POL00138402

Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

Board Briefing

Document, further to our report "Horizon: Desktop review of assurance sources and key control features" dated 23/5/14, responding to five specific matters identified by POL as critical to POL's legal position.

4th June 2014

POL00138402

1. Context and Background to Work Performed

Horizon is the point-of-sale IT system which records transactions in Post Office branches. Horizon was commissioned in 1995 and underwent modification in 2010 to provide the current day 'On-Line' solution.

Post Office Ltd (POL) is responding to allegations that Horizon is defective and/or that the processes associated with it are inadequate. These allegations have been, and can be anticipated to be advanced in the Courts, and relate to applications to the "Initial Complaint Review and Mediation Scheme" established by POL in August 2013 to resolve individual complaints concerning Horizon and its associated processes.

In connection with those complaints, we have been informed that POL's legal position is that:

- Horizon produces and maintains the accounts between POL and its Sub-postmasters and other agents;
- unless there is proof that Horizon is not operating as intended, POL can enforce its legal rights against agents relying on those accounts.

To better understand the assurance evidence currently available to POL that Horizon is operating as intended, Deloitte LLP ("We") were instructed on 9th April 2014 to consolidate and assess that assurance evidence. Our work was restricted to a desktop review due to POL's time constraints and cost sensitivity.

As our work progressed it became apparent that in some key areas, evidence based assurance materials were either not relevant or could not be located by POL. For example, because the Horizon On-Line modification in 2010 was found to have not significantly impacted features relating to the integrity of processing, the scope of testing did not identify and test such features; nor had any work been performed to test relevant inbuilt controls in Horizon and its surrounding business controls, other than access controls.

On 6th May 2014, we were therefore instructed to extend our desktop review to assess additional project documentation, where available, and assemble an initial schedule of key control features from the existing and additional documentation received from POL and Fujitsu.

These features, referred to as the "Horizon Features", were deemed relevant by POL to their objectives if they supported the statements that Sub-postmasters have full ownership and visibility of all records in their Branch ledger, and that audit trails kept by Horizon are complete and accurate. Horizon Features identified were those:

- built directly into Horizon to exert control over processing;
- relating to IT management activities over Horizon; and
- relating to POL's business processes that use Horizon.

No documentation from the Horizon's implementation in 1995 remained available. However, review of the extensive operational documentation relating to Horizon's design identified a number of Features that, if implemented, would support the robust operation of the system. The identified Features have been reported to management in our draft report "Horizon: Desktop Review of Sources of Assurance and Key Control Features", made available for discussion on 26th May 2014 (the 'full report').

To then assist the production of a focussed summary for the Board, POL identified five matters (the "Matters") where the design and operation of the Horizon Features is critical to supporting POL's legal position, being those whereby:

1. Horizon only allows complete baskets of transactions to be processed;
2. Baskets being communicated between Branch and Data Centre are not subject to tampering before being copied to the Audit Store;
3. Baskets of transactions recorded to the Audit Store are complete and 'digitally sealed', to protect their integrity and make it evident if they have been tampered with;
4. Horizon's Audit Store maintains and reports from a complete and unchanged record of all sealed baskets; and
5. Horizon provides visibility to Sub-postmasters of all centrally generated transactions processed to their Branch ledgers.

This Board Briefing therefore provides specific commentary on the design of the Horizon Features we identified from the documentation provided, in each of the five Matters, including commentary on the extent to which documentation asserts the historic (pre-2010) presence of the relevant Horizon Features.

POL00138402

2. Summary

The work we carried out to support our full report, and thus this Board Briefing document, did not constitute an audit or assurance engagement in accordance with UK or international standards. In order to deliver a formal assurance opinion, we would need to have carried out testing to address the scope limitations. Our conclusions and findings are therefore limited to the design of Horizon. They are also subject to the accuracy of the assumptions and limitations set out in Section 3.

Based on the desktop review we have performed, except for the lack of monitoring controls and the matters explicitly drawn out in our full report, we have not become aware of anything to suggest that the system as designed would not deliver the objectives of processing of baskets of transactions and keeping copies of them in the Audit Store with integrity.

