POL00222758

Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

Horizon: Desktop Review of Assurance Sources and Key Control Features

Draft for discussion

23 May 2014

DRAFT: Version 16
SUBJECT TO LEGAL PRIVILEGE

POL00222758

Contents

POL00222758

1 Executive Summary

Context

As outlined to us by the Post Office Limited ("POL") litigation team, " *POL is responding to allegations from Sub-postmasters that the "Horizon" IT system used to record transactions in POL branches is defective and that the processes associated with it are inadequate (e.g. that it may be the source and/or cause of branch losses). POL is committed to ensuring and demonstrating that the current Horizon system is robust and operates with integrity, within an appropriate control framework.*"

POL is confident that Horizon and its associated control activities deliver a robust processing environment through three mechanisms: POL have designed features directly into Horizon to exert control; POL operates IT management over Horizon; and POL have implemented controls into and around the business processes making use of Horizon. Collectively these three approaches of inherent systems design, ongoing systems management and business process control are designed to deliver a Horizon processing environment which operates with integrity.

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

Deloitte has been appointed to:

- consider whether this Assurance Work appropriately covers key risks relating to the integrity of the processing environment,
- to extract from the Assurance Work an initial schedule of the Horizon Features[1],
- to raise suggestions for potential improvements in the assurance provision.

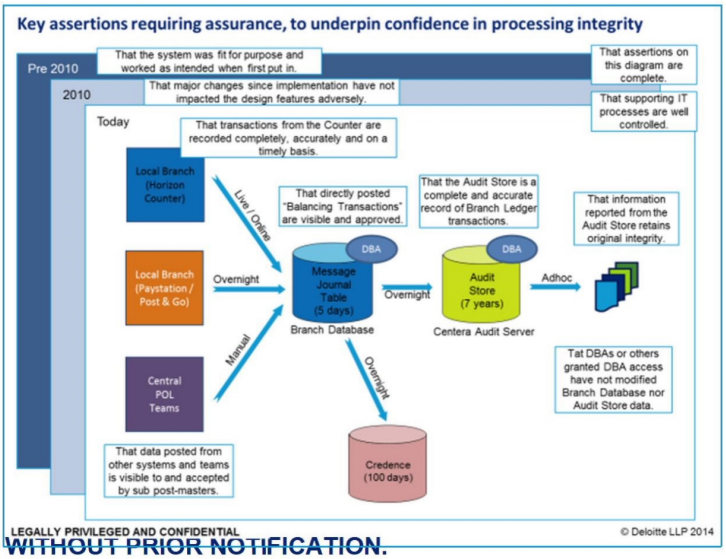
[1] "Horizon Features" is a term we have introduced to represent those features of the Horizon processing environment, including IT management and business use controls, which provide that:

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

Summary of Approach

We have structured our work around the key control assertions shown in the diagram (right), which has been agreed with POL. We consider these to be key matters that POL should control in order to gain comfort over the integrity of processing.

We have considered POL's three design approaches when evaluating the Assurance Work.



POL00222758

A key element of the approach was to identify the Horizon Features. POL did not have an existing document that could be described as representing the Horizon Features in a demonstrably complete way, therefore we have drawn out an initial view of the Horizon Features from the underlying documentation and considered Assurance Work relating to them (Appendix 2) for the purposes of this review.

As communicated to us by management, we have also considered the following 5 key control objectives during our activities to identify Horizon Features:

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.

These key control objectives are an important subset of the overall set of key control assertions highlighted in the diagram above.

We have grouped the Assurance Work provided to us into three areas, corresponding to POL's three mechanisms of exerting control over the processing environment, as follows:

- ***System Baseline Assurance Work:*** This aims to provide comfort that the original Horizon implementation and other changes performed under formal projects were well governed (compared to Deloitte project management methodologies) and that detailed testing was performed against agreed business requirements. Such activity would verify that the system was, at that point in time, fit for purpose and implemented as intended. This assessment considers the point when the system and processes are created.

- ***IT Provision Assurance Work:*** This aims to provide comfort that the IT management activities required to run the Horizon system with integrity are designed and operating effectively. Such activity verifies that key day-to-day IT management activities (e.g. security, IT operations and system changes) are appropriately governed and controlled.

- ***System Usage Assurance Work:*** This assurance aims to provide comfort that the controls in and around the business processes which make use of the Horizon system are appropriately designed, in place and operating as intended.

Our work has been performed as a desktop review of documentation made available and has neither tested the quality, completeness or accuracy of the Assurance Work provided to us or tested any controls relating to the Horizon processing environment.

Summary of Observations

Substantial Horizon-related system documentation exists, comparable to that typically seen in organisations of a similar scale where IT activities are outsourced and formal assurance activities are not mandated. Some organisations are externally mandated to have a greater level of end-to-end, risk orientated documentation and testing, e.g. in financial services. POL is not so mandated.

Based on our review of the available documentation, our key observations are:

- The extensive Horizon system documentation is structured from a technical rather than a risk and controls perspective and provides an understanding of the Horizon Features. POL should conduct a formal

POL00222758

assessment to identify a complete set of Horizon Features that respond to POL's control objectives.

- The integrity of the Audit Store is designed to be preserved by a system of "digital seals" and "digital signatures". This feature underpins the ability to confirm the completeness and accuracy of data kept in the Audit Store, and that of subsequent reports generated from the Audit Store. These digital seals and digital signatures are both key components in the Horizon Features which are both validated during the extraction process from the Audit Store.

- POL is relying on the Horizon Features being implemented and operating as described. Whilst our review focussed on the design of the Horizon Features, the Assurance Work we have assessed does not completely test these features for implementation and operating effectiveness. Only those Horizon Features relating to IT Provision have been validated and tested by independent third parties. In addition, during the course of our engagement, one of the Horizon Features has been discovered by POL to not be implemented as expected.

