control which Post Office relies on to mitigate this risk is Transaction Acknowledgements and, as noted above, Post Office has informed us that branches have access to reports which assist with the reconciliation of data received from third parties (see 2.2.7).

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.9 Phase 4 - Question 1

Question 1: *To perform a review of Fujitsu Report in conjunction with initial comments raised.*

For this specific scope area our procedures centred on performing a review of the report produced by Fujitsu and the initial comments raised by Bond Dickinson.

In the context of the allegations, this was to:-

1. provide Post Office with an independent view of the Fujitsu report;
2. provide the expertise required to challenge it; and
3. identify the residual risks.

Following the review we provided an email which set out our views in line with the above. This was then supplemented by the workshop and challenge described in the next section.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.2.10 Phase 4 - Question 2

Question 2: *Hold a workshop with appropriate Fujitsu resource to:*

a) Answer any outstanding comments / questions on the report; and

b) Produce a detailed commentary on what steps would need to be taken to replace the message log, as per section 2.2 of the Fujitsu report.

For this specific scope area our procedures centred on holding a workshop with appropriate Fujitsu personnel in order to answer specific questions on the Fujitsu report and address any outstanding comments. Further, we provided a detailed commentary on next steps required to replace the message log as per section ~~2.2~~ 2 of the Fujitsu report (See Appendix 9).

Our review of the Fujitsu deliverable highlighted that Fujitsu have acknowledged (in drawing the conclusions below, we have taken what Fujitsu have said on its merit):

1. There is a theoretical risk of Privileged Users making edits to the Branch Database without leaving an audit trail, as Privileged Users can, in theory, delete the audit trail of any edits they may have made to the Branch Database. Fujitsu have however also represented that audit trails cannot be 'switched off; in their entirety as this would 'break' the Horizon application i.e. any such attempt would be immediately identifiable.
2. The audit trails have been limited to logon/logoff events prior to 2015. This limits the value of the audit trail in trying to determine any misuse (or indeed legitimate use, of Privileged User accounts prior to this date).
3. Based upon the above findings, the value of further work over Privileged Users is diminished due to the lack of granularity of audit trail pre-2015, and the capability of users to only leave a trace audit trail (their final delete action – as described in 1. above).
4. ~~Therefore, any further work, if it is deemed necessary, should focus on looking at logon events to the key management servers by those individuals who have access to subvert the segregation of duties (whilst noting they could also potentially tamper with the logs there as well), as well as tying such access down to service desk requests (i.e. a substantive response to the residual risk exposure).~~
5. ~~4.~~ The Fujitsu report further highlighted that to take advantage of these deficiencies would require the use of a program. See section 2.2.4 above for further details.

Commented [A20]: I don't think this should be referenced in this section. It can be included in along with the other 'recommendations' earlier on in the report.

MU – I STILL DON'T THINK THIS NEEDS TO BE INCLUDED

MAMW: Agreed and removed.

POL00029097

2.3 Fundamental Limitations and Assumptions

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

2.3.1 Phase 0 and Phase 1

1. It should be noted that controls tested/to be tested for Phase 1 relating to the system were tested on the system (HNG-X) operating 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. 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.
2. Further, all analytical procedures for Phase 1 were subject to the availability of data / ~~evidence., it is noted that while a~~Aevidence. A full transactional audit log is available since October 2007., ~~logistical / time constraints limited the volume of data that is able to be retrieved and interrogat e~~We have not interrogated this entire data set. Our procedures have ~~leverafe~~dutilised data provided by Fujitsu extracted from this broader population ~~in some instances~~. Also any controls testing is subject to the availability of evidence.
3. Finally, our work performed for Phase 0 and 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.
4. Please see Section 5 for a full list of assumptions and limitations.

2.3.2 Phase 2

1. It should be noted that procedures performed for Phase 2 relating to the system were tested on the system (HNG-X) operating 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. 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.
2. Non counter transactions work was dependent on technical documentation and our understanding was based on these documents. Subsequent conversations with Fujitsu highlighted that in a number of cases this documentation was out of date. Certain controls were originally scoped in for testing and then de-scoped as a result of these discrepancies within the available technical documentation (see section 4.6.2 for details).
3. Further, all analytical procedures for Phase 2 were subject to the availability of data / evidence, and reliance was placed on Fujitsu around the successful extraction of data. Some procedures were performed to support the completeness of the population of data provided by Fujitsu.
4. Finally, our work performed for Phase 2 was specifically limited to the scope areas outlined in the scope section above.
5. Please see Section 5 for a full list of assumptions and limitations.

2.3.3 Phase 3

1. It should be noted that procedures performed for Phase 3 relating to the system were tested on the system (HNG-X) operating 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. 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.
2. Further, all analytical procedures for Phase 3 were subject to the availability of data / evidence. A full transactional audit log is available since October 2007. We have not interrogated this entire data set. Our procedures have ~~leverag~~fedutilised data provided by Fujitsu extracted from this broader population. Also, any controls testing is subject to the availability of evidence.
2. ~~Further, any analytical procedures for Phase 3 were subject to the availability of data / evidence.~~
3. Our identification of ~~non counter~~non-counter Transaction flows has been dependent on the availability of technical documentation, and the accuracy of the facts and figures communicated within this technical documentation.
4. Our testing of reporting available to Postmasters in branches was based upon testing at the Model Office facility within Finsbury Dials, and we are therefore reliant on this being representative of the live environment.

Commented [A21]: Can we set out exactly what data was not able to be retrieved i.e. to what extent was this actually a limitation?

MAMW: To determine this fully would require a full review of our working papers. Is the amendment sufficient?

MU LETS DISCUSS ON THE PHONE AS THIS READS LIKE A SIGNIFICANT CONSTRAINT UNLESS WORDED CORRECTLY

MAMW: Which data was able to retrieved?

UPDATED.

Commented [A22]: What does this mean? Are Deloitte happy that the data was extracted successfully / correctly – see above comment

MAMW: As far as we can be…. We are merely pointing out that we had minimal oversight or influence on the data extraction process.

MU – BUT YOU DID TEST THAT IT WAS A FULL EXTRACTION – CAN WE INCLUDE SOME WORDING TO THAT EFFECT

Commented [A23]: Was any evidence / data not available – if not what?

MAMW: I will flag to Andy you are concerned about more generic limitations, but I think you'll be hard pressed to get him to remove them.

MU – WE NEED TO DISCUSS

MAMW: Amended.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

5. We have not been asked to validate or test controls at third parties such as Wincor, Ingenico and Camelot, which would be a key component in managing the risks associated with completeness and accuracy of the data flows associated with ~~non counter~~non-counter transactions.
6. Finally, our work performed for Phase 3 is specifically limited to the scope areas outlined in the scope section above.

2.3.4 Phase 4

1. Our work for this phase was based on a report produced by Fujitsu. We reviewed that report and raised questions on it, but we did not conduct any further testing on it or the responses to our questions provided by Fujitsu.~~, and reliance placed on the accuracy of the content within that report~~.
2. Further, our work performed for Phase 4 is specifically limited to the scope areas outlined in the scope section above.

Commented [A24]: Is this correct? was the scope of the work not to test the accuracy of the content within the report?

MAMW: It was to review and provide challenge, but remember we have not actually conducted further testing as a result!

JG - I've suggested some alternative wording.

MAMW: I think the alternative wording is ok, but ANDY to verify.

The wording I am seeing here is fine

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

3. Background

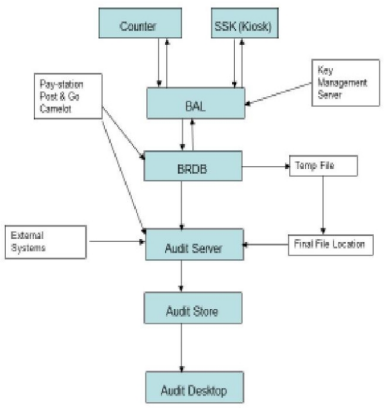
The Horizon system was developed by Fujitsu and is the core operational and Electronic Point of Sales (EPOS) platform for the Post Office network. Whilst formal benchmarking data is not available, it is considered by interviewed stakeholders to be one of the largest computer systems in existence in terms 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 and Phase 1 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 (data range is since October 2007). 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 Post Office, 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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).

Formatted: Not Highlight

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

DRAFT

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

3 Scope and Approach

3.1 Scope of Work

3.1.1 Phase 1

We structured our work around the three scope areas Post Office asked us to review, as shown in the table below:

Scope Area #	Post Office Instruction	Proposal
1	Post Office 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 is 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.	Post Office 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	Post Office 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 is possible, to independently confirm from Horizon system records the number and circumstance of their use.	Post Office 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	Post Office 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 is possible.	Post Office will instruct Deloitte to undertake this review, throughout the lifetime of the Horizon system, insofar as is possible.

DRAFT

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

3.1.2 Phase 2

The three additional scope areas agreed with Post Office were:

Scope Area #	Description	Proposal
1	Investigation of Privileged User Audit Logs from Branch Database, the controls over them, and corresponding data extract and interrogation options.	Hold a series of workshops and discussion meetings with Fujitsu personnel in order to discuss the relevant controls and audit trail configurations.
2	Investigation of analytics test results 1: 'Identify Gaps in Audit Logs Sequencing', and 6: 'Identify branches which are out of balance based on transactional data available'.	Pick a sample of 15 items from each analytic population for further investigation in conjunction with Post Office investigators and Fujitsu.
3	Investigation of controls over the integrity of non-counter initiated transactions e.g. Paystation.	Hold a series of workshops and discussion meetings with Fujitsu personnel in order to discuss the relevant controls and audit trail configuration.

The approach to 'Phase 2' was to hold workshops with relevant stakeholders from Post Office to support the delivery of the analysis described

3.1.3 Phase 3

This additional phase of work constituted 'Phase 3', the '~~Non Counter~~Non-Counter Transactions Phase', whereby Deloitte performed agreed procedures in relation to ~~non counter~~non-counter transactions to provide an assessment, as fully as possible within the time allocated to this exercise, on the factors to consider, controls, and risks in answering the following questions:

1. Are there any gaps in the controls around non-counter transactions that could call into question the integrity of the data generated in relation to these transactions?
2. If there are gaps:
   a. Could they be the cause of discrepancies in branch accounts (or could they mean that errors in Horizon would not be revealed and those errors could then be the cause of discrepancies in branch accounts); and
   b. What is the risk of those gaps (or resulting discrepancies) materialising?

We performed the following procedures:

1. Provisional workshop to corroborate understanding of data flows and validate the existence and completeness of controls over the current reconciliation process, and how Transaction Acknowledgements are utilised.
2. Review and test key reconciliation controls between key data sources within the data flow as highlighted within separate table (Appendix 8).
3. Perform detail walkthrough of the Transaction Acceptance (TA) process to confirm the granularity of information the Postmaster is provided with. Perform procedures to corroborate a TA is required for all ~~non counter~~non-counter transactions.
4. Analytics pilot to assess feasibility and then perform reconciliation between raw data files received by PODG and the interpretation of these ~~non counter~~non-counter transactions into the BRDB transaction files.

The approach to 'Phase 3' was to hold workshops and meetings with relevant stakeholders from Post Office and Fujitsu to support the delivery of the analysis described above.

Formatted: Not Highlight

Commented [A25]: Deleted as it serves no purpose - it is implicit that Post Office agreed because Post Office commissioned the work.

ANDY: TO CONFIRM HAPPY WITH THESE DELETIONS.

AW: Being agreed procedures is quite fundamental to scope and therefore can't be removed irrespective of who commissioned the work. Agreed Upon Procedures are vastly different in nature to Opinion reports.

JG - please explain the difference

MAMW: Let's discuss on our call.

Formatted: Not Highlight

DRAFT

POL00029097

3.1.4 Phase 4

Deloitte performed procedures in relation to the Fujitsu Report 'Database Security in Horizon Online', specifically:

1. Deloitte review of Fujitsu Report in conjunction with initial comments raised.
2. Workshop with appropriate Fujitsu resource to:
   a. Answer any outstanding comments / questions on the report.
   b. Produce a detailed commentary on what steps would need to be taken to replace the message log, as per section 2.22 of the Fujitsu report (reproduced in Appendix 9).

DRAFT

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

3.2 Summary of Approach and Work Performed

The work was performed in multiple phases. Phase 0 was 'Discovery' and Phase 1 was 'Testing' of the original scope. Additional phases of work were commissioned and specific agreed procedures were performed to provide clarity over the initial findings from Phase 1, against the three scope areas performed during that phase (Phases 2-4).

3.2.1 Phase 0 - Discovery

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

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

1. Reviewed relevant technical documentation as requested and provided by Fujitsu/Post Office during the course of this engagement.
2. Held workshops with Post Office Finance staff in Chesterfield on 14th and 23rd March, and 18th April 2016.
3. Held workshop with Fujitsu staff in Bracknell on 14th April 2016.
4. Held workshop with Case Handlers in Chesterfield on 8th April 2016

The aim of these procedures was:

1. 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 3.1.13.3.1).
2. 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 1.5, 2.3 and Section 5.1).
3. As a result of "1" and "2" 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 3.1.1see 3.1.1). We identified three core procedure types which were then utilised during Phase 1:

    a. *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.