We also highlight that:

- POL is reliant on the features identified being implemented and operating as described. In particular evidence based testing is not available relating to relevant business processes and inbuilt controls, other than access controls.
- Assurance evidence no longer remains available from the original implementation project POL's historic comfort is therefore sourced from assertions from POL and Fujitsu staff.
- Data is permanently deleted from the Audit Store after seven years. We understand that some allegations relate to periods older than seven years.
- It is possible for Fujitsu staff with suitably authorised privileged access to delete data from the Audit Store.
- Sub-postmaster reports showing detailed transactions of their Branch are limited to the current accounting period and part of the prior accounting period, and are not drawn from the Audit Store.
- Digital signatures and digital seals are a key control feature underpinning the integrity of Horizon.

In considering the design of the Horizon Features, we would expect that there would be activities or testing performed to verify it had been implemented as designed; the need for those controls is borne out by the fact that one of the features has not been implemented as expected.

In considering this conclusion, it is important to understand that no system of controls can prevent or detect and correct all errors or omissions in processing.

Our full report contains suggestions to POL management on additional activities which could be performed to provide further comfort to POL relating to the Horizon Features.

3. Limitations and Assumptions

Our findings and conclusions are presented in the context of the following limitations:

- As a desktop exercise we have not validated whether Horizon has been implemented or operated as described in the documentation reviewed.
- Our work was limited by significant gaps existing in the information available, relating to both the granularity of information and the existence of the Horizon Features over the entire timeline of operation of Horizon. The effect of which is that there are in gaps within what we are able to comment upon over this timeline. Our findings below are written in the context of the information available, which relates to the current system.
- An event occurred in 2010 which required the use of the exceptional Balancing Transaction process in Horizon to correct a Sub-postmasters position from a technical issue. Information has not been provided on the circumstances that lead to this system issue and how the issue was identified. It is assumed that verbal assertions received from Fujitsu that this was the only time this process has been used hold true.
- We have not had direct contact with any third parties other than named contacts you have provided to us;
- We have not validated or commented on the quality of the documentation supplied to us.

POL00138402

Our work was also based on the following assumptions:

- The documents provided are a complete and accurate representation of the Horizon design. We therefore cannot comment as to whether the Horizon Features described below are complete nor whether other processes or mechanisms exist which would need consideration in the context of the Matters;
- All changes made after the initial implementation have been properly approved, tested and validated as not undermining the Horizon Features i.e. that the system's controls have retained their integrity throughout and thus the controls identified within the documentation have been consistent over the system's lifetime.
- The assertions received relating to the major upgrade of Horizon in 2010 not materially changing the design of the Horizon Features hold true.
- The cryptographic keys underpinning the digital signatures in Horizon have not been compromised.
- The mechanisms for issuing cryptographic keys for signing baskets is secure and authenticates requests to prevent unauthorised provision of keys.
- Fraud or collusion to undermine or work around the Horizon Features has not occurred, in particular within database administrator and security teams in Fujitsu.
- Assertions made by POL and Fujitsu staff have been accepted as accurate without corroboration or verification.

4.1 Specific Comments - General IT Controls

Relevant to all five Matters are controls that underpin Horizon. These need to be in place and operating to provide foundation level day-to-day comfort and are referred to as "General IT Controls". They are typically IT management activities, many of which are operated for POL by their outsourced provider (Fujitsu). They are fundamental because they underpin the integrity of the inherent controls which are described below.

In this area, POL has established governing forums to oversee the performance of outsourced IT providers, including Fujitsu, and performed a detailed risk and control assessment. Since 2012, Ernst and Young LLP (E&Y) has independently tested and opined upon key controls over day-to-day IT management activities to a recognised assurance standard (ISAE3402). POL has also documented its complementary controls outlined in E&Y's report.

E&Y did not report any material control deficiencies in 2012 or 2013. Prior to this assured period, there is no independent assurance available, although we have received verbal assertions from POL and Fujitsu staff that no material changes in the design of these IT management activities can be recalled.