- Business use (process) documentation is not complete or up to date, by some years in cases. As part of completing or updating the documentation of Horizon Features, all relevant business uses should be identified and evaluated from a control objectives perspective to identify potential additional matters being relied upon.

- Pre 2010 Baseline Assurance Work could not be provided by POL. This Assurance Work is required to evaluate the comfort that the system was originally built and tested to specific business requirements. The implementation in 2010 of HNG-X is asserted by POL to have not significantly impacted the design of the Horizon Features.

- Governing controls over key, day-to-day IT management activities have been independently tested and opined by Ernst and Young (since 2012) to a recognised assurance standard (ISAE3402).

- A number of third party systems are used by Horizon on a day-to-day operational basis. Documentation asserts that these interactions do not impact on the Horizon Features.

Scope Limitations

Our work has been subject to the following exclusions:

- Only matters relating to the Horizon Features within the Horizon processing environment have been considered during our review;

- 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;

- We have not had direct contact with any third parties other than named contacts that you have provided to us (Appendix 3);

- We have not verified or tested any information provided directly by you, or directly or indirectly by third parties (the schedule of information received is in Appendix 3);

- We have not reviewed any contractual provisions in place between you and third parties;

- 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.

POL00222758

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 tested any of the Horizon Features; and
- We have not validated or commented on the quality of the Assurance Work supplied to us.

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.

POL00222758

2 Introduction

Introduction

The Horizon system has been used by POL since 1995. During this time it has processed many millions of transactions across thousands of branches. Horizon is accredited by Payment Card Industry Data Security Standard (PCI DSS) and ISO27001. It is currently used by more than 68,000 users across 11,500 POL branches and is administered by Fujitsu as part of a managed service agreement. It is a key operational system for POL and integrity of processing on the system is crucial to the day-to-day operations of the business.

POL is responding to allegations that the Horizon processing environment, used to record transactions in POL branches, is defective and/or that the processes associated with it are inadequate.

In order to respond better to the allegations (which have been, and will in all likelihood continue to be, advanced in the Courts), POL management want to demonstrate that the Horizon processing environment is robust and operates with integrity, within an appropriate control framework.

In particular, management at POL has highlighted two key statements they would like to assess their comfort over in response to the allegations, being:

1. That Sub-postmasters have full ownership and visibility of all records in their Branch ledger; and
2. That the Branch ledger records are kept by the system with integrity and full audit trail.

These statements have then been further sub-divided into the following statements:

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.

POL management have previously either been provided with or commissioned work (including independent assurance reviews) into matters relating to Horizon's operating environment and processing integrity. Documents outlined in Appendix 3 have been provided to us and considered as part of the planning and delivery of our review.

Objectives and Activities Undertaken

The purpose of this report is to provide, based upon the information made available to us by you, an independently produced summary of the Assurance Work undertaken over your current day Horizon processing environment and make recommendations on further work that could be done to enhance these assurance sources.

The work we have performed to produce this report has included:

- Obtaining an understanding of the Allegations; POL's key risks in and internal controls over the Horizon processing environment relevant to the integrity of processing; the measures in place to record and preserve the integrity of system audit trails and other background matters that we may deem necessary to complete our review;

POL00222758

- Obtaining an understanding of the key differences between the current Horizon processing environment, and the system which this replaced (here-to referred to as the "Legacy System");
- Reviewing, understanding and consolidating the Assurance Work (e.g.: investigations, assurance activities and remediation actions) which POL or third parties have undertaken;
- Holding discussions with relevant members of POL staff and other key stakeholders;
- Reviewing project documentation relating to the 2010 implementation of Horizon, in order to compare the nature and extent of project governance and documentaton with Deloitte's good practice project management methodology;
- Preparing an initial schedule of Horizon Features and assessing the level of comfort over these, provided by POL's Assurance Work (including the use of a specialist to assess the design of the Audit Store's tamper proof mechanisms); and
- Recommend further activities that management could undertake to improve the assurance provision.

Scope limitations and assumptions are outlined in the Executive Summary above.

Understanding of Historical Issues and Concerns

As an initial step, in building the requisite understanding required of the historical context leading to this review, we have reviewed the documentation provided by POL in order to understand the history of issues and concerns which have been raised in relation to the system.

From the documents provided, we have identified the following matters which have helped to provide us with a high level understanding of the nature and extent of the potential concerns with the Horizon processing environment, and thus focus our work in certain higher risk areas:

Branch 14 Issue - Involved a processing error where historic accounting entries in the 2010/11 financial year were replicated in accounts for 2011/12 and 2012/13.

Branch 62 Issue - Involved a Receipts and Payments mismatch in Horizon when discrepancies were moved into the local suspense account (this is an account which aggregates all discrepancies into a single gain or loss for a branch trading period).

Falkirk Issue - The Falkirk Anomaly occurred when cash or stock was transferred between stock units.

Spot Review Bible – This outlines a sequence of matters raised during the work performed by Second Sight over the allegations raised over the Horizon system, and summary commentary on 10 issues within.

Lepton Detailed Spot Review Information (included within Spot Check Bible) – Detailed documentation has also been provided in relation to Spot Review 1. The issue raised was that a Sub-postmaster will not be notified about automatic reversals of transactions when not connected to the data centre.

Reflecting on the nature and substance of these issues, and documentation relating to their follow-up and resolution, we have understood the importance of the audit trail to provide evidence relating to disparities between Sub-postmaster accounts of events and subsequent investigations, based on audit trail evidence, by POL/Fujitsu.