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

    c. *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:

1. Performed on-site review and visit to Fujitsu and tested controls between May 2016 and September 2016.
2. Reviewed case data provided by Post Office case handlers and tested for characteristics which could illustrate the Horizon system has not operated as expected.
3. Reviewed relevant technical documentation as requested and provided by Fujitsu/Post Office during the course of this engagement.

Commented [A26]: Check reference

MAMW: Check references spelling and grammar once this version has solidified.

Commented [A27]: Check reference

MAMW: Check references spelling and grammar once this version has solidified.

DRAFT

POL00029097

3.2.3 Phase 2 – Further Investigations Phase

The objective of the further investigations phase was to obtain sufficient information and background on the specific areas in response to findings in certain scope areas looked at in Phase 1, and report on the associated findings from these procedures.

In performing work for Phase 2, Deloitte conducted the following procedures:

1. Held workshops with Fujitsu personnel to investigate the controls over Privileged User Audit Logs from Branch Database
2. Tested a sample of items from each analytic population, 1: 'Identify Gaps in Audit Logs Sequencing', and 6: 'Identify branches which are out of balance based on transactional data available'
3. Held workshops with Fujitsu personnel to investigate controls over the integrity of non-counter transactions, e.g. Paystation

The aim of these procedures was to answer the following questions, posed by Post Office:

1. What exact information is logged by the Privileged User Audit Logs?
2. Would this logged information definitively reveal that:
   a. A Privileged User had done something that could change a branch's accounts in the real-world; and
   b. What that Privileged User had done (e.g. does it show the change in such a way that it could be identified and either isolated or reversed out)?

3. If the Privileged User Audit Logs would not reveal all actions by Privileged Users that could affect branch accounts, please describe (in detail) the types of ways that a Privileged User could amend a branch's accounts in a way that would not leave behind a footprint of their activity?
4. What is the root cause of the gaps identified in analytics 1 and 6?
   a. Are these root causes indicative of problems in Horizon / evidence of flaws in Horizon's controls around the core audit process?
   b. Would these issues cause discrepancies in the branch accounts?

5. Are there any gaps in the controls around non-counter transactions that could call into question the integrity of the data generated in relation to these transactions?

6. If there are gaps:
   a. Could they be the cause of discrepancies in branch accounts (or could they mean that errors in Horizon would not be revealed and those errors could then be the cause of discrepancies in branch accounts); and
   b. What is the risk of those gaps (or resulting discrepancies) materialising?

3.2.4 Phase 3 – ~~Non Counter~~Non-Counter Transactions

This additional phase of work will constitute 'Phase 3', the '~~Non Counter~~Non-Counter Transactions Phase' whereby Deloitte will perform procedures agreed with Post Office in relation to ~~non counter~~non-counter transactions to provide an assessment as fully as possible in the time allotted by the exercise, on the factors to consider, controls and risks, in answering the following questions:

1. Are there any gaps in the controls around ~~non counter~~non-counter transactions that could call into question the Integrity of the data generated in relation to these transactions?
2. If there are gaps:
   a. Could they be the cause of discrepancies in branch accounts (or could they mean that errors in Horizon would not be revealed and those errors could then be the cause of discrepancies in branch accounts); and
   b. What is the risk of those gaps (or resulting discrepancies) materialising?

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

The procedures performed were as follows:

1. Held initial workshop to corroborate understanding of data flows and validate the existence and completeness of controls over the current reconciliation process and how Transaction Acknowledgements are utilised.
2. Reviewed and tested key reconciliation controls between key data sources within the data flow as highlighted within separate table.
3. Performed detailed walkthrough of the Transaction Acceptance (TA) process to confirm the granularity of the information the Postmaster is provided with. Performed procedures to corroborate a TA is required for all ~~Non Counter~~Non-Counter transactions.
4. Performed analytics pilot to assess feasibility and then performed reconciliation between raw data files received by PODG and the interpretation of these ~~non counter~~non-counter transactions into the BRDB transaction files.

3.2.5 Phase 4 – Privileged User Access

This additional phase of work constituted 'Phase 4', whereby Deloitte performed procedures agreed with Post Office in relation to the Fujitsu Report 'Database Security in Horizon Online', including a review of the report and a subsequent workshop to clarify understanding on certain areas.

DRAFT

POL00029097

4. Work Performed

4.1 Summary of Work Performed

For each scope area for Phase 0 and 1 we have laid out our work performed as follows:

1. Setting the Scene – We have described in a narrative format the work we have performed, and our understanding of the relevant subject matter.
2. A tabular format of the procedures performed in Phase 0, and the key learnings relevant to our planning.
3. The procedures which have been performed in Phase 1 and the findings obtained from the performance of those procedures.

For each scope area for Phases 2 to 4 we have laid out our work performed as follows:

1. Setting the Scene – We have described in a narrative format the work we have performed, and our understanding of the relevant subject matter.
2. The procedures which have been performed in this phase and the findings obtained from the performance of those procedures.

4.2 Phase 0 and 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 is 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 3.24.1 and 3.24.2. 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.

Commented [A28]: Check reference

MAMW: Check references spelling and grammar once this version has solidified.

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

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

DRAFT

POL00029097

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

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

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

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

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

3. Alongside the inherent system controls available for our review, we identified two tranches of data analytics work that we could perform to assess the risk of system failure or 'bugs':

   b. Using the case data provided (for all the branches with links to Postmasters for which this case relates via Post Office's file sharing platform 'Huddle')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.

   c. 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 of unsummarised transactions). Using tools already available via Fujitsu we were able to 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).

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.2.2 Summary Table of Phase 0 Procedures and Conclusions

Post Office 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 (Post Office) 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 was to profile the available case data for characteristics of interest in relation to the correct operation of the system.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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. *'25 IT users (at the time of test) 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 (configured within Horizon) for Horizon to automatically commit unprocessed transactions to the Branch Database tables. As part of the walkthrough testing performed, it was observed that Horizon is configured to automatically lock a user account after 15 minutes of inactivity, at which point the user is required to re-enter their user credentials. After a further period of 59 minutes of inactivity, Horizon is configured to automatically log the user out, ending a user session and committing any unprocessed transactions within a basket to the Branch Database. When next authenticating into Horizon, after being automatically logged out, the user is immediately presented with a till receipt confirming that the transactions had been committed to the Branch Database. From review of the printed receipt, an enhancement point was noted in that there is scope for the till receipt to include further detail to the user, highlighting that an unattended transaction had automatically been committed by Horizon to provide*

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	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 <specified user> between Live and Development, it is felt that there is a strong business need for this access for <specified user>. 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 theoretical 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 48 (0.0015%) session ids from a total of 3,124,140 which were out of balance based on the transactional data received. Those 48 session ids out of balance related to 18 distinct branches from 118 in total. The session ids out of balance were all pre system migration to HNG-X in 2010. The results after responding to the challenges in the original analytic were: a) *Analytic 1* –The analytic logic was revised following discussion with Fujitsu and following this revision there were no gaps in audit log

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	sequencing. b) *Analytic 6* – There was a logic error in the production of the extracts originally provided by Fujitsu. A sample of 15 items which were errored in the original data was investigated to confirm they were fixed when looking at the revised data provided by Fujitsu and confirmed the root cause was issues with the data extraction rather than the underlying data within the system. Given the original discrepancies in these analytics have been explained away, no further work against this area is recommended or required. 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 We have observed a theoretical risk in relation to this control. 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

Commented [A29]: Why would a recovery script ever be coded to do nothing? Is it not more likely for the risk to be that a recovery script is not written?

TO DISCUSS WITH LEWIS

MU – HAVE YOU DISCUSSED?

MAMW: I have – Have updated the wording. The insight no longer makes it to the Exec Summary. I think this is the correct balance.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.3 Phase 0 and 1 - 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 is 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 3.24.1 and 3.24.2 above.

Commented [A30]: Review references

MAMW: Check references spelling and grammar once this version has solidified.

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 Post Office Finance staff, which are then subject to Transaction Acknowledgement by Postmasters prior to being accepted into a branches accounts.

Fujitsu have advised that whilst there have been several hundred instances (circa 1,650) 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:

1. 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.
2. 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.
3. Fujitsu Support with access to post Balancing Transactions cannot amend the related audit files.
4. 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.
5. 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.

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:

1. 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.
2. Other 'Privileged Users' – At various layers of the Horizon infrastructure there exist accounts with privileged access rights which could be used to modify or insert data relevant to transactions at branches should they not be adequately controlled. For example a Privileged User account on the Oracle DB forming the nucleus

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 'Privileged User' risks:

1. 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.
2. Privileged User activity is monitored via log files which are transferred to the Audit Store following aggregation by the Event Management System which collects log files from across the Horizon estate. Regardless of this control, for transactions related to the Counter and Kiosks any attempt to insert transactions into the database by an individual with the privileged access rights to do so, would be identifiable due to the Digital Signature process applied to Message Journals from the Counter. To circumvent this a 'Privileged User' 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:

1. As discussed above Fujitsu highlighted that while the Balancing Transaction module has been used several hundred times in the past 7.5 years, only 1 of these uses has been a 'complex' Balancing Transaction. As described in our procedures below, Aanalytical procedures ~~could be~~were 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.

Commented [A31]: Has this not already been done?

MAMW: Yes, but this is the background section and that fact is then articulated within the tables below.

MU – CAN WE NOT JUST CHANGE "COULD" TO "WERE"?

MAMW – Amended.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.3.2 Summary Table of Phase 0 Procedures and Conclusions

Post Office Instruction	Procedures Performed	What we have discovered
Post Office 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 is 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 Postmaster knowledge, such as Global Users, and 'Privileged User' 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 – C1). 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. **Substantive**	**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 but 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 but 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: '*25 users (at the point of test) have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user*

Commented [A32]: Currently or over lifetime

MAMW: Added

JG - point about specific date/consistency of wording around 25 and 26 users repeated.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
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.	*'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. A direct observation of Fujitsu extracting Balancing Transactions was performed and supported that the population of Balancing transactions Fujitsu had originally extracted was correct. This direct interrogation of the data supported that there had been only one 'true' usage of Balancing Transactions for the available data period of HNG-X data (12/03/2010 through to 28/05/2016 when the testing was carried out). There were 1,644 Balancing Transactions utilised in total throughout that period, but the others were all used to update the Recovery Transactions flag in response to a known bug with the system where it frequently gets set to the wrong value. 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. Additional context around the usage of this tool was obtained from ticket review: a. The original TFS helpdesk ticket was obtained which is the legacy system used by Post office where branch incidents are recorded. The TFS ticket 2091569 was reviewed and it was noted that this had been raised by Anthony Vasse (Service Desk) on 02/03/2010 and transferred to Cheryl Card (SSC Product Specialist). Within the incident ticket it was noted that the after investigation the clerk had incorrectly doubled a transfer of stock of £4000.00 to £8000.00; therefore creating an incorrect loss to the branch of £4000.00. It was noted this issue was required to be fixed by 17/03/2010 as the branch was due to roll into

Formatted: Font color: Auto

Formatted: Normal, Indent: Left: 1.31 cm, No bullets or numbering

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	the next transaction period; therefore meaning that the branch required a fix to ensure the accounts were correctly recorded. An update was provided by Cheryl Card on 11/03/2010 confirming that the issue had been resolved using the transaction tool to insert transactions into the BRDB_RX_REP_SESSION and BRDB_RX_EPOSS_TRANSACTIONS tables to reverse the incorrect £4000.00 charge. The ticket confirmed that the Post Master had been advised to print a balance snapshot of the accounts before and after the transaction correction took place to ensure the transaction had been reversed correctly. A subsequent update was provided confirming that the balances had been correctly fixed. The ticket was subsequently closed on 04/04/2010. b. Evidence was obtained of the Peak Incident ticket raised in relation to this balancing transaction performed. Incident ticket 'PC0195561' was raised by Lorraine Elliot (Service Desk) on 15/04/2010 in relation to a Post Master attempting to transfer £4000.00 when the system crashed resulting in the post master being issued with 2 x £4000.00 receipts. ~~9.~~c. An OCP ticket was also raised which is the solution management system used by Fujitsu which tracks issues and resolutions. From this OCP reference 25882 it could be seen that the branch had performed a transfer out of stock for the value of £4000.00 but due to a system error this had incorrectly doubled in value creating an imbalance of £4000. Therefore, a balancing transaction of £4000.00 was required to correct the loss using the transaction correction tool. This was approved by Emma Langfield (Post Office) on 10/03/2010 at 15:33. From this OCP ticket, it could be seen that this incident was raised by Cheryl Card (SSC Product Specialist) on 10/03/2010 who subsequently performed the work and inserted the balancing transaction. **Substantive** 10. No issues noted

Formatted: Indent: Left: 2.44 cm, No bullets or numbering

Formatted: Indent: Left: 2.44 cm, No bullets or numbering

Formatted: Tab stops: 1.82 cm, Left

Formatted: Font: 9 pt

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.4 Phase 0 and 1- 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 is possible.*

4.4.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 3.24.1 and 3.24.2 above.

Commented [A33]: Check references

MAMW: Check when stable.

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:

1. Transaction initiation within either the Counter, Kiosk, or 'third party interface source', and subsequent interface to the Branch Database.
2. Archival from the Branch Database to the Audit Server.
3. Sealing of Audit Tracks via MD5 Message Digest and Archive to the Audit Store itself (Now based on Eternis technology).
4. Subsequent Retrieval of Tracks, validation via the ARQ (Audit Track Retrieval) process, and Investigator validation on the received data.
5. Non-Branch Transaction Data Records of Relevance

Commented [A34]: When did this change happen?