4.2 Specific Comments – Other Key Controls (Summary)

Other key controls in the IT system and business processes arise in the following three areas:

- **Development testing** provides confidence that the controls built into Horizon are working as described before the system goes into use or is changed during its period of use. Due to the time which has passed since first implementation (in 1995), neither POL nor Fujitsu could provide any of the testing evidence from that time.
- **Monitoring controls** are business as usual activities implemented by management to regularly check that controls are still implemented and operating as expected. There was a general assertion by POL staff that Horizon processes millions of similar transactions a day without apparent pervasive issues or trends in incidents appearing to occur but neither POL nor Fujitsu provided documentary evidence to show such ongoing management monitoring of controls.
- **Specific testing** represents point in time, evidence based reviews of the correct operation of procedures and controls. Neither POL nor Fujitsu have commissioned any evidence based testing relating to Horizon's inherent controls, other than as part of the General IT Controls work above (that includes user access control testing).

POL00138402

These three areas were reviewed in the context of the five Matters. Based on our desktop review, noting the limitations and assumptions underpinning our work, our overall findings are:

- Matter 1 - "Horizon only allows complete baskets of transactions to be processed". From the documentation we have reviewed it appears that Horizon is designed such that only complete baskets of transactions can be processed.
- Matter 2 - "Baskets being communicated between Branch and Data Centre not subject to tampering, before being copied to the Audit Store". From the documentation we have reviewed, it appears that Horizon is designed such that data in transit between the Counter and the central system, and data stored in the central system before being copied to the Audit Store, has mechanisms that would enable tampering to be detected. It is however not clear from documentation to what extent these mechanisms are actively checked such that if any tampering occurred, it would be detected on a timely basis.
- Matter 3 - "Baskets of transactions recorded to the Audit Store are complete and 'digitally sealed', to protect their integrity and make it evident if they have been tampered with". From the documentation we have reviewed, it appears that Horizon is designed so that its Audit Store has a complete representation of Counter transactions and audit events, and the data would be kept with integrity for seven years.
- Matter 4 - "The Horizon Audit Store reports from a complete and unchanged record of all sealed baskets". From the documentation we have reviewed, it appears that Horizon is designed such that extracts from the Audit Store represent a complete and unchanged record of basket data.
- Matter 5 - "Horizon provides visibility to Sub-postmasters of all centrally generated transactions processed to their Branch ledgers". From the documentation we have reviewed, it appears that Horizon is designed such that the Sub-postmaster has visibility of all centrally generated transactions to their Branch ledgers in that accounting period. Central transactions require Sub-postmaster approval to be processed, except for Balancing Transaction postings. This appears to be an exceptional process, performed only by Fujitsu, and asserted by them to have only been used once (in 2010) between 2008 and the time of their assertion in this area (15th May 2014). Usage pre 2008 is currently not known.

4.3 Specific Comments – Other Key Controls (Further detail)

Our commentary below provides further descriptions of the specific Horizon Features identified and their sources which we consider to be relevant to each of POL's five Matters.

Matter 1: Horizon only allow complete baskets of transactions to be processed

Just like financial accounts it is essential that the books balance. In accounting terms, this is called "double entry book-keeping" i.e. for every debit there is a corresponding credit, so at all times the books balance by netting to zero. Horizon is designed to operate on this same principle. A group of Counter entries, typically relating to sales to the customer and the cash receipt from the customer, are called Baskets, and Horizon requires thateach basket must net to zero in order to be accepted (or "committed" in Horizon terminology). If a basket did not net to zero, it would mean something has gone wrong and the Sub-postmaster accounts would not balance.

Key Horizon Features, identified from Fujitsu's current day technical documentation provided to us are:

- Only baskets that balance to £0 can be accepted by the central database (double entry concept exists).
- Horizon records a basket into its central database as a single step. If there was a problem with this step, for example a technical issue like a network communications problem, nothing is recorded and an error message is sent back to the Counter system. Only complete baskets can thus be recorded.
- As part of the process of transmitting the basket to the central database, every basket is assigned a unique sequential number (called the Journal Sequence Number or "JSN"). The JSN enables the source Counter to be identified and provides information on the relative chronology of baskets from that Counter.