As a result of the above understanding, our work relating to IT Provision and System Usage Assurance Work paid particular (but not exclusive) focus on Information System Operations (IT environment processing), and business processes controlling relevant key data flows (the key data flow for our assessment being that of the complete and accurate transmission of data from the Counter system at the Branch to the Branch Database and subsequently into the Audit Store).

POL00222758

3 Approach

In the absence of POL's own holistic risk assessment relating to the Horizon processing environment, key to our assessment of sources of assurance has been the formulation of an initial "risk universe", against which coverage of the associated risks by the relevant sources of assurance can be assessed ("mapped").

We have considered this risk universe across three key areas:

1. Control objectives and risks relating to the 'System Baseline'.
2. Control objectives and risks relating to 'IT Provision'.
3. Control objectives and risks relating to 'System Usage'.

Risks relating to the System Baseline – these are risks that the original implementation project and other changes performed under formal projects were not conducted in line with good project management practices, and that detailed testing was not performed against agreed business requirements. These risks are governed and controlled outside of day-to-day system operating procedures. Controls which mitigate these risks are often referred to as "Project Controls" and "Inherent System Controls" (those designed and built into the IT system).

Risks relating to IT Provision – these are risks that the underlying IT activities, necessary to provide a system that can run and be used with integrity, are not designed and operating effectively. Such risks relate to key day-to-day IT management activities, relating to security, IT operations and system changes. Controls which mitigate these risks are often referred to as "General Computer Controls". Our work focussed on assurance provided over Fujitsu's activities in these areas.

Risks over System Usage – these are risks that key features of Horizon and corresponding business use activities (processes), aiming to prevent or detect matters that would impact the integrity of processing, are not designed, in place or operating as intended. These are the more detailed risks in relation to particular aspects of capturing and processing transactions across the Horizon processing environment. Controls which mitigate these risks are often referred to as "End User Controls", "Application Embedded Controls" and "Process Controls". Our work focussed on the internal dataflows within Horizon (Counter to Branch Database to Audit Store for example) and we also considered the relevance of interfaces with other systems such as the DVLA.

In the context of these three areas of risk we have performed knowledge gathering activities in order to understand the Horizon processing environment in sufficient detail to identify specific risk areas and those Horizon Features identified to exert control over these risks.

1. Approach to Understanding of System Baseline Risks

In considering Baseline risks we have considered past iterations and changes to the Horizon IT system, including:

- Any that lead to changes to the Audit Store;
- The Horizon Implementation Programme in 2010-2011;
- The Data Strategy Foundation project in 2012 and 2013 (which updated the dataflows into Horizon from certain third party transactional systems, including 'Post and Go', and 'Paystation +'); and
- The original Horizon platform delivered in 1995.

POL00222758

2. Approach to Understanding of IT Provision Risks

Our understanding of IT Provision risks has been formulated through our understanding of the system via documentation review and verbal discussion with supporting POL and Fujitsu SMEs. Due to the nature of the System Provisioning risk areas, the formulation of this understanding has been mainly through interview with Fujitsu and POL security team members.

3. Approach to Understanding of System Usage Risks

Our understanding of System Usage risks has again been formulated through documentation review and verbal discussion with supporting SME's to identify additional support areas. Due to the nature of the System Usage risk areas, the formulation of this understanding has been mainly through interview with Fujitsu, POL Finance Shared Services and POL Security team members.

4. Approach to Consideration of the Horizon Features

In the formulation of our risk universes across the three areas highlighted in 1 – 3 above we have considered the 5 key matters relevant to the Horizon Features as instructed by management:

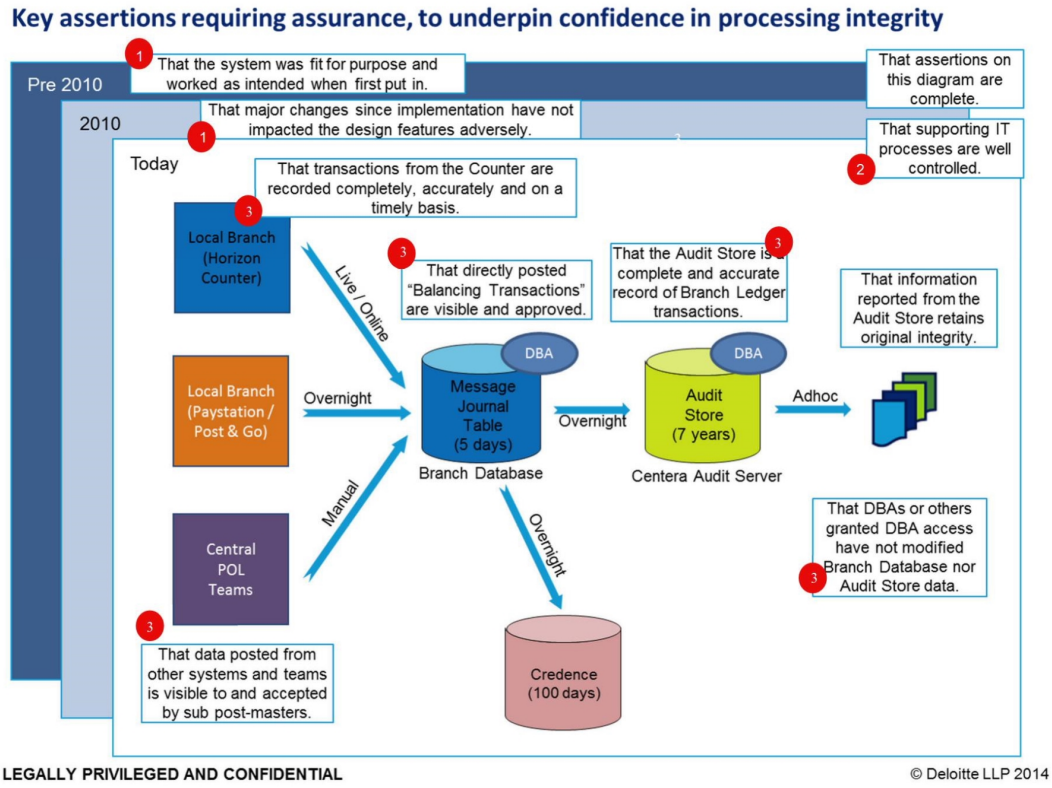
1. Horizon only allows complete baskets of transactions to be processed;
2. Baskets being communicated between Branch and Data Centre are not subject to tampering before being copied to the Audit Store;
3. Baskets of transactions recorded to the Audit Store are complete and 'digitally sealed', to protect 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.