Do you need to revisit the Executive Summary which talks about MD5 being obsolete?

MAMW: No need to revisit. Just the hardware which has changed not the processes involved.

MU- SHOULD STILL INCLUDE DATE FOR COMPLETENESS

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

1. 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.
2. 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 mismatch between signature value and message content, would highlight downstream risks of data corruption.
3. 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
4. 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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

B. Archival from the Branch Database to the Audit Server

1. 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.
2. 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

1. 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.
2. 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.
3. Therefore once again both 'data at rest' and 'data in transit' controls are relevant to this stage of the process.
4. 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.
5. 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

1. 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 Post Office investigative staff.
2. There are a number of logical access controls operating over this process, including role based access mechanisms, a strict 'segregation of duties' from Post Office staff and audit logs over the process.
3. Upon receipt of the data files Post Office investigators carry out a number of additional checks themselves in order to validate the data integrity.

E. Non-Branch Transaction Data Records of Relevance

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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2.a. 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.

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

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

Formatted

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.4.2 Summary Table of Phase 0 Procedures and Conclusions

Post Office 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 is 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	**Controls** 1. No issues noted 2. Issue noted: '*25 IT users (at the point of test) 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

Commented [A35]: Currently or over lifetime?

MAMW: Context added.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
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.	6. See Appendix 5 for details of which controls have been subject to change.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.5 Phase 2

4.5.1 Work Performed, and Analysis Results

Our procedures centred on the workshops and documentation reviews highlighted in Section 3.1 above.

Commented [A36]: Check reference

MAMW: to finalise at end.

In particular the following procedures were central in each case to our understanding:

Scope Area 1 – Audit Logs for Privileged Users

1. A work shop was conducted with Fujitsu in order to discuss Privileged Users, audit logs, and the controls thereon.

Scope Area 2 – Analytic 1 and 6 Follow Up

1. Workshops were conducted with Fujitsu in order to determine the relevant root cause in each case.
2. Where necessary additional data was requested.
3. Analytics were re-run with revised logic and the issues found in the original analytic were found to have been rectified by the changes made in each case.

Scope Area 3 – Non-Counter Initiated Transactions

1. Technical documentation was reviewed in order to determine the nature of ~~non counter~~non-counter transaction process flows, the related risks, and the responding controls for the three ~~non counter~~non-counter transaction sources (Camelot, Paystation, Post and Go).
2. A workshop was held with Fujitsu in order to validate this understanding.
3. A memo was produced highlighting the proposed recommended procedures, which was then translated into Phase 3b scope and approach.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.5.2 Phase 2 Procedures

Performed Procedures

Procedures	Findings
Scope Area 1 1. Perform workshop with Fujitsu in order to ask further questions around Privileged Users, and determine scope for future meetings.	**Scope Area 1** 1. The workshop was held and an approach adopted whereby Fujitsu produced a report on Privileged Users for future review (See Phase 4). Some basic findings were determined around the audit logs operating over Privileged Users in order to support with these determinations: a. Regardless of access rights to amend and delete audit logs, the digital signature controls should still allow for the detection of data which had been modified, deleted or inserted subsequent to receipt from the Counter. b. There are a limited number of users who could theoretically, due to a segregation of duties breach between database administration and the key management server, amend the Message Log for one or more Counters in one or more branches and make the transaction/s amended, look legitimate when it is retrieved from the audit store (through spoofing of the digital signature). c. However to do this would require an existing systems administrator with a large amount of technical expertise and systems knowledge, it would almost certainly require a program to be installed onto the Horizon online system, and a release process would have to be bypassed in order for this to be installed maliciously (and avoid file integrity checking controls operated by Fujitsu).
Scope Area 2 *Analytic 1* 2. Workshops were performed with Fujitsu in order to determine the root cause in the gaps in sequencing highlighted by the original analytic. 3. The analytic was re-run with revised logic to determine if the correct root cause for	**Scope Area 2** *Analytic 1* 2. There was an error in the original analytic logic which was supposed to remove duplicated transactions from the dataset but was in actuality removing both the duplicates and the original transactions from the data.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
the gaps had been determined for these 25 data items. *Analytic 6* 4. The original data for the 480 session IDs which were noted to be out of balance were investigated. To do this a sample of 15 out of balance session IDs were selected for further investigation with Fujitsu support. 5. Root causes for the original data appearing to show a branch as being out of balance were determined. 6. A workshop was performed with Fujitsu and the data provided to support for all 15 items the established root cause was responsible. **Scope Area 3** 7. A variety of Fujitsu technical documents pertaining to the Horizon system were reviewed in order to understand the dataflowsdata flows for ~~non-counter~~non-counter transactions, and identify the relevant risks and areas of control. 8. An approach memo was produced highlighting the relevant approach details and used as the basis for Phase 3.	3. When the analytic was corrected for this it was noted that there were no gaps in JSN sequencing were identified based on the data provided. *Analytic 6* 4. The root cause for the 480 transactions appearing not to balance was determined as: a. Some of the audit log sequences were missing a start time and hence were not extracted properly. b. Some of the audit log sequences were missing a SC (Serve Customer) record and hence were not extracted properly. 5. These issues were shown to have been overcome by looking at the raw audit log sequence data (as it was the extraction logic performed by Fujitsu which was causing records to be dropped). 6. It was confirmed through the walkthrough with Fujitsu and through checking the 15 sampled files independently that there were no session ids out of balance based on the new transaction data provided and it was concluded that the out of balance session ids identified on the initial run through were out of balance due to the 2 errors identified above in extracting the data from the raw audit log sequence. **Scope Area 3** 7. The technical documents were reviewed, analysed and used to highlight the controls and risks as documented in Appendix 8. 8. An approach memo was produced and utilised in formulating the scope for Phase 3. 9. The review performed highlighted that the key area of risk was in ensuring Postmasters had adequate visibility of the data being received from systems external to Horizon and were in a position where they could reconcile the Transactions Acknowledgements they received back to the data captured on Camelot, Paystation and Post and Go devices at source.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.6 Phase 3

Scope Area 1: *Are there any haps in the controls around non-counter initiated transactions that could call into question the integrity of the data generated in relation to these transactions?*

4.6.1 Work Performed, and Analysis Results

In commissioning this work Post Office asked for a Deloitte viewpoint on the below questions which we have provided:

1. Are there any gaps in the controls around ~~non-counter~~non-counter transactions that could call into question the Integrity of the data generated in relation to these transactions?

   The first potential area of interest from a controls perspective in relation to the completeness and accuracy of the flow of data, is around the sending, processing by, and subsequent receipt of data from third parties. The primary control in relation to this is the requirement for Postmasters to 'Transaction Acknowledge' such data before it is accepted into their accounts, but the formalisation of the processes and controls ensuring Postmasters reconcile their financial position accepting transactions has not been enforced. Reviews of the supporting documentation primarily from the Horizon Online Help references a number of reports which are available to facilitate this and Post Office has represented that Postmasters can reconcile data received from third parties...

   Originally it was theorised there was a second key area of interest, being that no digital signature is applied to ~~non-counter~~non-counter transactions, potentially opening up this category of transactions to greater risk of interference subsequent to processing into the BRDB (as the digital signature control is the primary control preventing this). However, further discussion with Fujitsu established that when the BRDB receives ~~non-counter~~non-counter transaction data, it pushes it down to the counter for acceptance by the Postmaster, at which point the Counter digitally signs the acknowledgement of the transaction and therefore in theory a reconciliation between these digitally signed TAs and the raw data files received from the third parties (which are interfaced into the Audit Store) should also be possible mitigating this risk.

2. If there are gaps:

   a. Could they be the cause of discrepancies in branch accounts (or could they mean that errors in Horizon would not be revealed and those errors could then be the cause of discrepancies in branch accounts); and

      Theoretically they could – if a third party incorrectly reflected the data they had received from a non-Counter system, and this incorrect total was then downloaded into the Branch accounts, then in the absence of formal controls to reconcile data transmitted to the third party, back to data received, the branch could, theoretically, cause discrepancies in the branch accounts. The control which Post Office relies on to mitigate this is the Transaction Acknowledgements.

   b. What is the risk of those gaps (or resulting discrepancies) materialising?

      Without a full investigation of the controls at the third parties, and any other mitigating controls which may exist, it is difficult to quantify the risk exposure.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.6.2 Phase 3 Procedures

<table>
<tr><th>Procedures</th><th>Findings</th></tr>
<tr><td>Hold an initial workshop to corroborate understanding of data flows and validate the existence and completeness of controls over the current reconciliation process, and how Transaction Acknowledgements are utilised</td><td>This workshop was performed with Fujitsu on the 9th May 2017.

As a result of the workshop the understanding that Deloitte had originally obtained on the operation of the interfaces between the systems was validated with a couple of amendments. The attached diagram (Appendix 8) displays the finalised viewpoint in relation to the ~~dataflows~~data flows.

As part of this review the decision to exclude ATMs from scope as ~~non counter~~non-counter transactions was examined and it was highlighted by Fujitsu that all interactions between ATMs and the Counter/BRDB are by rekeying of the data – i.e. this is not a system driven process. Therefore the original decision to exclude ATMs from scope was adhered to.</td></tr>
<tr><td>Review and test key reconciliation controls between key data sources within the data flow</td><td>Fujitsu discussion highlighted that one of the controls identified for potential testing was only operated temporarily during the switch from Riposte to the Branch Database, and as a result no control exists to test in the present day. The remaining two controls are legitimate controls to test, as they are currently worded, and one requires a wording tweak in order to test.

The below table captures the controls in scope, and the required updates to the original control wording where required:

<table>
<tr><th>#</th><th>Summary Control Wording</th><th></th></tr>
<tr><td>1</td><td>External transactions sent via PODG such that the External Transaction files that are currently sent from Ingenico (PAYSTATION) and Wincor Nixdorf (POST&GO) are routed to the Branch Database as well as sending the data to the Credence system. There is a reconciliation between Credence and BRDB.</td><td>Not an existing control. TPS – BRDB is a rec, not Credence – BRDB.

Update final sentence of control wording to ‘There is a reconciliation between TPS and</td></tr>
</table>
</td></tr>
</table>

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings		
			BRDB'.
	2	For each Transaction Acknowledgement generated, a new transaction pair is created for POLSAP. The transaction delivered to POLSAP will have a Reference number that matches the reference number used in the Transaction Acknowledgement record generation. This allows POLSAP to match with the Transaction Acknowledgement once the TA has been accepted by the Postmaster.	Control exists.
	30	AP Client File Reconciliation APSS2222.ksh will reconcile the data in the files that it delivered to a Client with the data in the files that Credence delivered to a Client.	No longer an existing control – no further testing to be performed.
	31	TPS to AP Reconciliation TPSC227 writes APS transaction data to a formatted file that will later be used by the APS host program APSC2051 to reconcile data from TPS with that from APS.	Control exists.
Perform detailed walkthrough of the Transaction Acceptance (TA) process to confirm the granularity of the information the Postmaster is provided with. Perform procedures to corroborate a TA is required for all ~~Non Counter~~Non-Counter Transactions.	Detailed analysis of the TAs process was conducted through the following steps: 1. Review of Horizon Online functionality within the Model Office at Finsbury Dials on 29/03/2017 with assistance from Mark Underwood		

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	and Phil Jeary. 2. Confirmation via review of the system screens that the Horizon system included TA functionality relating to all of the ~~non counter~~non-counter transaction areas under review, including: a. Post and Go; b. Paystation; and c. Camelot. No evidence was witnessed during this review, that there were other transaction types for which TAs would apply, although this should not be construed by the reader to categorically mean other ~~non counter~~non-counter transactions for which Transaction Acknowledgements would be processed do not exist. To provide fuller assurance over the completeness of the transaction population for which TAs are produced and relevant a detailed review of product types, and the related population of transaction types, would be required, and this was beyond the scope of this piece of work. 1. Walkthrough of the receipt and processing of Transaction Acknowledgements on the Model Office test system. This walkthrough highlighted the following key points: a. On Receipt of a TA the Postmaster is able to review both at a header and line level of granularity. b. On Receipt of a TA the Postmaster must complete the processing of it, before trading can continue. c. If the Postmaster disputes the TA, then the TA ID should be noted to dispute with the helpline after the TA is processed (this could then trigger a further Transaction Correction). 2. Review of the Model Office counter for each of these transaction types, in particular the Horizon Online Help Guide pages (which are available within the system to all Postmasters), confirmed that various reports on the balances are available to allow reconciliation between the terminals involved and the TAs received and values within the Branch Database, as well as guidance on the usage of TA functionality. Below is a summary of the findings against each of the three transaction types

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	which have been represented by Fujitsu and Post Office to formulate the population of non-counter transaction types for this work. *Paystation TAs* The following sections of the Horizon Online Help Guide were reviewed: *'Paystation Transaction Acknowledgements'* This is a ten page document which upon review provides guidance on: 1. What TAs are. (Page 1) 2. Accounting for TAs (page 2) a. Including having to reconcile / check against all Paystation transactions. 3. Non Receipt of TAs (Page 3) 4. Receipt & Processing TAs (page 6) 5. Including guidance on checking/reconciling the TAs against Paystation transactions 6. Office Daily Reports (Page 9) a. Including details of a 'Outstanding & Processed TAs' report that is available b. This report gives detailed information on all TAs that have been received over the last 40 days and their existing status. c. "There are no audit requirements for you to print and retain this report. However you may find it useful if you need to verify information contained within the TAs against any terminal reports"