Documentation showing evidence based testing of the implementation and operation of these Horizon Features was not available. There was also no documentation provided to explicitly confirm that these Horizon Features have been in place from the inception of Horizon; however, POL and Fujitsu staff asserted that they have been in place since that time.

POL00138402

Matter 2: Baskets being communicated between Branch and Data Centre are not subject to tampering, before being copied to the Audit Store

POL can be confident that the data copied to the Audit Store is an accurate representation of the basket of transactions conducted with the customer, by ensuring that mechanisms are in place to enable the detection of any amended baskets, after they have been committed to the system.

Key Horizon Features, identified from Fujitsu's current technical documentation, E&Y's ISAE 3402 report and from verbal assertions provided to us by POL and Fujitsu include:

- A private cryptographic key is securely established.
- A digital signature is applied to each basket, pre-transmission of data from the Counter to the central database. This digital signature is a unique code for each basket, calculated by using industry standard cryptography using a 'key' managed by Fujitsu's Cryptographic Security Team. For control reasons, this team is operationally segregated from teams responsible for the day-to-day running of Horizon and administering of the databases. If the basket were to change, then the digital signature would be 'breached' and it would be possible to detect that the data had been tampered with. The presence of this Feature is only a control if the digital signature is checked at relevant points. Digital signatures are checked when data is extracted from the Audit Store, but we have not identified from documentation provided whether they are checked at points in the process up to and including the activity of copying data to the Audit Store.
- As part of the process of transmitting the basket to the central database, every basket is assigned a JSN The JSN forms part of the data that is digitally signed before transmission starts. The JSN is also a key control in this area, as its sequential nature provides a mechanism to both check thattransmissions from Counter to the central database have not gone missing, and to detect potentially phantom baskets.
- Database access privileges that would enable a person to delete a digitally signed basket are restricted to authorised administrators at Fujitsu.
- Database access privileges that would enable a person to create or amend a basket and re-sign it with a 'fake' key, detectable if appropriately checked, are restricted to authorised administrators at Fujitsu.

We have not identified any documented controls designed to:

- Validate the digital signature up to and including the point of copying data to the Audit Store (noting documentation asserts that it is validated during reporting from the Audit Store).
- Confirm that every JSN is present, without duplication or omission up to and including the point of copying data to the Audit Store (noting documentation asserts that checks are done during reporting from the Audit Store).
- Prevent a person with authorised privileged access to the digital signing process from sending a 'fake' basket into that digital signing process.

The Horizon Features relating to privileged database access rights have been assured under E&Y's ISAE3402 testing since 2012. As is usual with these reports, it does not describe the testing performed in sufficient granularity to enable us to determine the extent to which explicit privileged access has been tested. Documentation showing evidence based testing of the implementation and operation before this time, and for those other Horizon Features above, was not available. There was also no documentation provided to explicitly confirm that these Horizon Features have been in place from the inception of Horizon; however, POL and Fujitsu staff asserted that they have been in place since that time.

POL00138402

Matter 3: Baskets of transactions recorded to the Audit Store are complete and 'digitally sealed', to protect their integrity and make it evident if they have been tampered with.

POL can be confident that the data copied to the Audit Store is a complete and accurate representation of the basket of transactions conducted with the customer, until the point the basket is permanently deleted from the Audit Store (after seven years), by ensuring that mechanisms are in place to check the sequence of every Counter's transactions in the Audit Store and that both physical and logical mechanisms are in place to protect such data from amendment in the Audit Store.