5. Combining the Above

Following our assessment across these four areas, the diagram below (see overleaf) describes the key risks identified within the Horizon processing environment. We have number coded the risks in the below with **(1)** corresponding to Baseline Risks, **(2)** corresponding to IT Provision Risks, and **(3)** corresponding to System Usage Risks.

This diagram thus represents the framework of key risks that need to be controlled by Horizon Features and appropriately assured in order to provide the comfort required by POL management.

POL00222758

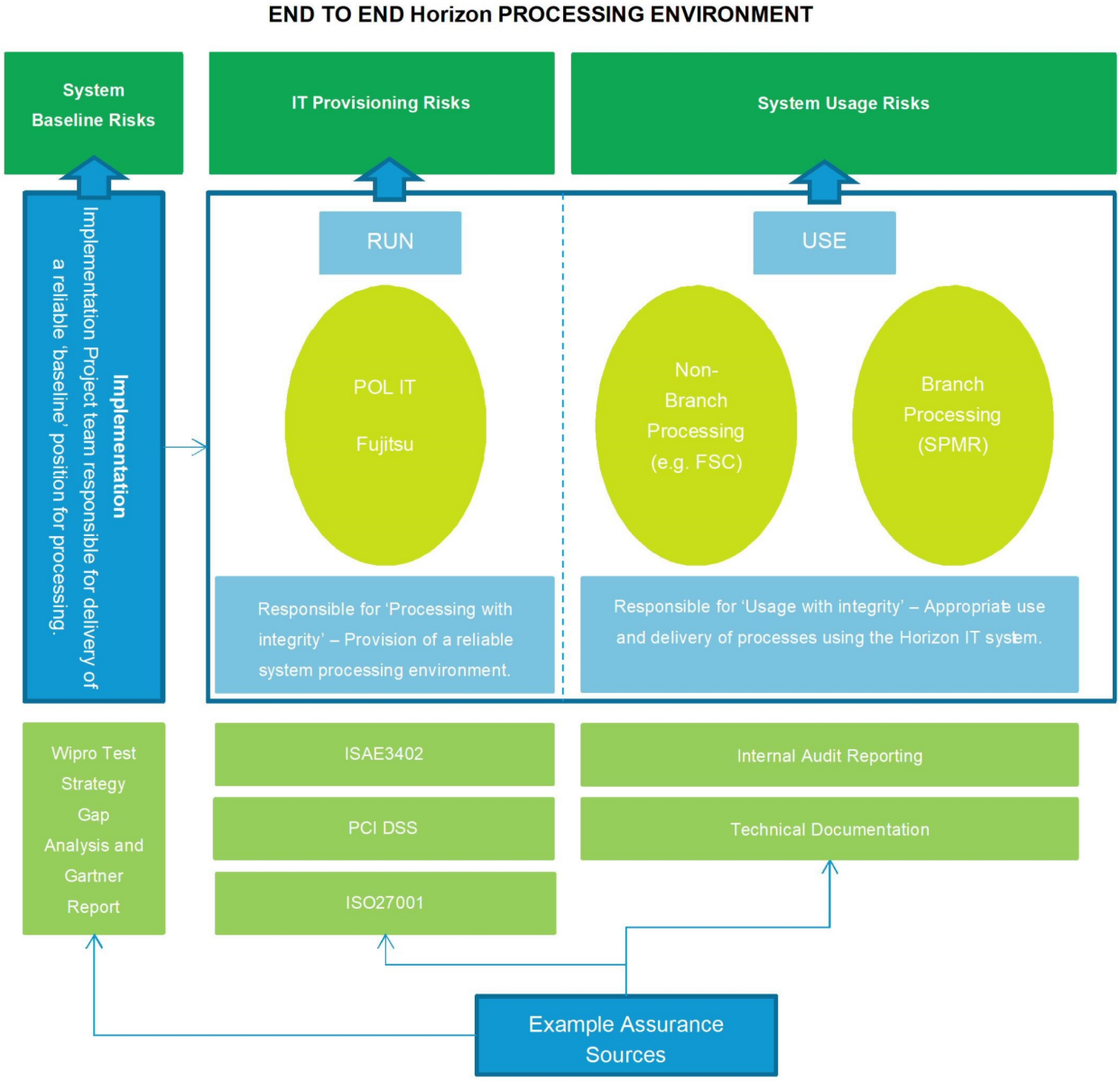


It can be observed that the majority of the risks identified are System Usage risks, which is expected based on the complexity of the IT processing landscape and the diversity and volume of transactions being handled.

POL00222758

Sources of Assurance Work relating to the Horizon Processing Environment

The diagram below summarises key examples of the Assurance Work reviewed and referred to as part of our assessment.



When considering the sources of assurance over IT Provision Risks, System Usage Risks and System Baseline Risks, a number of parties have been (and continue to be), involved in performing work over the Horizon processing environment which contributes to the overall assurance management has over the correct operation of the system.