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings

	'Accounting and Balancing Instructions for Paystation'
	
	This is a four page document, which upon review provides guidance on:
	
	1. What a TA is (page 1)
	2. Reconciling transactions from Paystation against the TAs
	
	Post and Go TAs
	
	The following section of the Horizon Online Help Guide was reviewed:
	
	'Transaction Acknowledgements for Post & Go'
	
	This is an eight page document which upon review provides guidance on:
	
	1. What a TA is in relation to Pay & Go (Page 1)
	2. Daily processing of a trading report at close of business & prior to business the next day to compare against TAs received. (Page 2 & 3)
	3. Non Receipt of TAs
	4. Receipt and Processing of TAs (Page 6)
	    a. Including recommending all Post & Go transactions are checked/reconciled against the TAs received.
	5. Office Daily Reports (Page 7)
	    a. Including details of a 'Outstanding & Processed TAs' report that is available:
	    b. This report gives detailed information on all TAs that have been received over the last 40 days and their existing status.
	    c. "There are no audit requirements for you to print and retain this report. However you may find it useful if you need to verify information contained within the TAs against any terminal reports"
	6. TA Accounting Arrangements (Page 8)

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	a. Including recommendation to check and reconcile the cash against the TAs received the following working day. *Camelot TAs* The following section of the Horizon Online Help Guide was reviewed: 'Transaction Acknowledgements for Camelot' This is a three page document which upon review provides guidance on: 1. What a TA is. (Page 1) 2. Accounting instructions for TAs a. Including check and reconcile the cash against the TAs received the following day (Page 2) 3. Non Receipt of TAs (Page 2) 4. TA report (page 3) *Additional Sections of Horizon Online Guide Identified as of Relevance* In addition to the above it was confirmed that there is a help page within Horizon Online Help providing contact details which Postmasters can use should they have issues with Transaction Acknowledgements for Paystation. This page was entitled Contact Names, Addresses and Telephone Numbers' and was two pages long. 1. To supplement these procedures further a review of additional sources of process narrative and guidance were obtained and reviewed from Post Office staff. The documents reviewed as part of this further exercise were: a. 'Self ServeSelf-Serve Kiosk User Guide V4.1' b. 'HNG Branch Trading Reports 310317'

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	c. 'HNG BT Balancing and despatch of docs 310317' d. 'HNG Camelot Lottery On-line games 030417' e. 'HNG Camelot Scratchcard games 030417' f. 'HNG Cash and Secure Stock Rem Services 310317' g. 'HNG Equipment and Admin Pages 310317' Review of these documents, highlighted a number of areas which provided additional context/assurance: *Guide 'HNG BT Balancing and despatch of docs 310317'* This document makes reference to an 'Office Snapshot Report' and details how to create the report, but does not explicitly say this can be used to reconcile against TA's: 1. 'Producing the Office Snapshot report to list stock and cash on hand and all the transactions carried out during the current Branch Trading Period up to the time the report was requested, for all stock units in your branch.' (Page 109) *Guide 'HNG Camelot Scratchcard games 030417'* This document has a section that details account of scratchcards. This section highlights that National Lottery transactions are accounted for via Transaction Acknowledgements and that a Camelot terminal creates a report which shows: 1. The total daily scratchcards sales 2. The daily prize payments 3. Any returns 4. Commissions (this figure will always be zero) However the guide does not explicitly say that this report that shows all ~~non counter~~non-counter transactions for National lottery should be reconciled

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	against the TA which accounts for National Lottery transactions.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.7 Phase 4

Scope Area 1: *Deloitte review of Fujitsu Report in conjunction with initial comments raised.*

4.7.1 Work Performed, and Analysis Results

For this specific scope area our procedures centred on reviewing the Fujitsu report in conjunction with the comments raised, and providing commentary on residual question areas or concerns back to Post Office.

Subsequent to these procedures a workshop was held with Fujitsu staff, whereby residual questions and concerns were dealt with.

These procedures confirmed that a Privileged User would, theoretically, be able to amend data in a manner where it looked legitimate, and delete the audit trail of them carrying out such activity with minimal footprint. The technical hurdles that would need to be overcome would be significant, and the user in question would likely require access to a programme to do so. The Privileged User would then be required to locate the programme on the correct hardware, and Fujitsu have pointed to the state monitoring software which should detect if unauthorised programmes have been added to the relevant hardware, whilst recognising this is not a formal control.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4.7.2 Phase 4 Procedures

Procedures	Findings
Deloitte review of Fujitsu Report in conjunction with initial comments raised.	This review has been performed with an email provided as per the agreed deliverable in the Statement of Work.
Workshop with appropriate Fujitsu resource to: 1. Answer any outstanding comments / questions on the report. 2. Produce a detailed commentary on what steps would need to be taken to replace the message log, as per section 2.2 of the Fujitsu report. We have also produced section (c), which includes, as requested recommendations on the further work to be performed in relation to the Fujitsu report.	A workshop was held on 11/05/2017 with attendees from: - Deloitte (Mark Westbrook, Lewis Keating) - Fujitsu (Torstein O'Godeseth, Gareth Jenkins) - Bond Dickinson (Jonathan Gribben, by telephone) **a)** The following agenda items were discussed, with Deloitte asking the numbered questions (in black), and Fujitsu providing responses (*In red italics).* **Horizon Online** 1. Is the segregation of duties breach between database administration and the key management server, the only way in which a weakness could be exploited to overwrite transactional information in a way where it cannot be traced and looks legitimate to the system? It is the only way known by Fujitsu staff. Fujitsu do however stress that there are numerous levels of security which would make any way to break through very difficult. 2. Is 1am the following day stipulated as the date and time by which overwrite would need to be achieved by due solely to the audit store, and if so are there other more timely data feeds which would highlight a discrepancy between actual 'transactional reality' and what is recorded in the Audit Store or the BRDB? Yes, 1am is when 'harvesting' of data from BRDB to the audit store happens (the job is scheduled to run at 1am, so actual harvesting is likely to happen in the minutes after this time). Therefore the maximum time slot for manipulation would end at 1am. In reality there are other interfaces which occur on a more frequent basis, (which would leave a footprint on another system / part of Horizon) however only certain products are involved in these interfaces (mainly transactions which

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	settle with clients, and are recorded in somebody else's system). Therefore any manipulation would have to avoid these specific products. This adds another layer of complexity, theoretically however these transactions in the session could be replaced 'correctly' (like for like), and not leave a footprint if done before 1am. 3. For step 6 of the replacement routine, can you remind us the technical reasons for requiring access to the BAL Private Key? The BAL private key signs messages which come from the counter. If you are going to create a fake counter key, you need the correct BAL private key to make the digital signature look legitimate. 4. On step 9 on the Privileged User audit log – how long can this log be edited by the Privileged User? Same 1am window before transmission to the Audit Store? Also a reminder that it is the hardware protection rather than the digital seal which is important on the Audit Store due to the usage of the cracked MD5 algorithm for sealing? It is a daily pull occurring at around 1am, therefore the window is as previously described. 5. On the point on editing the log, if I'm reading correctly it would always be possible to see the last action by the Privileged User, even if they deleted all else? Can we be provided with further detail on how this would work – In order to make the changes to the Message Log described in section 2.2, the Privileged User would need Read access to the Key Store database which runs on the NPS and Read / Write access to the BRDB. Note that should the rogue application run on the BAL, then this isn't necessary as the BAL's have access to the Key store based on the IP address. You can always see the last action by a Privileged User, if a Privileged User deleted their actions, it would always leave a footprint of the deletion of logs. They could theoretically remove what they have done, but they cannot remove that they have done something.

Commented [A37]: ?

MAMW: Referring to previous sentence.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	Fujitsu note that turning off audit logs completely will 'break' the application. A 'Delete' record on the audit trail is likely to be highly unusual & easy to spot. Please see Section (C) for suggested procedures around this. It also recommended procedures are performed to validate that the audit logging feature cannot be turned off without breaking the application. a. Could a Privileged User (theoretically) cover their tracks completely by removing log on / log off activity from the audit log without leaving a trace? If not how feasibly is a comparison between all log on/ log off activities of Super-Users' and MSCs in order to detect un-authorised access? As above in answer to question 5, they would always leave a trace. It is noted that log on / log offs by Privileged Users on BRDB / BAL are likely to be very rare (limited to system upgrades) and should always be approved by an MSC (record of the reason Super-User access is required and approval for this access). Please see Section (C) for suggested procedures around this. 6. Although the Database Audit tables are not regularly examined they were recently checked as part of an external Audit of Horizon Online. – Could you provide further context on this audit? What was checked and why? Fujitsu have confirmed that NCC Group conducted an audit of HNG-X security in 2014 and PCI DSS audits are conducted annually. Further detail on the coverage of these audits of the database audit tables has not been provided. 7. How often would the individuals who contravene access SoD between the NPS and BRDB tend to logon to the NPS? Also does the point raised on not needing to logon with access to the BAL broaden this concern? Fujitsu advised they would not expect Privileged Users to log onto the NPS on a regular basis (limited to upgrades /

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	changes etc). 8. For step 2, how big is the average message log associated with any log on session. (i.e. is a log on session generally all day and therefore the message log will hold thousands of transactions?) Normally 2-3 hours if not all day. (Some quiet post offices it would be notably less) A log on session likely to be hundreds / thousands of lines. (1 audit line for every customer been server plus few extras for printing reports etc.) However even if a session was a small number of lines, a program would still be required in order to effectively amend transactions without leaving a footprint due to the complexity of re-creating the digital signature for 1 transaction / locating a suitable transaction. 9. For step 4, are there any barriers to uploading this application onto Fujitsu systems (if this would be required). Presumably this would be required due to the volume of work required? There is a detailed release process which all releases should follow. However there are no preventative logical access controls preventing a user from releasing programmes outside of this process. However if someone tried to not follow this process then File Integrity monitoring is in place on BRDB & BAL. This checks if files appear on a platform and flags things which have changed, the security ops team then investigate. Please see Section (C) for suggested procedures around this. 10. On step 8, is there a formal control operated by Fujitsu which can be referenced which would provide evidence for 'any instance of slow running on the system would be investigated by the support teams'. If not can we articulate how obvious this would be to evidence it would be picked up in BAU activity? Fujitsu noted that if the system behaves poorly this would be very obvious to Fujitsu employees who monitor system

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	performance on an ongoing basis. **Riposte** 1. The Riposte product managed the Message Store and it did not allow any message to be updated or deleted. – Is there any further information available on this control? Each message also had an associated CRC, this was basically a checksum that was included to ensure that the message had not become accidently corrupted. Note that this was not a cryptographically secure seal and it would be possible for a sufficiently technically skilled person to alter a message and recalculate the CRC if they had access to the message outside the message store. – i.e. the level of protection on Riposte was lower? The message store was a specialised database designed so that all you could do was add messages on, not amend messages. There is no known loophole by Fujitsu to amend transactions due to the nature of database. As soon as messages arrived centrally, they were copied into audit trail immediately. 2. The Digital Seal for the Riposte Audit Store remained the same as for Horizon Online – i.e. MD5? And the hardware protection was applied the same as well? Yes 3. Due to the size of the Post Office Network, branches were split into 4 separate Clusters. Each Cluster included 4 Correspondence Servers (2 in each Data Centre), thus ensuring that there were normally 4 copies of the data held in the Data Centres. – Does this mean you would need to duplicate corrupted data across 4 servers? To inject rogue transactions theoretically a user would inject artificial messages into Riposte, as they could not amend messages due to this replication.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	4. In Detecting Changes to the Audit Trail the following is stated, however, if such data were injected at the Correspondence Server, it would be clear that this had occurred since the Node Id associated with the message would be that of the Correspondence Server at which the message had been injected and not a normal Counter Node Id. This would be clearly visible in any audit extract. Could this not be spoofed? Would need to run application on the counter remotely to inject transactions from the counter. "Very difficult but not impossible". (This was not a Fujitsu owned system, source code owned and managed by another third party. As Fujitsu did not own or manage the source code, changes to the source code of the system would have to be applied by the third party, this adds another step of complexity in running a rogue application). **(b) Detailed commentary on what steps would need to be taken to replace the message log, as per section 2.2 of the Fujitsu report** In theory, a Privileged User, could amend the Message Log for one or more Counters in one or more branches. The following describes what would be required to replace the Message Log for a single counter in a single branch. This process could be repeated for multiple counters / branches if required. 1. To exploit this, the work would need to be completed before 1am the following day (since the Message Log is extracted from BRDB at some point after 1am each night and the data is then sealed and held in the Audit Server). As such there is a limited window of opportunity. A log on session can last up to all day for a counter in a branch, and is essentially how long the counter machine is 'logged into' in any one sitting. If a branch is still logged into a session, and performing transactions in that session whilst someone was attempting to amend the transactions in the BRDB there are likely to be additional complications around maintaining JSN continuity and order, and ensuring the digital signature for all transactions in the session are valid and 'match'. 2. The entire Message Log associated with a Log On Session that is to be corrupted would need to be replaced,