Key Horizon Features, identified from Fujitsu's current technical documentation, E&Y's ISAE 3402 report and verbal assertions made to us by POL and Fujitsu staff are:

- Transactional data received into the central database is copied to the Audit Store during an overnight process. The Tivoli Workflow Scheduler (TWS) controls and monitors overnight processing to the Audit Store. Any issues or errors are reported and responded to by Fujitsu as part of day-to-day IT Operational activities.
- As part of this copying process, a 'digital seal' is applied to groups of baskets. The digital seal is additional to the digital signature described above in Matter 2 (indeed, the digital signature forms part of the data which is 'protected' by the digital seal). The digital seal is different to the digital signature in that it does not use cryptographic keys, relying instead on the physical hardware control described below to maintain the integrity of the digital seal itself.
- The Audit Store physically runs on separate specialist IT hardware which protects data once it is written, preventing alteration of data in the Audit Store. The digital seal codes are also written to the Audit Store, thus providing a source for integrity checking that they cannot be altered. If any data components within the relevant group of baskets were to be altered, go missing or get added to, then the digital seal for that group would be "breached" and thus the tampering could be detected. The configuration of the physical hardware does however permit administrators to delete data from the Audit Store during the seven year period, which was a matter found to be possible and contrary to POL's understanding of this physical protection Feature. This could allow suitably authorised privileged staff in Fujitsu to delete a sealed set of baskets and replace them with properly sealed baskets, although they would have to fake the digital signatures.
- Database access privileges that would enable a person to delete Audit Store data are restricted to authorised administrators at Fujitsu.
- Database access privileges that would enable a person to create new entries, re-sealing it with a valid, (publically available) 'hash' are restricted to authorised administrators at Fujitsu.

We have not identified any documented controls designed to:

- Prevent a person with authorised privileged access from deleting a digitally sealed group of data and replacing it with a 'fake' group within the Audit Store (which could still have a valid digital signature, if they have access to keys, and a valid digital seal created using a publically available formula).

The Horizon Features relating to access controls and overnight processing have been assured under E&Y's ISAE3402 testing since 2012. As is usual with these reports, it does not describe the testing performed in sufficient granularity to enable us to determine the extent to which explicit privileged access and Audit Store overnight process / error handling have been tested. Documentation showing evidence based testing of the implementation and operation before this time, and for those other Horizon Features above, was not available. There was also no documentation provided to explicitly confirm that these Horizon Features have been in place from the inception of Horizon, however, POL and Fujitsu staff asserted that they have been in place since that time.

POL00138402

Matter 4: The Horizon Audit Store reports from a complete and unchanged record of all sealed baskets.

POL wants to have a high degree of confidence that reporting from the Audit Store is based on reliable and accurate data.

Key Horizon Features, identified from Fujitsu's current day technical documentation, E&Y's ISAE 3402 report and verbal assertions made to us by Fujitsu and POL staff are that:

- The integrity of the digital seal is checked for all groups of baskets used in the extracts.
- The integrity of the digital signature is checked for all baskets used in the extracts.
- The complete sequence of JSNs is checked for the period from which the extract is performed.
- Exceptions identified by the above checks are formally raised and handled as part of day-to-day IT operational processes within the Tivoli Monitoring tool. As our work did not involve testing, we are not able to comment on whether such alerts have occurred or whether matters identified by the alerts have been resolved.

We have not identified any documented controls designed to:

- Formally report, review and consider the impact and resolution of any exceptions identified by the checks.
- Reconcile or check data reported from the Audit Store to other financial data used in the running or reporting activities of the business on a day-to-day basis.

The Horizon Features relating to the management of exceptions in the Tivoli Monitoring tool may have been assured as part of IT Operational testing in E&Y's ISAE3402 report since 2012. However, as is usual with these reports, it does not describe the testing performed in sufficient granularity to enable us to determine the extent to which this, and also explicit errors relating to JSN sequence, digital signatures and digital seals have been tested. Documentation showing evidence based testing of the implementation and operation before 2012, and for those other Horizon Features above, was not available. There was also no documentation provided to explicitly confirm that these Horizon Features have been in place from the inception of Horizon; however, POL and Fujitsu staff asserted that they have been in place since that time.

It was not in the scope of our review to assess the design of the ad hoc (bespoke) reporting processes in place in Fujitsu for ensuring that the extracted data is a complete and accurate response with respect to the reporting query.