Assurance Work from the following organisations, in addition to information provided from POL, have been identified and considered in our work:

- Fujitsu, who designed, built and now operate Horizon;
- Bureau Veritas, who perform ISO27001 certification over Fujitsu's networks, including that of Horizon;
- Information Risk Management (IRM) who accredit Horizon to PCI DSS;

POL00222758

- Ernst & Young, who produce an ISAE3402 service auditor report over the Horizon processing environment; and
- Internal audit, who perform risk based reviews within POL.

In considering the Assurance Work provided to us by management during the course of this engagement we have considered whether they constitute assurance provided under an assurance engagement, as defined by IFAC, or are sources of information that provide comfort in other ways. For the purposes of clarifying the Assurance Work, we have assigned each document received to one of two classifications, defined as follows:

"Assurance" –The Assurance Work has been provided under an assurance engagement by an independent third party, suitably qualified in the subject matter constituting the focus of the engagement to provide a valid opinion. Sources of such assurance include:

- Internal Audit functions;
- External Audit; and
- Other third party reviews, not involved in the original design nor day-to-day operation of the system containing (a) a formal opinion, such as those performed in line with recognised standards, such as ISAE3402 or (b) no formal opinion (i.e. a report based on evidence and facts without interpretation).

"Other Sources of Comfort" – The Assurance Work is either not produced by an independent party or by an individual who is suitably qualified in assurance engagements, or both. Other sources of comfort include:

- IT Project Documentation;
- Operational Documentation, such as policies, procedures and process / system information produced by functional teams;
- Reviews or investigations performed by outsourcers (e.g. deep dives, diagnostics, spot reviews);
- Business peer group review teams and functions; and
- 'Second line' compliance teams.

In Appendix 3 we have documented all the Assurance Work we received and added our classification of those sources by these two categories.

Summary of Work Performed

Based upon the concepts outlined above we have performed the desktop based work below (further detail of which is outlined in our Engagement Letter shown in Appendix 4). We have not performed any testing to validate the information provided to us as part of our work.

Step 1: Analysis and Review

- **Activity 1. Documentation Review -** We have reviewed a number of documents produced by several different organisations in order to understand key matters relating to the Horizon system and the Assurance Work available.

- **Activity 2. Risk Universe Formulation -** We have then, in the absence of a holistic risk assessment being performed by POL and thus for the purposes of our assessment, created a risk universe based on our experience of information processing systems encompassing the three primary risk areas previously identified IT Provision, System Usage and Baseline Risks. The five key matters for consideration outlined by management were also considered during this process.

- **Activity 3. Review of Assurance Work –** The available documentation was reviewed in order to understand the Assurance Work available to POL, against each of the three identified risk areas.

POL00222758

Step 2: Gap Analysis and Assessment

Based on the analysis in Step 1 we have produced:

- **Activity 4. System Provisioning Assurance Assessments and Gap Analysis -** Considering key potential gaps or areas of ambiguity in the available assurance sources when considering the System Provisioning risk universe.

- **Activity 5. System Usage and Baseline Assurance Assessments and Gap Analysis –** Assessing the documentation relating to System Usage Risks and then performed deep dives into the following areas of specific risk:

    - *Horizon interfaces (including DVLA);*
    - *Branch Database;*
    - *Audit Store;*
    - *Horizon Implementation Project;*
    - *Audit Store Changes; and*
    - *Data Strategy Foundation project.*

- **Activity 6. Peer Comparison to Assurance Available to Similar Organisations –** We have assessed the Assurance Work available to similar organisations over System Provisioning Risks (the area of risk where a benchmark is most valid due to the level of information available from POL) and assessed therefore whether POL has comparable levels of assurance.

Step 3: Reporting

The analysis and interpretation in Step 2 has allowed us to formulate:

- **Activity 7. Produce an Assurance Schedule over Horizon Features, and Recommendations –** Mapping control assertions, Horizon Features and Assurance Work and reporting on the level of comfort that we have assessed in each of these areas. Identification of the key considerations for management arising from our analysis and plan of action to respond to these recommendations.

A more detailed description of these activities performed follows.

Activity 1: Documentation Review

All of the documentation reviewed during the course of our review has been documented within Appendix 3. This documentation can be divided into the following classifications:

- Technical documentation on the Operation of the Horizon System – Reviewed in order to gain a deeper understanding on how the Horizon system works, how complex it is, and where we should be focusing further efforts and analysis;
- Independent Third Party Assurance documentation – This documentation has been reviewed in order to understand the existing assurance sources relevant to the environment;
- Documentation of Historical Issues and Allegations in relation to the Horizon System – This documentation has been reviewed in order to understand the background context and better position the IT Provision, System Usage and Baseline System risk work performed over the environment; and
- Service Provider Analysis and Response to Issues – This documentation has been reviewed to gain an understanding of the work performed by Fujitsu in investigating the issues raised, and how these will be responded to.

POL00222758

A number of individuals from POL have been interviewed during the course of formulating this report to supplement our understanding from the provided documentation.

Activity 2: Risk Universe Formulation

System Baseline Risk Universe

The original implementation of Horizon in 1995, together with subsequent changes (whether routine via change management processes, or large complex change programmes such as the Horizon system implementation in 2010-11), represent events affecting Baseline System Risk.

To assess these risks we have understood the history of the Horizon system and selected three areas for more detailed investigation including:

- Horizon Implementation;
- Data Strategy Foundation project; and
- A sample of changes to the Audit Store (subsequent to determining that this key risk area for the system had been left largely untouched by the key implementation events highlighted in the previous two bullets).

For each of these change areas we have assessed the Assurance Work from a governance and control perspective, and POL ability to take comfort that the Horizon system was fit for purpose at the time of the change and operated in line with management intentions (through business requirements definitions and project testing against these).