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	as a new Counter private key would need to be generated, and as such all messages would need to be signed by this key. *This is because there is no known way to obtain the counter's Private Key and so a new one would need to be generated as described below.* 3. The records being replaced would have to correspond on a one-to-one basis to the original records otherwise there would be gaps or duplicates in the sequence of JSNs which would then be detected as part of the Audit Retrieval process. There is an estimated 1 to 1 ratio between 'records' and transactions, as such there can be hundreds of transactions in any one session; all of which would need to be re-signed. Amending or replacing certain records relating to transactions which are involved in more regular interfaces from BRDB such as third party systems would have to be specifically avoided (or replaced on a like for like basis – this is replacing the transaction with a transaction which matches it exactly) otherwise they would trigger errors in other reconciliations; this adds an additional layer of complexity to this process. 4. An application / programme would need to be run by a Privileged User in order to correctly construct the revised Audit Records due to the high level of complexity involved in generating new private keys / digital signatures, and the volumes of transactions these would be required for within the time limitations noted in point #1. There is a release process which would have to be bypassed in order to get an application / programme onto the relevant systems. It is expected file integrity monitoring / checks would identify if a user attempted to introduce a rogue application / programme onto the relevant systems. 5. This application would need to generate a Private / Public key pair similar to the one originally generated by the counter. Called an "Attack Counter key" in the rest of the document. 6. The application would need to have access to the BAL's Private Key. Since this is stored in the Key Store which is an Oracle Database running on the NPS, then it is assumed that a Privileged User would be able to read this value and make it available to the application. This would then enable the application to generate a Log On Message Log message containing the fake Counter Public Key and to sign it using the genuine BAL

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	Private Key. 7. All subsequent messages for the session would then need to be amended as required and then re-signed using the Attack Counter Private Key generated at step 5. An application would be needed to do this due to the high complexity. 8. Having constructed all these false Message Log messages, the Privileged User would then need to delete all the genuine messages from the Message Log in BRDB and replace them with the false messages on a one for one basis. 9. Note that as stated earlier, corrupting the Message Log in this way has no impact whatsoever on the Branch Accounts, since these never refer to the Message Log. The Branch Accounts are based on copies of some of the data held in the Message Log being stored in "working tables" within the BRDB. Clearly any application that is capable of corrupting the Message Log in BRDB would also be capable of updating (i.e. corrupting) the data used to calculate the Branch Accounts. Therefore the above steps, if followed, could theoretically amend the audit store record without leaving a trace, however there would be no impact on branch accounts unless a programme was also configured to make the same amendments to data used to calculate Branch Accounts in order to impact on branch accounting. This adds another layer of complexity to this hypothetical and unlikely scenario. **(c) Recommendations on the further work to be performed in relation to the Fujitsu report.** 1. As per section (a) question 5 above, it is suggested that the following procedures could be performed: a. Identify how far back Privileged User activity on the BRDB / BAL audit logs are held for b. Obtain audit log records for as many years back as possible c. Perform an analytic procedure over the log's to identify:

Formatted: Highlight

Formatted: Normal, No bullets or numbering

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedures	Findings
	Any DELETE record (there should be a very low volume / if any of these) Any log on records to the BRDB / BAL by Privileged Users and match these to an MSC to confirm the actions were known to the business, planned and approved. Validate that switching the audit logging off would 'break' the application. This would provide information as to whether there have been ANY tampering of transactional data (through DELETE audit record) (for the period data is available). This would also identify if there have been any un-authorised accesses to BAL / BRDB by Privileged Users or whether all access was authorised (for the period data is available). 2. As per section (a) question 9 above, it is suggested that the following procedures could be performed: a. Obtain documentation to evidence a detailed release process is in place which all changes to systems (including introduction of applications / programmes) should follow. b. Identify and test the file integrity monitoring controls in place which would identify if the release process had been bypassed c. Obtain documentation to evidence the escalation process in place for items flagged by the file integrity monitoring checks.

Formatted: Highlight

Formatted: Normal, No bullets or numbering

Commented [A38]: Can these be moved to the recommended further procedures section or deleted if it is already included there

To be deleted and moved to standalone doc

MAMW: TO BE ACTIONED

MAMW: Now actioned.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

5. General Assumptions and Limitations

5.1 General 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 unless stated in this report;
2. For scope areas across all Phases, only matters relating to Horizon Features[2] 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). These third parties have been limited to Fujiitsu and Accenture. ~~, and QCs we met with under your instruction~~;
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 technical documentation ~~information~~ available, relating to both the granularity of information and the existence of the Horizon Features over the entire timeline of operation of Horizon process documentation. The effect of which is that there are 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[3] 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, and audit store 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 a view as to whether the control was likely to have operated at the time of the allegations.

Formatted: Highlight

Commented [A39]: I do not think this is an entirely accurate statement. Presumably this is boiler plate text that needs to be reviewed.

MAMW: ANDY ARE WE OK TO DELETE? I THINK THIS IS A HANGOVER FROM ZEBRA WHEN WE DIDN'T ACTUALLY DO ANY TESTING

AW - This is true of a lot of the information but not all. I have suggested an amend

MU COULD WE TURN THIS ON ITS HEAD?

MAMW: Have spoken to Andy and we cannot flip this on its head as will require a complete report rewrite

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Commented [A40]: Is this a defined term?

Defined below - need to define here

MAMW: Have defined the term

Formatted: Highlight

Commented [A41]: Is this entirely accurate?

MAMW: ANDY?

This is how our work has been set up. We have provided statements related to the accuracy of the system but these do not constitute an opinion as defined in auditing standards which would be a natural inference for a reader to make as we are often viewed as being an "Auditing" firm. We therefore always exclude the making of an opinion unless it is formally under an auditing standard.

Could amend from "any other opinion" to "assurance opinion" if that helps.

Formatted: Highlight

Formatted: Highlight

Commented [A42]: QCs?

MAMW: Added.

JG - We shouldn't refer to meeting with QCs in the report for privilege reasons. I think this section is focused on third parties who could contribute to the issues.

MAMW: Amended then to reference Fujitsu and Accenture.

Commented [A43]: As per previous comment. Any gaps needs to be called out explicitly i.e. what information that you requested were we / FJ not able to provide??

MAMW: I think this would likely require a document in itself. Left as is for now!

[2] "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 Postmasters; and
- Audit trails kept by the system are complete and accurate.

[3] Since its implementation in branches, Post Office 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Appendix 1

Documents Reviewed

Commented [A44]: Does this cover all four Phases of work?

MAMW: It should do but to be checked

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~~Branch Database support guide
DEV/APP/LLD/0199	Schema definition for ~~branch database~~Branch Database, standby ~~branch database~~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
DES/APP/DPR/0006	Design Proposal for Transaction Acknowledgments
EA/IFS/006	Application Interface Specification
SVM/SDM/SD/0020	End to End Reconciliation Reporting
REQ/APP/AIS/0004	Transaction Acknowledgements Application Interface Specification
N/A	Post Office Pay Station Manual
N/A	1- Self Serve Kiosk Guide
N/A	HNG Branch Trading Reports 310317
N/A	HNG BT Balancing and despatch of docs 310317
N/A	HNG Camelot Lottery On-Line games 030417
N/A	HNG Camelot Scratchcard games 030417

Formatted: Highlight

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Document Ref	Document Title
N/A	HNG Cash and Secure Stock Rem Service 310317
N/A	HNG Equipment and Admin pages 310317

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Individuals Interviewed

Name	Job Title
Patrick Bourke	Post Office – 'Bramble' Project Manager
Mark Underwood	Post Office – 'Bramble' Project Manager
Rodric Williams	Post Office – Post Office Legal
Rod Ismay	Post Office - Head of Finance Service Centre
Lorraine Garvey	Post Office - Enquiries Manager
Sarah Haywood	Post Office - Finance Team Leader
Tracy Middleton	Post Office - Finance Team Leader
Paul Smith	Post Office - Operations Support Manager
Lorna Evans	Post Office - Central Data Manager
John Willacy	Post Office – Financial Control Framework Manager
Neil Page	Post Office – Client Settlement Team
Gillian Hoyland	Post Office – Operational Support Manager
Joy Lennon	Post Office – Master Data Manager
Andy R Pearson	Post Office - Finance
Debbie Gratton	Post Office – Finance
Stuart Nesbit	Post Office – Finance Director
Phillip Jeary	Post Office - Finance
Jon Hulme	Post Office – Domain Architect
Shirley Hailstones	Post Office – Support Services Resolution Team Manager
Katherine Alexander	Post Office – Support Services Resolution Team Manager
John Simpkins	SSC Team Leader
Paul Stewart	Fujitsu – Database Administrator
Ken Westfield	Fujitsu - Change Manager
Michael Greene	Fujitsu – Support Technician
Michael Harvey	Fujitsu - Head of Commercial
Pete Newsome	Fujitsu - Business Change Manager
Torstein O'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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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.
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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Ref	Control Description
	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 • 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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Ref	Control Description
	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 columns on the table are named in the SQL • Check that the values to be inserted are provided by a SELECT … FROM dual, (SELECT … FROM … WHERE) i.e. not a VALUES • Check that if any of the name/value pairs that are listed in the BRDB_TXN_CORRECTION_ENFORCED_VALUES configuration parameter are present on the table, they are set to the listed value.
O	Balancing transaction audit files (BRDBC033), unlike the files produced by BRDBC002, are not compressed, but are still encrypted.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Ref	Control Description
	• Summary of messages that have failed individual message integrity checks Any failure of the data integrity checks will not prevent subsequent execution of the query. The audit workstation user will be warned of the failure via the server process status notification mechanism.
K	As Audit tracks are retrieved from the archive, they are seal checked (by re-application of the MD5 message digest function) to ensure that the source data has not been tampered with while it was stored in the archive.
L	Only authorised users may access the Audit workstation applications. Authorised users are required to log on to the workstation using two factor authentication and the HNG-X Identity Management system. An Active Directory group 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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	Post Office 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 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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.
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	N/A - see change to left	N/A - see change to left

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
						same file as previously - i.e. via Transaction Acceptance.		
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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	No	-	-	-		Source code was reviewed at a point in time. Please refer to 1.1-1.5.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		supports the key inherent control operation around:						
1	5a	Refer to control 1.1						
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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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.)	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure
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	No	-	-	-	Yes	Fujitsu represented that no such equivalent role or ability to remote access onto counters

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		Role of ADMIN cannot log onto to any Branch other than Global (Including Remote access controls to branch infrastructure (e.g. Counter)).						existed in Riposte.
2	9	Review a sample of the full population (already extracted by Fujitsu - 7.5 years) of balancing transactions to validate the branch was aware of their usage / no transactional postings were made in the balancing transaction.	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure	N/A Data Procedure
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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		"OPS$SUPPORTTOOLUSER".						
2	5c	The PL/SQL package PKG_BRDB_TXN_CORRECTION will execute with the permissions of the OPS$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.
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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		column values specified in the template should not be changed – these are annotated with comments as appropriate.						
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						
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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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	No	-	-	-	N/A	It is not known whether Balancing Transactions (or equivalent) and associated tool existed in Riposte.
2		./BRDBX015.sh MyTransactionFile.sql 2001						
2		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.						

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	No	-	-	-	No	JSN check in its current format did not exist in Riposte. However Fujitsu assert that a data density check was applied.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		the count of missing sequence numbers. Duplicate records 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		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						

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		validation provides security in case the privileges are not correctly set up.						
		• Check that all the columns named in the SQL exist on the table, and that all the columns on the table are named in the SQL						
		• Check that the values to be inserted are provided by a SELECT … FROM dual, (SELECT … FROM … WHERE) i.e. not a VALUES						
		• Check that if any of the name/value pairs that are listed in the BRDB_TXN_CORRECTION_ENFORCED_VALUES configuration parameter are present on the table, they are set to the listed value.						
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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		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							

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
								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.
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	Yes	R10.20 (Refresh of Eternis Storage infrastructure)	Release notes obtained and reviewed. Seen to document various management reviews /	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	N/A - see change to left	N/A - see change to left

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		allegations.			approvals and testing steps.	created in the branches at the time that transactions were carried out were persisted and 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	1c	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.	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 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.						