Matter 5: Horizon provides visibility to Sub-postmasters of all centrally generated transactions processed to their Branch ledgers.

Based on verbal assertions from staff at POL and Fujitsu, there are three ways in which centrally generated transactions can be processed to a Sub-postmaster's ledger:

1. **Transaction Acknowledgement** processes – these create transactions to ledgers via the basket concepts described above, from non-Horizon third party systems in branches (such as Post and Go machines and Paystation terminals). Processes exist for each type of feed from third party systems and are operated by POL's finance service centre with full Sub-postmaster visibility and approval of entries via their local Counter system. Formal resolution processes exist for any disputes that may arise from this process.
2. **Transaction Correction** processes – these create transactions to ledgers via the basket concepts described above and are also known as 'adjustment postings'. A number of processes (over 30) exist which involve transaction corrections. These are operated by POL's finance service centre with full Sub-postmaster visibility and approval of entries via their local Counter system. Formal resolution processes exist for any disputes that may arise from this process.
3. **Balancing Transaction** process – this is an emergency process, accessible only to restricted individuals in Fujitsu, which can create transactions directly in Branch ledgers. This process creates an identifiable transaction in the ledger, verbally asserted by POL staff to be visible to Sub-postmasters in their branch reporting tool, but does not require positive acceptance or approval by the Sub-postmaster. The use of the process has a full audit trail, monitored by Fujitsu. It is asserted by them that the process has only been used once (in 2010) between 2008 and the time of their assertion in this area (15th May 2014). As our work did not involve testing, we cannot comment on the circumstances behind this event.

POL00138402

Documentation relating to these processes is either not available or significantly aged, so key Horizon Features, based on limited documents and principally verbal assertions from POL and Fujitsu staff are:

- All processes, with the exception of Balancing Transactions, operate on the principle of full Sub-postmaster disclosure and acceptance.
- All processes create an identifiable transaction in Horizon, with an audit trail to the originator in the finance services team. This transaction is protected by the JSN, digital signature and digital seal Features as described above.
- For any outstanding (non-accepted) Transaction Acknowledgement or Transaction Correction at month end, a formal resolution process exists which enables non-accepted items to be identified, held in suspense and actively investigated to the point of resolution with the Sub-postmaster. Business as usual resolution activities can be taken to conclude outstanding items and have them cleared down. It was outside the scope of our review to assess or test these resolution processes and the nature of the day-to-day acknowledgements, corrections and/or disputes that exist.
- Balancing Transactions processes are controlled by Fujitsu via formal change control and monitoring processes. An audit trail is retained over the use of this process and, since 2008, when reporting became easier, it is asserted by Fujitsu staff that the audit trail is monitored by a Fujitsu department independent of those with access to the function also in Fujitsu. The degree of formality over this monitoring, and its frequency, is unknown. It is also not known if or how often the process was followed pre-2008.
- Sub-postmasters have access to view all transactional records underpinning their current accounting period's ledgers. This information is used to support their daily branch cash declarations and reconciliation, their weekly balance of cash and stock and reconciliation and their monthly trading period roll over activities.

We have not identified any documented controls designed to:

- Routinely monitor all centrally initiated transactions, to verify that they are all initiated and actioned through known and governed processes.
- Reconcile or check data sources which underpin current period transactional reporting for Sub-postmasters to the Audit Store record of such activity.

The Horizon Features relating to the management of Balancing Transactions may have been assured as part of testing in E&Y's ISAE3402 report since 2012. As is usual with these reports, it does not describe the testing performed in sufficient granularity to enable us to determine this, and the extent to which the explicit activities and audit trails have been tested. Documentation showing evidence based testing of the implementation and operation of these Horizon Features was not available. There was also no documentation provided to explicitly confirm that these Horizon Features have been in place from the inception of Horizon; however, POL and Fujitsu staff asserted that they have been in place since that time or from the point that the process was first implemented (for example, the Post & Go and Paystation processes were fundamentally improved in 2011/2012).

POL00138402