IT Provision Risk Universe

This risk universe was formulated from our prior experience of auditing and assuring information systems and involved the identification of high level risks across three core areas:

- Information Security;
- Information System Operations; and
- Change Management.

Once the IT Provisioning risk universe had been formulated a mapping of control objectives within the Assurance Work was performed in order to assess coverage.

The three sources of assurance included within this mapping were:

- ISAE3402 report on the Horizon managed service;
- PCI DSS compliance report on Horizon; and
- ISO27001 Statement of Applicability.

System Usage Risk Universe

As POL has not conducted a holistic assessment of risk in this area, a full understanding and assessment of assurance over the System Usage risk environment was not available for our review.

Instead we focussed our assessment on two key areas of risk: those relating to the completeness and accuracy of the Audit Store, the Branch Database and key system interfaces with a significant third party, such as the DVLA. We sought to understand the Assurance Work that has been done against each of these areas.

This involved:

- Enquiry with relevant SMEs;
- Review of documentation;

POL00222758

- Formulation of a risk universe in these specific areas; and
- Understanding of existing assurance work over controls which mitigate these risks.

Horizon Features

Across each of the three risk universes we identified features within the processing environment that exert control and provide that:

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.

We refer to these identified features as the "Horizon Features" and identification of these features in response to the matters for consideration listed above was a core component of our work.

Activity 3: Review of Assurance Work

With the background context of the three risk universes outlined within the previous section, we reviewed the available Assurance Work in order to assess the coverage and nature of the comfort provided by the work.

The documentation reviewed during this stage has been listed within Appendix 3, as are the names of individuals consulted in relation to our work.

Activity 4: System Provision Assurance Assessments and Gap Analysis

Once the System Provisioning risk universes had been formulated a mapping of control objectives within each of the main assurance sources was performed in order to assess coverage. The three sources of assurance included within this mapping were:

- ISAE3402 report on the Horizon managed service;
- PCI DSS compliance report on Horizon; and
- ISO27001 Statement of Applicability.

The results of this mapping exercise are summarised within Section 5 and reproduced, in detail, within Appendix 1.

In parallel to this assurance exercise we have also summarised key matters relating to each assurance source. This involved considering the context and focus of the relevant Assurance Work and comparing these to the context and focus that would be required for coverage of the key risks (this was in recognition of the risk that some of the documents could be used or applied out of context from their original purpose).

Activity 5: System Usage and Baseline Assurance Assessments and Gap Analysis

Following our understanding of the system and historical issues the following areas were singled out as relevant for deeper analysis, and this approach was agreed with POL management:

1. **Audit Store –** The audit store has been used frequently in investigations by POL / Fujitsu and is used as supporting evidence during legal proceedings. Therefore its integrity is paramount to responding to these issues. However the audit store cannot be relied on in isolation, as its integrity is dependent upon the correct processing of transactions by the wider Horizon system (upstream events if processed incorrectly will be recorded incorrectly by the audit store).

POL00222758

2. **Horizon interfaces (including DVLA) –** Horizon is reliant on a significant number of batch processes and online services (including interfaces with third party systems) in order to function correctly. These routines need to be functioning correctly and accurately for the transactions processed by the system and ultimately recorded in the audit trail to be reflective of the underlying commercial realities and business transactions they pertain to represent.

3. **Branch Database –** The Branch Database is a key 'staging post' for data being transacted on counters within individual branches prior to transmission onwards to the Audit Store. As data from branches in held within the messaging journal table on this system for up to a day before being processed into the audit store the security controls and processes protecting this data whilst in temporary storage here are paramount.

4. **Horizon Implementation Project –** This change represented the largest single change to the Horizon system since implementation, and also the change implemented prior to adoption of the current major release of the system, and so was considered of particular relevance to our overall understanding of Baseline System risk.

5. **Audit Store Changes –** Our understanding of the HNG-X Implementation Project quickly highlighted that this project had very little impact on the Audit Store itself. As a result we performed procedures to understand some of the changes which had been made to the Audit Store following its original implementation.

6. **Data Strategy Foundation Project –** We determined during the course of our work that this was another key implementation project in the recent history of the Horizon system of particular relevance to a sub-group of the system interfaces on Horizon. This project was therefore also deemed key for our understanding of system Baseline risk.

For each of the areas outlined in 1 – 6 above an assessment was made of the coverage and nature of the Assurance Work provided.

For areas 1 - 3 (System Usage Risks) the functionality of the particular area was further understood and key controls over the corresponding risks then sought.

For areas 4 - 6 (System Baseline Risks) we adopted a different approach, whereby the typical good practise documentation requirements and project governance methods as stipulated by 'Prince 2' (amongst others) were utilised as a baseline, and the approach to each of the sampled change initiatives assessed from the available documentation. This work was conducted through a mixture of verbal discussion and the receipt of supporting evidence where applicable.

Activity 6: Peer Comparison to Assurance Available to Similar Organisations

As part of our analysis we have also assessed whether the IT Provision assurance POL has obtained is proportionate to that provided to similar organisations.

We have also considered the best practice approach outlined by the COSO framework, as published by The Committee of Sponsoring Organisations of the Treadway Commission, in formulating suggestions for potential areas of improvement in the risk, control and assurance activities of POL.

POL00222758

The COSO Cube: Presents a framework for best practice approaches to risk, controls and assurance activities.

Activity 7: Produce an Assurance Schedule over Horizon Features and raise Recommendations and Plan of Action

We have written up our assurance schedule, which maps the Assurance Work to specific controls relating the Horizon Processing Environment, and commented on the level of comfort that the Assurance Work provides in each area.