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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.
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)	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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
		• Modifications to system configuration (Inc. software configuration and account details) • System start up and shut down • Recovery actions • Exception conditions • Change of user rights						
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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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.
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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	3c	Post Office 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:	No	-	-	-	-	-
3		• Completeness of data – contiguous message sequence numbers					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		• 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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		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.
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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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						

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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	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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Appendix 6

Case Data Analytics Overview

The below analytical procedures were performed on 'Case Data'. 'Case data' refers to transactional data provided by Post Office, 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	Post Office Instruction	Proposal	Relevant Analytics Procedures	Analytic
1	Post Office 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 is 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.	Post Office 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	Identify branches which are out of balance based on transactional data available (should not be possible based on inherent system

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Tab Index	Description
id	controls).
Analytic 7	Identify transactions posted by non-branch users without subsequent branch acknowledgement.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Appendix 6a

Case Data Summary Findings

~~Post Office 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 Post Office's investigators to conclude. This has been discussed with Post Office management during the course of our work.~~

Commented [A45]: This is old text

Procedure	Comments	Summary	Impact
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 13,666,238 transactions. ~~10.~~ There was an error in the original analytic logic which was supposed to remove duplicated transactions from the dataset but was in actuality removing both the duplicates and the original transactions from the data. ~~11.~~ ~~12.~~ When the analytic was corrected for this it was noted that there were no gaps in JSN sequencing were identified based on the data provided.	None – following further work performed.
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 49,320 (0.36%) 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 13,666,238 transactions	In less busy branches these could be legitimate gaps. Extensive further manual analysis would be required to positively conclude these findings are indicative of issues..
Analytic 3 : Identify two user logon events in sequence without the expected logoff event in between,	In order to identify two user logon events in sequence without the expected logoff event in between, an indicator of a connectivity	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	This is a low volume and could be indicative of power / communications fluctuation / failure. Extensive further

Formatted: Normal, Space After: 0 pt, Line spacing: single, No bullets or numbering

Formatted: Font: (Default) +Body (Arial)

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedure	Comments	Summary	Impact
an indicator of a connectivity issue	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.	on/off events.	manual analysis would be required to positively conclude these findings are indicative of issues..
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	This is a low volume and likely to be indicative of expected system functionality. Specific controls have been tested over recovery transactions, during our production of this report. Where legal counsel is aware that part of the case may focus upon hard reset of branch counter equipment (e.g. by physical removal of network connectivity), these transaction types may support that this activity was occurring.
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	This is a low volume and likely to be indicative of expected system functionality. Specific controls have been tested over recovery transactions.
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 Customer' were identified and a summary per item is produced.	There were a total 1,344,773 (9.84%) zero valued transactions with a quantity not equal to zero from a total of 13,366,238. These transactions were against a total of 432 products	The impact of a zero value transaction is not likely to affect branch accounts, unless a value should have been present. Extensive further manual analysis would be required to positively conclude these findings are indicative of issues.
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	There were 48 (0.0015%) session ids from a total of 3,124,140 which were out of balance based on the transactional data received. Those 48 session ids out of balance related to 18 distinct branches from 118 in total. The	None – following further work performed.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedure	Comments	Summary	Impact
	branch (Group) and session id and those session ids that do not sum to zero were identified, and are ordered by balance descending. The data used was filtered for transaction mode 'SC' only.	session ids out of balance were all pre system migration to HNG-x in 2010. ~~13.~~ ~~14.~~ The root cause for the ~~40~~ 48 transactions appearing not to balance was determined as: a. Some of the audit log sequences were missing a start time and hence were not extracted properly. b. Some of the audit log sequences were missing a SC (Serve Customer) record and hence were not extracted properly. ~~15.~~10. These issues were shown to have been overcome by looking at the raw audit log sequence data (as it was the extraction logic performed by Fujitsu which was causing records to be dropped). ~~16.~~11. It was confirmed through the walkthrough with Fujitsu and through checking the 15 sampled files independently that there were no session ids out of balance based on the new transaction data provided and it was concluded that the out of balance session ids identified on the initial run through were out of balance due to the 2 errors identified above in extracting the data from the raw audit log sequence.	

Formatted: Normal, No bullets or numbering

Formatted: Font: (Default) +Body (Arial)

Formatted: Font: (Default) +Body (Arial)

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Procedure	Comments	Summary	Impact
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 19 (3.31%) users from a total of 574 users classified as non-branch users who posted transactions	The specific transactions are listed below in 'Analytic 7 detail.' Extensive further manual analysis on the population of transactions identified would be required to draw meaningful conclusions, as well as a further understanding of the owners of these 19 accounts.

Analytic 7 detail.

Branch No	User	Debit Value	No of rows
394329	*BMA01	233089.08	170
198424	*JHO05	214684.08	39
394329	*GDR01	204135.62	184
197941	*NST01	95703.47	130
207320	*DWA01	91762.85	12
158644	*JBA03	83825.54	311
219420	*RLY01	74781.24	16
363642	*DJO03	63600.32	66
260604	*TAK01	51489.96	62
229555	*DCU02	45022.32	7
243205	*PJO07	39660	12
202604	*STU03	29267.14	4
6458	*DSI02	25425.82	5
266418	*MWE01	24724.77	6
363642	*LSH01	23798.63	15
362217	*JCA01	13485.55	2
282422	*TAK01	8382	2
225329	*BMA01	7500.18	4
238420	*RCR01	5923.36	4
198424	*TAK01	1080	6
243205	*GMU01	1040	10
197941	*PJO02	15.07	10

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 branch's 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)?

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

    However the window of opportunity to do (a) in the BRDB is finite, if the edit/delete of the transaction was not done before the data had been 'collected' by the Audit Server (typically every 15 minutes for some products with a maximum exposure in the order of 24 hours for others), 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.

    Any amendment to transactions after the BRDB, whilst potentially impacting the audit store record, would not impact branch accounting, only the master record in the Audit store. 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.

Formatted: Font: Italic, Font color: Auto
Formatted: Font: Italic
Formatted: Font: Italic, Font color: Auto
Formatted: Font: Italic, Font color: Auto

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 server / 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.

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, thus there is the theoretical risk transactions could be amended with no footprint left. However to do (a) without leaving a footprint in the system would be a complex procedure, new 'keys' would need to be generated for all messages in the session, which is a time consuming process, as such it is likely a 'programme' would have to be written and performed in order to perform this.

d. Whether (a) has ever actually happened?

Audit logs of Privileged 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 Privileged 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 Privileged User.

Formatted: Font: Italic, Font color: Auto

Commented [A46]: Check

MAMW: Check all references at the end.

Formatted: Font: Italic

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic, Font color: Auto

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 Privileged User change could theoretically cause a shortfall in branch accounts.

Formatted: Font: Italic, Font color: Auto
Formatted: Font: Italic, Font color: Auto

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 Privileged User, would automatically impact the daily cash rec report (impact dependent on nature of BT / change).

Formatted: Font: Italic, Font color: Auto

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).

Formatted: Font: Italic, Font color: Auto

Specific questions on the Interim Report

1. 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.

   Formatted: Font: Italic, Font color: Auto
   Formatted: Font: Italic

      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?)

      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

      Formatted: Font: Italic, Font color: Auto

   b. Transaction corrections generated by Post Office: Where does a Transaction Correction fit on this diagram?

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

   Formatted: Font: Italic, Font color: Auto

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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).

Formatted: Font: Italic, Font color: Auto

2. Page 10:

a. Point F – says Post Office 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.

Formatted: Font: Italic, Font color: Auto

3. Page 19:

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

a. 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.

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

b. 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 Privileged User amending existing transactions does exist as highlighted above in question 1.

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

4. BTs in relation to the Stock Unit 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.

Formatted: Font: Italic, Font color: Auto

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).

Formatted: Font: Italic, Font color: Auto

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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?

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.

Formatted: Font: Italic, Font color: Auto

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. So no.

Formatted: Font: Italic, Font color: Auto

5. 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.

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

b. How far back do the audit files go?

The audit files commence at 12/03/2010

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

6. 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 DBA access to the live BRDB database and therefore could theoretically make changes to transaction tables as described in (10b) below.)

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

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

The process followed by FJ is:

Formatted: Font: Italic, Font color: Auto

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 Post Office 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.

Formatted: Font: Italic, Font color: Auto

Senior approvals are required by Post Office 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.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 Post Office for implanting / authorising a BT (if this is out of scope, please say and we will pick up direct with Post Office)?

Out of scope. Agreed Post Office will answer.

Formatted: Font: Italic, Font color: Auto
Formatted: Font: Italic

7. 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?

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

Formatted: Font: Italic, Font color: Auto

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).

Formatted: Font: Italic, Font color: Auto

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.

Formatted: Font: Italic, Font color: Auto

~~*Post Office 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).*~~

Commented [A47]: Is this still correct?

TO CHECK WITH LEWIS

Formatted: Font: Italic

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

Formatted: Font: Italic, Font color: Auto

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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?

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.

Formatted: Font: Italic, Font color: Auto

i. What controls were there around these?

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

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

ii. Were they logged?

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

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

8. Privileged Users

a. Can Privileged Users only access the BRDB or can they access other servers (i.e. audit server, audit store)?

Privileged 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.

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic

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.

Formatted: Font: Italic, Font color: Auto

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.

Formatted: Font: Italic, Font color: Auto

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 Privileged User edits data in the BRDB, how might this affect the branch accounts from the perspective of the Postmaster?

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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 (e.g. 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 Privileged 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 Post Office / FJ?

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

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic, Font color: Auto

Formatted: Font: Italic, Font color: Auto

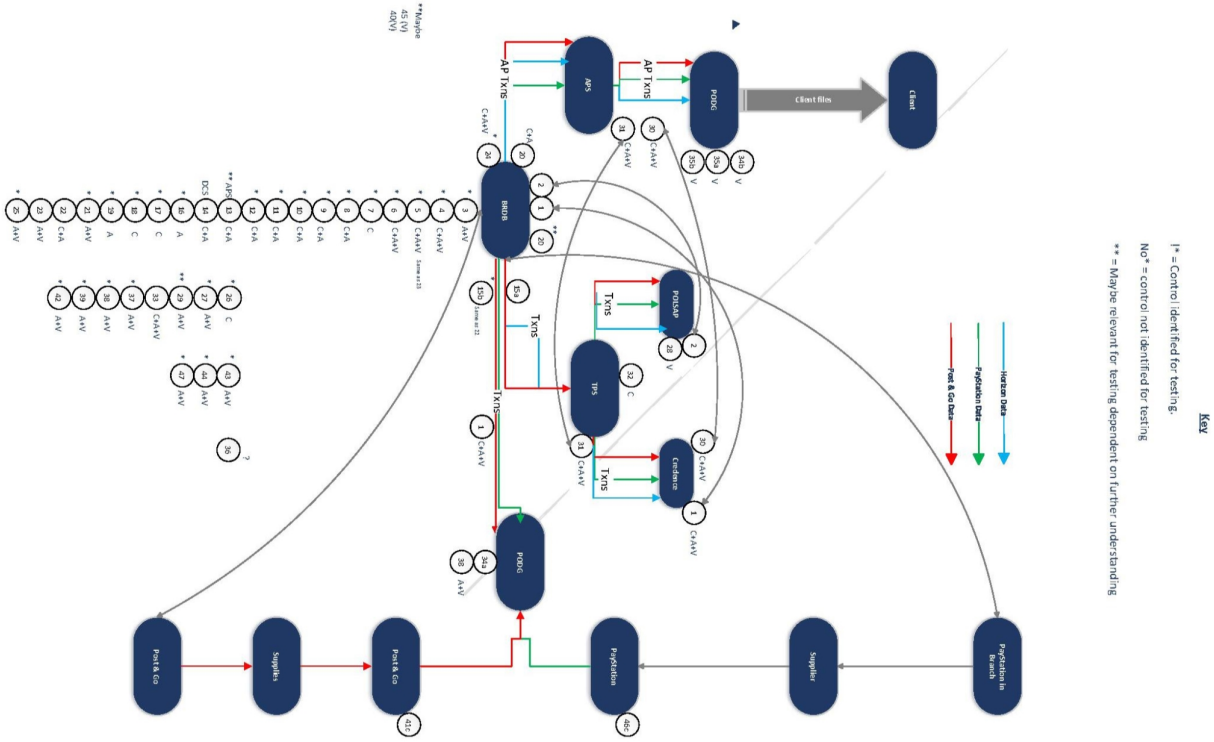
Formatted: Font: Italic, Font color: Auto

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Appendix 8

~~Non Counter~~Non-Counter Initiated Transactions – Understanding of Data Flow and Related Risks and Control



POL00029097

Reconciliation Controls

Note: Errors sources are Completeness (C), Accuracy (A) and Validity (V).

#	Error Sources Addressed	Summarise Control Wording
1	C & A & V	External transactions sent via PODG such that the External Transaction files that are currently sent from Ingenico (PAYSTATION) and Wincor Nixdorf (POST&GO) are routed to the Branch Database as well as sending the data to the Credence system. There is a reconciliation between Credence & BRDB.
2	A & V	For each Transaction Acknowledgement generated, a new transaction pair is created for POLSAP. The transaction delivered to POLSAP will have a Reference number that matches the reference number used in the Transaction Acknowledgement record generation. This allows POLSAP to match with the Transaction Acknowledgement once the TA has been accepted by the Postmaster.
30	C & A & V	AP Client File Reconciliation APSS2222.ksh will reconcile the data in the files that it delivered to a Client with the data in the files that Credence delivered to a Client.
31	C & A & V	TPS to AP Reconciliation TPSC227 writes APS transaction data to a formatted file that will later be used by the APS host program APSC2051 to reconcile data from TPS with that from APS.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Interface Controls

#	Error Sources Addressed	Summarise Control Wording
3	A & V	If any one transaction fails validation / load, then the whole sub file (all rows for the same branch / trading date) will be rejected.
4	C & A & V	Processing of the files will commence when the last file is received. The last file is identified by 'Y' in the Last File Indicator field in the File Trailer Record.
5	C & A & V	Generic file receipt process (BRDBC038) will handle receipt of the different files that arrive at the external interface and will perform registry of the files in the file audit trail and will move the files to the input directory and the audit directory.
6	C & A & V	Any transactions that would have been incorporated in the Transaction Acknowledgement feed that are delivered in the Paystation / Post&Go files will be automatically included in the Branch Accounts without being presented to the Postmaster for acceptance. Transaction Acknowledgements for this transaction detail will be created at the same time for later acceptance by the branches. It also takes transactions that have previously been held aside due to the lack of Transaction Acknowledgement / Stock Unit mapping or due to the SU being locked at the time of original posting and retries posting of these transactions.
7	C	An automated Daemon process operates that starts to look for the arrival of the External Transaction files at hh:mm O'clock but gives-up and alerts if not arrived by nnn minutes later. (This allows Horizon transactions to get processed if External Transaction files are late). This process performs the necessary copy / rename and creates links to audit directory. Hh:mm will initially be 18:00 and nnn minutes will be 120 minutes.
8	C & A	FILE PROCESSOR • If the file pre-processor returned with an error in the range of 102-105, then the table BRDB_FILE_ERRORS will have a row added to it with an error value equal to the return value of the file pre-processor and the associated row in BRDB_FILE_AUDIT_TRAILS will be updated to status 'X'. No other error values are expected and, if they occur, the process will abend and alert the Operations staff. • If the file pre-processor was successful, then the file validation and database upload process will be called and exit status checked.
9	C & A	FILE PRE-PROCESSOR The pre-processor performs a number of operations including splitting the files according to parameters. In addition it validates: • The first record is a header record

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

#	Error Sources Addressed	Summarise Control Wording
		• The last record is a trailer record • The number of sub-files in the file equals the count in the trailer record • The total value of sub-files (in the trailer) equals zero If any of these validations fails, then the whole file will be rejected, a row will be inserted into BRDB_FILE_ERRORS and no further processing is performed on the current file. Page 60 HAS TABLE OF THESE 8!
10	C & A	DATA LOADING & VALIDATION This function is initiated by the File Processor. The 8 files generated in the previous process will be attached to Oracle as external tables and the data therein will be validated and loaded into staging tables. It will validate data items such as product, mode, branch etc. A log will be held for each file processed and each sub-file processed that will indicate the filename, status (valid/not-valid), and history of the file processing. A separate error table will record each error type and error code encountered.
11	C & A	Ensure that the count and value of transactions equals the number recorded in the sub-file trailer and that the value of transactions nets to zero otherwise record in BRDB_FILE_ERRORS with record type = STZ, Error Code = 108, Description = "Sub-File Trailer totals incorrect"
12	C & A	Load the Transaction Data and Validate At this point, the file structure has been validated and we now need to copy the data from the external files into the Branch Database in preparation for Transaction Posting later-on in the schedule. During the copy process the data will be enriched with missing attributes and validated against reference data held in the Branch Database. During processing of each record, transaction-level validations will be performed and any errors found will be written to BRDB_FILE_ERRORS with record type = OXZ and FAD Code and Business date = Sub-File details. The error code depicts the type of error found.
15b	C & A	If there is an entry in the error file with error_code = 101, then the file is a duplicate. The previous file that was delivered of the same name might have had errors recorded against it and, so as not to confuse matters, only the 101 error is returned in the error file.
16	C	Completeness Check A process will check the table BRDB_SUB_FILE_AUDIT to test whether data has been received from all external sources for the current date. If it has not, then an alert will be raised that lists all External Transaction sources that have not provided data so

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

#	Error Sources Addressed	Summarise Control Wording
		that relevant stakeholders can be notified.
17	C	External transaction processing. Immediately following the cessation of the Transaction Loading Daemon, the transaction posting process will be invoked using TWS Schedule BRDB_TXN_POST.
18	C	The final stage of External Transaction Posting is to copy the transactions for the current sub-file from the Staging/Holding tables into the Branch Database Receipt tables ready for onward delivery to the TPS and the APS subsystems.
19	A & V	A validation process will be followed that validates the content and format of data and records errors against bad rows.
20	C & A	Transfer of data to TPS & APS… Reconciliation totals are generated to ensure that the data that is sent to TPS and APS matches with the totals of data within BRDB.
21	A & V	Rejected and Held-up Transactions Report A report is produced which highlights any transactions that have been loaded into BRDB but withheld from processing due to lack of Transaction Acknowledgement mapping or due to the associated stock units being locked. The report will also list those Sub-Files that have been rejected and have not yet been re-delivered error-free. This report will execute in the BRDB_EXT_REP schedule.
24	C & A & V	External data imported into Branch Database is copied across into BRDB_REP_SESSION_DATA. This ensures that they are picked up for any Branch reports and Branch accounting.
25	A & V	In order to post the transactions to the branch accounts, two criteria need to be met: • A mapping of External System and Terminal Id for all transactions must exist in the Transaction Acknowledgement/SU mapping table • The stock unit for the branch must not be locked
26	C	A report will be produced that lists any sub-files that have been held-back from processing for more than one day.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

#	Error Sources Addressed	Summarise Control Wording
27	A & V	Camelot ONLY: Retailer data is required to validate that the Retailer Number is a valid. Validation includes a check that the Retailer Number maps to the correct valid FAD Code.
28	A & V	POLSAP Load process: The Post Office SAP load process in XI has some explicit checks (introduced to prevent files being accidentally loaded more than once) that there will not be multiple sub-files with the same Branch / Trading Date combination.
29	A & V	Validation should be performed such that when loading the data from external files it is checked that the Product can be transacted on that particular type of external system.
32		TPS Processing monitoring A monitor job tests for successful completion of the TPSTIPL schedule at 03:00 and alert operations if not.
34	V	PODG will be used to transfer data between the Fujitsu data centre and External Transaction Suppliers. For External Transaction interface files, there needs to be an inbound route to the Branch Database and also there needs to be an outbound route from the Branch Database to Suppliers for the return of Error/confirmation files. Logical access rights to these holding directories are appropriately secured.
35	V	PODG to APS Interface Old process: APS already has links to EDG1 and EDG2 for the delivery of AP Client Files. Access to these directories is appropriately secured. New process: APS configuration has been updated to deliver client files to revised directories that will be shared with PODG. Access to these directories is appropriately secured.
36	A & V	Post & Go: Post Office ETL will validate incoming files in terms of shape, structure and check totals.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

#	Error Sources Addressed	Summarise Control Wording
37	A & V	Post & Go: The Transaction Detail record will always contain a core of mandatory fields, and the records will be rejected if these fields are not populated. An alert will be raised within Wincor Nixdorf in the event that the file transfer fails. The Post Office Live Service (Team) will be informed and procedures invoked to rectify the problem.
38	A & V	Post & Go: If the file and sub-files contain no errors, Post Office ETL will rename both the copy file held on Post Office ETL and create an error file with records type OKZ, to be sent back to Wincor Nixdorf to indicate the file is good. When Wincor Nixdorf have investigated and corrected the records in error a new / corrected file it sends with the same name as the error file, as Post Office ETL will know it has sent the errorfile and will expect the corrected error file to be replaced. NB: If Post Office ETL receives a duplicate transmission file and / or sub-file(s), Post Office ETL will report this error to Wincor Nixdorf, and will also send these back to Wincor Nixdorf.
39	A & V	Post & Go: Validation criteria for received Post and Go Files are as follows: • Post Office ETL to reject a file should any error be found within the file, sub-file, or records within the sub-file that Post Office ETL cannot accept. In such a case, Post Office ETL will create an error file specifying the errors found • Post Office ETL will return the error file to EDG to be picked up by Wincor Nixdorf, specifying any rejected files that need to be corrected and resubmitted • Wincor Nixdorf will return repaired error records in a new file (and sub-file) for repaired records • Post Office ETL must inform Wincor Nixdorf of an error within 24 hours. Wincor Nixdorf must keep the source files for 7 calendar days in case Post Office ETL require a file to be re-sent.
42	A & V	Paystation: The Transaction Detail record will always contain a core of mandatory fields, and the records will be rejected if these fields are not populated.
43	A & V	Paystation: When Post Office ETL has processed the file it will rename the file as shown in Table 2 indicating whether:

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

#	Error Sources Addressed	Summarise Control Wording
		a. The incoming file from Ingenico has been received OK (suffix .TPB) b. Any errors have been detected in the file (suffix .TPX) together with an error file (suffix .TPZ)
44	A & V	Paystation: Any files which are re-sent are to be given the same File Name and File Header information, with the 'Transmission Status' set to RES. RES is to be used for whole file rejections only.
47	A & V	Paystation: For reversal transactions, the original Transaction Mode is shown in the transaction details that are sent to Post Office ETL. Post Office ETL will know if a reversal has taken place by referring to the reversal indicator within the transaction line.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Appendix 9

Formatted: Width: 21 cm, Height: 29.7 cm

Note: This content has been produced by Fujitsu and replacroduced faithfully here.

Formatted: Font: 10 pt, Font color: Auto
Formatted: Font: 10 pt, Font color: Auto
Formatted: Line spacing: At least 16 pt

Fujitsu Report on Privileged Users

Database Security in Horizon Online

Formatted: Font: 12 pt, Bold, Font color: Accent 1
Formatted: Normal

Ref: 170406 DOC 3545053Database Securityv1.0.docx

Author: Gareth I Jenkins

Updates: Pete Newsome, Torstein Godeseth

Date: 12/12/2017 ~~18:27:0012/12/2017 18:27:0012/12/2017 18:27:0029/11/2017 09:27:0029/11/2017 09:27:0029/11/2017 09:27:0029/11/2017 09:27:0029/11/2017 09:27:0024/11/2017 11:29:0015/11/2017 10:42:0015/11/2017 10:42:0015/11/2017 10:42:00~~

Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 11 pt, Do not check spelling or grammar
Formatted: Font: 12 pt, Bold, Font color: Accent 1
Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

Version: 1.0

Introduction

This note has been prepared by the Author to provide some clarity as to the veracity of some of the concerns raised by Deloittes in its report to the Post Office regarding the Horizon system and specifically Super User access. The purpose of this note is to explore the extent to which it is technically possible for:

1. Post Office / Fujitsu to have the ability to log on remotely to a Horizon terminal in a branch so to conduct transactions.
2. Post Office / Fujitsu to have the ability to conduct transactions (either remotely or locally) under another user 's ID,
3. Post Office / Fujitsu to have the ability to push transactions into a branch's accounts without either a postmaster's (a) knowledge or (b) consent.
4. Post Office / Fujitsu to have the ability to amend or delete transactions entered by branch staff on Horizon (and can do so in a way that is hidden from postmasters).

In the previous reviews by Deloittes they have concluded there was a theoretical possibility that a limited number of 'Super Users' had a level of access that would allow some of the actions 1 to 4 above, or their equivalents, to take place.

This paper shows the steps that a 'Super User' would have to make in order to alter the Horizon Online Audit Trails. It also goes on to discuss, if such modifications were made, how they would be detected. This is covered in Section 3.

Section 4 then considers the equivalent mechanisms in the old, Riposte based, Horizon system. Finally, section 5 considers things from the Postmaster's viewpoint.

This document assumes that readers have some familiarity with the technical documentation that has been supplied to Deloittes to support their reviews.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt, Line spacing: At least 16 pt

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

Executive Summary

Formatted: Font: 12 pt, Bold, Font color: Accent 1

Fujitsu's view and conclusion remains that whilst such unauthorised amendments by Super Users to the Horizon Online Audit Trails are theoretically possible (as in all IT systems) they would be very difficult and even if they were made, would almost certainly be detected as a result of the discrepancies in the relevant logs and audit trails. In addition, it should not be forgotten that the various Horizon systems provide records of transactions as opposed to access to the funds themselves and as such, even if one were to satisfy oneself that this theoretical risk were real then it is difficult to imagine how someone exploiting this approach would be able to benefit financially without detection. It is our reasoned estimation that to carry out the complex and detailed technical steps necessary to over-ride the systems check and balances and then to make artificially generated funds disappear is not credible.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

Horizon Online

Formatted: Font: 12 pt, Bold, Font color: Accent 1

Section ~~3.1~~1 describes how the Horizon Audit Trail is generated and secured. Section ~~3.2~~2 then explores how, in theory, a portion of the Audit Trail could be deliberately replaced by a Super User. Finally, section ~~3.3~~3 discusses how such changes could be detected.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

1. How the Horizon Online Message Log is Generated and Secured

The Horizon Online Message Log is primarily a log of all auditable messages sent from the Horizon Counter to the Horizon Data Centre where they are processed by the Branch Access Layer (BAL) which in turn updates the Branch Database (BRDB).

Note, that not all messages sent from the Counter are audited. However, any that could impact on the Branch accounts should be audited. Each message sent from the Counter to the Data Centre indicates whether or not it is to be audited (ie the decision is part of the counter application and not the BAL).

The BAL configuration also decides which messages pass through the Audit Filter (which does the auditing).

It is part of the system's design to ensure that the counter and BAL configurations are consistent in this respect.

Specifically, messages have jsns if and only if they are auditable and so the checks on jsn sequences described below ensure the completeness of the audit trail.

Each Auditable message sent from the counter includes a "digital signature" generated using the counter's Private Key. This key is generated by the counter as part of the Log On process. The corresponding Public Key is included in the Log On message sent from the counter to the BAL allowing the BAL to confirm subsequent messages in the session come from the same counter. Unlike other messages in the Message Log, the BAL adds a wrapper to this Log On message which includes a further digital signature (of the entire message including the counter's digital signature and the counter's Public Key) generated by the BAL, using the BAL Private Key which is obtained from the NPS Key Store by the BAL at start-up.