Our report also contains recommendations for management together with a suggested plan of action for management consideration.

POL00222758

4 Understanding the Horizon Processing Environment

Overview of the Processing Environment

The Horizon IT system was designed specifically for POL, and therefore an understanding of its operations, processing environment and configuration was required in order to fully quantify the risks applicable to the IT components of the processing environment.

Horizon has been the main operational system of POL since 1995 and:

- Has a user base of 68,000 users;
- Terminals within 11,500 branches;
- Processes an average of 6 million transactions a day; and
- Interfaces with over 20 third party systems.

As highlighted in our 'Approach' section above, we have categorised the risks posed on the system into three distinct areas (System Baseline Risk, IT Provision Risk and System Usage Risk), and the remainder of this section outlines our understanding of the IT system that underpins these.

System Baseline Risk

Horizon (HNG-X) Project

The change to the HNG-X system in 2010 was governed using Royal Mail's "Harmony" project methodology (the governing project standard at the time). The project saw the phased implementation over 18 months of the HNG-X solution (also known as "Horizon On-Line"). Individual POL Branches were migrated from the Legacy System to the new HNG-X system, one by one.

No historical data was migrated, although six months of data was maintained within the Legacy System. Our review of Assurance Work shows that a number of key controls were operated over the project, which was managed by Fujitsu on behalf of POL. These included:

- POL signing off acceptance criteria;
- A phased migration including a model office pilot; and
- Branch by branch reconciliation between opening balances on the new system and closing balances on the legacy system.

Wipro, an independent third party, were commissioned to provide a report on the performance testing strategy including gap analysis and recommendations, and Gartner provided an assessment of the overall system design and strategy.

The benefits from the migration included the removal of transactional data being held at local branches levels and this data instead being stored centrally within the data centres.

Data Strategy Foundation Project

The project focused on moving the Accounts Payable file feed which was initially received into Credence via Transaction Integrator to processing via Fujitsu Horizon systems (i.e. not the Counter). The goal of the project was

POL00222758

to provide a longer term system solution which would provide complete reconciliation, resilience and disaster recovery capabilities, as well as reduce the risk of client withdrawal.

The POL strategic requirements to expand its offerings to other platforms beyond Horizon introduced the requirement for a data integrator function. Originally POL approached Fujitsu Services to supply this service as plans to incorporate an integrator service within the Horizon architecture were considered to represent a clean solution. However, Fujitsu Services were unable to respond within the desired timescales as it would have diverted their resources from key Horizon on-line delivery milestones.

POL therefore investigated alternative options, finally selecting the use of IBM datastage as the Transaction Integrator. This was delivered as part of the POLMI project. Fujitsu Services then submitted a high level design proposal for the provision of a service for processing client transaction files which would provide end-to-end data validation / reconciliation, with resilience and DR (the incumbent IBM datastage solution did not provide resilience, DR or end to end reconciliation, presenting a threat to relationships and future contracts).

Assurance Work provided included:

- Project overview document;
- Business Case;
- Weekly Project Meeting Committee Presentation;
- Business Requirements;
- Test Strategy;
- Test Sign off; and
- Test Report.

Audit Store Changes

In assessing change risks in relation to the Audit Store, documentation has asserted that the recent significant changes above did not result in significant changes to the operation of the day-to-day Counter transaction flows or the operation of the Audit Store.

To assess Baseline risk for the Audit Store the original implementation documentation for the Audit Store was requested. Due to the data retention policy this documentation could not be provided and so a review of Fujitsu provided documentation over subsequent changes over a large period of the Audit Store's history was performed.

In producing the diagram on page 9, we have considered the key System Baseline Risks in the context of two control assertions below, which became the overall focus of our work in this System Baseline area:

- The Horizon Features were fit for purpose and worked as intended when first implemented; and
- Major changes since implementation have not significantly impacted the Horizon Features.

POL00222758

IT Provision Risk

As part of our work, through review of documentation and discussions with subject matter experts in POL, we familiarised ourselves with the topology and operations of the Horizon IT system.

The systems documentation and understanding obtained (shown in summary in diagrams below) highlights the complexity of the Horizon IT system and the level of data being transacted via batch and real-time data flow. This volume and level of complexity in the data flows, including interactions with other systems, highlights the importance of effective IT Provisioning controls to the integrity of the processing environment.