All auditable messages are written to a single table within the BRDB known as the "Message Log". Each day (at some point after 1am) the previous day's Message Log is written to a number of files which are then passed to the Audit system which then "seals" each file and stores them until they are retrieved (if they ever are) or deleted. Note that each file will include records from a number of different Branches and there may be multiple files for a single day containing the records for a specific Branch.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

Deletion of Audit records is currently suspended. They should be deleted after 7 years, but deletion was switched off sometime in 2014 (I think). Therefore, all audit records since Horizon Online went Live in 2010 should be available.

This seal is cryptographically generated and is based on the entire contents of the Audit File. Any subsequent change to the contents would then invalidate the seal. The seal is held in a seals database separate from the Audit Data. A feature of the Audit System is that data cannot be amended or deleted until the pre-defined "Purge Date". Super Users do **not** have access to the Audit data.

All updates to the BRDB will be based on the information held in the auditable message and the accounts (both as seen in the Branch and also as passed to Post Office Ltd's back end accounting systems) are based on this information (and not on the actual auditable message). This means that in order to corrupt the Branch accounts, it is necessary to corrupt a number of different records within the BRDB and not necessarily the Message Log. However, any evidence provided by Post Office Ltd is based on the Message Log – hence the need to corrupt the Message Log as well.

It is asserted that by going back to the audited data (ie the Message Log) sent from the Counter to the BRDB, then all Transactions that that counter carried out and their implications on the Branch Accounts can be re-calculated and compared with the reports produced by Horizon based on the other data held in the BRDB and Post Office Ltd's back end systems. This would enable any corruption of the data used to create the Branch reports to be detected from examination of the Message Log.

When audit data from the Message Log is retrieved for whatever reason, a number of checks are carried out to ensure the completeness and integrity of that data. These checks are:

- Each entire Audit File is checked to ensure that the digital seal stored at the time the Audit was produced (ie the day after the transactions took place) is valid.

Normally a Data retrieval will be for a number of days and so a number of Audit files will need to be retrieved.

- The data for the Branch in question is then filtered out from these audit files and checks are then carried out on a counter by counter basis as described below for the period of the extract:
    - No part of the Message Log is missing or duplicated. Each auditable message sent from the counter to the BAL incudes a unique sequence number (the Journal Sequence Number or jsn). The audit records for any counter over a period of time should have no missing or duplicate jsns. The standard Audit Extracts into Excel include a report indicating that this check has been successfully carried out. This is a sheet labelled 'Summary' in the standard ARQ report provided to Post Office Ltd.
    - The message audited as part of the Log On process, is checked and the Digital Signature generated by the BAL is checked by using the BAL's Public Key (which is known to the Audit System). This shows that this message was signed by an application which had access to the BAL's Private Key. This then provides access to the Counter's Public Key for that Log On Session (as this is included by the message audited by the BAL and was signed by the BAL's private key).
    - All subsequent messages sent from the counter to the BAL during that Log On Session are then checked to ensure that their Digital Signatures are correct (using the Counter's Public Key obtained from the Log On message)

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

2. Replacing the Message Log

In theory, a Super User, could amend the Message Log for one or more Counters in one or more Branches. The following describes what would be required to replace the Message Log for a single counter in a single branch. This process could be repeated for multiple counters / branches if required.

1. The work would need to be completed before 1am the following day (since the Message Log is extracted from BRDB at some point after 1am each night and the data is then sealed and held in the Audit Server
2. The entire Message Log associated with a Log On Session that is to be corrupted would need to be replaced

This is because it is not possible to obtain the counter's Private Key and so a new one would need to be generated as described below.

3. The records being replaced would have to be in one-to-one correspondence to the original records otherwise there would be gaps or duplicates in the sequence of jsns which would then be detected as part of the Audit Retrieval process.
4. An application would need to be run by the Super Users in order to correctly construct the revised Audit Records
5. This application would need to generate a Private / Public key pair similar to the one originally generated by the counter. Called an "Attack Counter key" in the rest of the document
6. The application would need to have access to the BAL's Private Key. Since this is stored in the Key Store which is an Oracle Database running on the NPS, then it is assumed that a Super User would be able to read this value and make it available to the application. This would then enable the application to generate a Log On Message Log message containing the fake Counter Public Key and to sign it using the genuine BAL Private Key.
7. All subsequent messages for the session would then need to be amended as required and then re-signed using the Attack Counter Private Key generated at step 5.
8. Having constructed all these false Message Log messages, then the Super User would need to delete all the genuine messages from the Message Log in BRDB and replace them with the false messages on a one for one basis.

Or this could be done just by updating the rows with the new data.

Note that the table in the database is set to allow 'append' access only and has been designed to be appended to at all times. The Super User would need to amend the access rights to the table before records could be amended or deleted, and this would change the performance characteristics of Oracle; this alone may be sufficient to make such an attack detectable as any instance of slow running on the system would be investigated by the support teams.

9. Note that as stated earlier, corrupting the Message Log in this way has no impact whatsoever on the Branch Accounts, since these never refer to the Message Log. The Branch Accounts are based on copies of some of the data held in the Message Log being stored in "working tables" within the BRDB. Clearly any application that is capable of corrupting the Message Log in BRDB would also be capable of updating (ie corrupting) the data used to calculate the Branch accounts.

Note that the relationship between data held in the Message Log and the Branch accounts is e complex. Therefore, a significant amount of knowledge and skill would be required to attempt this.

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

It should be noted that since R12 (July 2015) all access and actions carried out by Super Users to any database is strictly audited to an Oracle Audit table. The records in the Audit Table records the following information:

- User Id of the Super User
- Action (eg Log On, Execute a SQL command, Log Off etc.)
- Date and Time of the action
- Actual SQL statement executed (where applicable)

This Audit Table is again extracted from BRDB soon after 1am and the data picked up and sealed before being copied to the Audit Server.

Note that it is possible for the Super User to manipulate the Audit table (including removing entries from the table). However, should the table be removed entirely, then the database would stop working. If only old entries are removed, then the removal of entries will be recorded, thus making it clear that the table has been manipulated though the details of the changes would not be fully visible.

Prior to R12, when the BRDB was upgraded to run on a later version of Oracle, (ie from 2010 to July 2015), only Log On and Log Off activities by Super Users were audited. For all planned access, then an MSC (Managed Service Change document) would have been signed off and the Logs of the Super User activities would have been attached to the MSC. Therefore, a correlation of Log On / Log Off activities of Super Users against MSCs should detect any rogue activities.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

3. Detecting Changes to the Audit Trail

In order to make the changes to the Message Log described in section 03.2, the Super User would need Read access to the Key Store database which runs on the NPS and Read / Write access to the BRDB. Note that should the rogue application run on the BAL, then this isn't necessary as the BAL's have access to the Key store based on the IP address.

Note that the BAL Private Key only needs to be accessed once as the same key is used for a year.

However the BRDB would need to be accessed each day that the Message Log is to be corrupted.

All such access by a Super User would be audited in the Audit Table; since R12 such logs would show the activities carried out whilst logged on, and prior to R12 the logon (and logoff) events would be recorded.

Therefore, should there be any allegations that any data has been corrupted, an examination of the Database Audit tables should ensure that this has not occurred. Although the Database Audit tables are not regularly examined they were recently checked as part of an external Audit of Horizon Online and no issues were reported.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

Old Horizon

Formatted: Font: 12 pt, Bold, Font color: Accent 1

On the old Horizon system, the mechanisms were very different from those used by Horizon Online. Section 4.14 provides an overview of how the Riposte Message store operates, then section 4.25 describes the Riposte Audit Trail. Finally section 4.36 shows how injections of messages by a super users would be detected in the audit trail.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

4. Overview of Riposte

All Counter data was held in a bespoke Message Store which was part of the Riposte product supplied by Escher Inc. This data was replicated within each Branch to all counter positions and from each Branch to the Data Centres where it was held in the Correspondence Server Message Stores. Similarly, any data inserted into the Message Store at the Data Centre (eg Reference Data or authorisations for Banking Transactions) would be replicated back to the Branch Counters.

Selected data was then extracted from the Correspondence Servers to update Post Office Ltd's Back End systems.

All accounting at the counter was carried out based on the data held in the Message Store. The Riposte product managed the Message Store and it did not allow any message to be updated or deleted. Therefore all that could be done to corrupt the data in the Message Store was to inject additional messages which could then influence the Branch accounts. Such injections were possible at the Correspondence Server for users with sufficient access permissions.

Each message included 3 key bits of information which together provided a unique identification for each message:

- Group ID: this was the 6 digit FAD Code of the Branch with which the message was associated
- Node ID: This indicated the Counter Position at which the message was originally written for messages generated at the Counter or the Correspondence Server identifier for messages generated at the Data Centre. Counter Node Ids where between 1 and 31, and Correspondence Server Node Ids where between 32 and 63.
- Message ID: A unique number for each Group ID / Node ID. This number starts at 1 for the first message written at that Node, and increase by 1 for each subsequent message. This allows checks to be made that no messages are missing as that would result in gaps in the sequence of Message IDs

The concept of jsns used in Horizon Online was based on this.

Messages also have an associated "Expiry Date". This indicates the number of days after the message is first written before it can be deleted. An archive process ran on each counter and Correspondence Server at around 3am which deleted all messages that were past their Expiry Date, thus ensuring that the Message Store did not continue to grow indefinitely.

Some special messages which are referred to as "Persistent Objects" did not expire in this way but could be removed after they were replaced.

However again they were all held for a minimum of 34 days and in general were not relevant to generating the Branch Accounts.

In particular, Riposte was configured such that no messages where allowed to expire until they were at least 34 days old. This was to allow for counters that were offline for a significant period.

Each message also had an associated CRC, this was basically a checksum that was included to ensure that the message had not become accidently corrupted. Note that this was not a cryptographically secure seal and it would be possible for a sufficiently technically skilled person to alter a message and recalculate the CRC if they had access to the message outside the message store.

Due to the size of the Post Office Network, Branches were split into 4 separate Clusters. Each Cluster included 4 Correspondence Servers (2 in each Data Centre), thus ensuring that there were normally 4 copies of the data held in the Data Centres.

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

5. The Riposte Audit Trail

An Audit Application was run on the Correspondence Servers to take an audit copy of all data visible to that Correspondence Server.

The Audit Application was run on one Correspondence Server on each Cluster in each Data Centre. This means that there were two independent Audit Trails for each Branch. However when retrieving the data only one Audit Trail was used.

This application read every record that was visible to that Correspondence Server (ie all data in that Cluster) and wrote a text copy of that data to a text file. Each Audit application wrote data to 10 text files (based on one of the digits in the FAD Code) and when the text file got to a certain size it was closed and a new file created for that text stream. The file included a hash value of the file contents to ensure that should it be accidentally corrupted, then this would be detected. Also around 1am each day the file was swapped thus ensuring that data associated with a given day was in discrete files.

Once these files had been written they became visible to the Audit server which would pick the files up and Seal them and store them until they are retrieved or deleted.

This process was not changed for Horizon Online.

Deletion of Audit records is currently suspended. They should be deleted after 7 years, but deletion was switched off sometime in 2014 (I think). Therefore all audit records since sometime in 2007 should be available. Those from before that time are no longer available.

If the audit trail is retrieved, then similar checks to those carried out on Horizon Online were made, namely:

- Each entire Audit File is checked to ensure that the digital seal stored at the time the Audit was produced (ie the day after the transactions took place) is valid.

Normally a Data retrieval will be for a number of days and so a number of Audit files will need to be retrieved. There would also normally be a number of audit files for each day.

- The data for the Branch in question is then filtered out from these audit files and checks are then carried out on a counter by counter basis as described below for the period of the extract:
  - No part of the Audit Data is missing or duplicated. This is done by ensuring that there are no missing or duplicate Message Ids for each counter / CS. The standard Audit Extracts into Excel include a report indicating that this check has been successfully carried out.
  - The CRC is recalculated and confirmed as correct for the message.

6. Detecting Changes to the Audit Trail

Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

If a malicious Super User wished to interfere with the Branch's Data, then that would need to be done by injecting messages into the Correspondence Server or Counter Message stores using the Riposte APIs. Support Staff did have the capability (and occasional need) to do this at the Correspondence Server. Processes where in place to ensure that any such messages included information as to who had done this. Such information would not be visible in the standard audit extracts (but would be visible in a detailed examination of the raw audit data). Clearly any malicious corruption would be done without such trace information. However, if such data were injected at the Correspondence Server, it would be clear that this had occurred since the Node Id associated with the message would be that of the Correspondence Server at which the message

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

had been injected and not a normal Counter Node Id. This would be clearly visible in any audit extract.

Postmaster's View

Formatted: Font: 12 pt, Bold, Font color: Accent 1
Formatted: Normal, Left, Space Before: 0 pt, After: 0 pt

The Horizon system records all transactions and uses its records to generate a view of how much cash and other items of value should exist in a branch at any time. Subpostmasters are required to carry out daily cash balances where they should check that the cash they hold in their tills corresponds to what the system says they should have. If the system has been manipulated to present a false view of the cash they hold in the branch this should be immediately obvious when they carry out these daily processes.

In the theoretical scenario that a Super User has manipulated the transactions for a Branch they thus have to address the problem of making the physical cash or some other representation of value, appear in, or disappear from, the Branch without triggering any investigation.

Formatted: Normal

© Deloitte 2017 Private and Confidential – Subject to Legal Privilege - DRAFT

POL00029097

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
November 2017

Commented [A48]: Date?

MAMW: Updated

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 other document, 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.

© 2017 Deloitte LLP. All rights reserved.

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