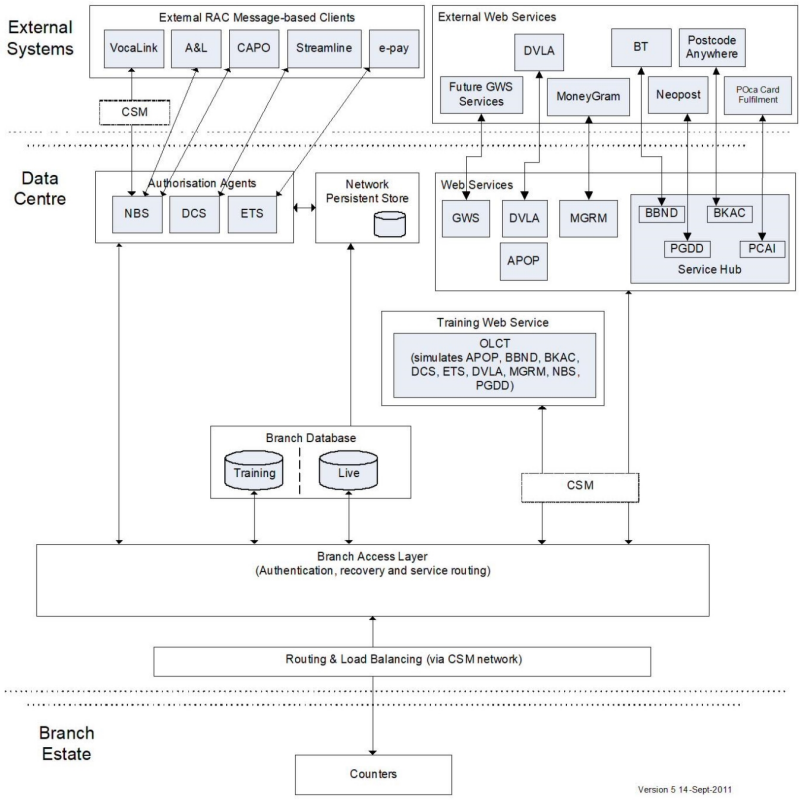


Diagram provided by Post Office Limited

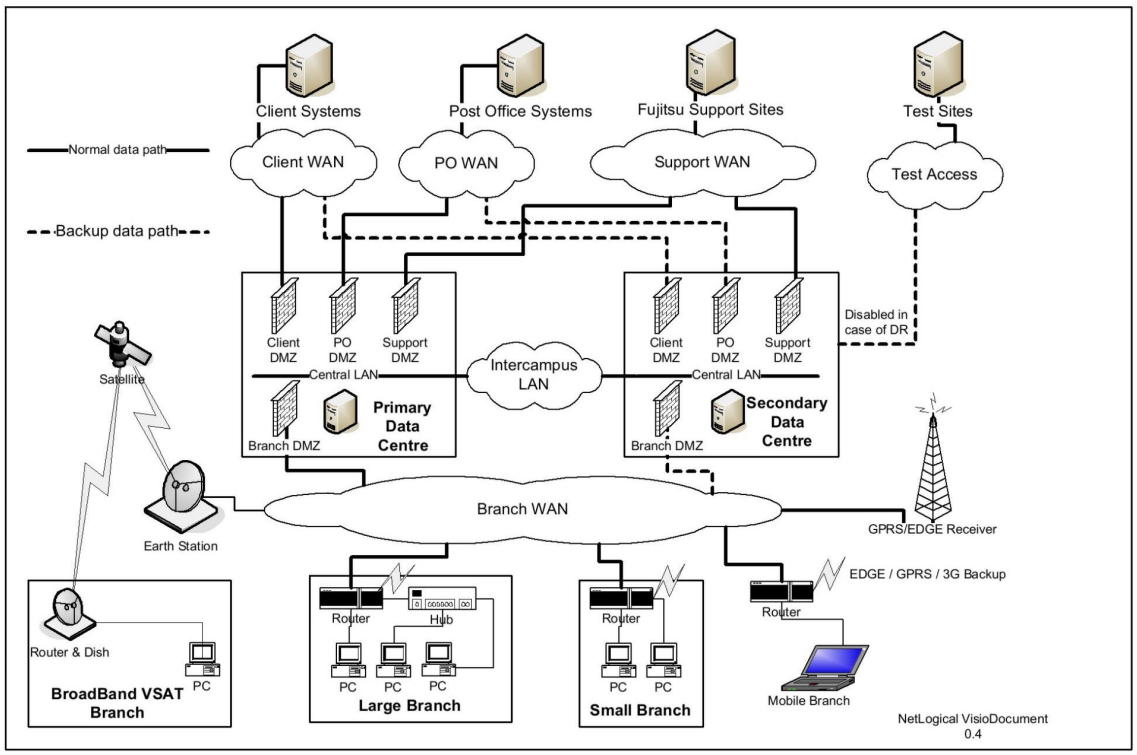
The Horizon IT system is built in line with key principles that all data is held centrally within the data centre with the exception of some standing data which is held locally within the branch. This centralisation principle applies to all 'completed' transactional data (known as "baskets") and to the Audit Store.

To support this principle the network architecture of Horizon is formulated on:

- Data centre;
- WAN Services (connecting datacentres, POL central sites, and Fujitsu sites); and
- Branch Network.

POL00222758

The diagram below provided by Fujitsu shows the high level IT system infrastructure:



The IT system is hosted on Bladeform technology with systems software being provided by:

- Windows 2003 Server (Enterprise and Standard, 32Bit and 64Bit);
- Red Hat Enterprise Linux (Release 4, 32Bit and 64Bit);
- Solaris 10 (Discrete platforms only); and
- Windows XP, Windows 2000 and Microsoft NT operating systems for some legacy services.

A number of internal and external interfaces are necessary for the reliable day-to-day processing of the IT systems, and hence the integrity of the Horizon Features which control these activities and interfaces; which is key to the effective operation of the overall system.

External interfaces include (not an exhaustive list):

- DVLA;
- Lottery; and
- Bank Payment Channels (Vocalink, e-pay, Streamline).

Internal Interfaces include (not an exhaustive list):

- Paystation;
- POL SAP
- Pay and Go; and
- ATMs

A number of batch processes also run in facilitating the successful processing by the system.

POL00222758

Managing the processing of the real-time and batch processing environment is Tivoli Workflow Scheduler (TWS) which is used to execute, monitor and handle exceptions within the processing environment. TWS is managed and monitored by Fujitsu as part of the managed service contract between the two parties.

In producing the diagram on page 9, we have considered the IT Provisioning risks in the context of the following assertion:

- Supporting IT management processes are well controlled.

System Usage Risk

Responsibility for the administration of the system rests with Fujitsu who provide change control, security management, system operations, and end-user support.

Responsibility for the effective usage of the system, including complaint and effective business processes, remains the responsibility of POL.

The user base of Horizon can be subdivided into two core areas:

- Central Users – including Finance, and users at the Network Business Support Centre.
- Branch Users – Sub-postmasters and their staff who are processing shop floor transactions.

Outside of the POL user base, Fujitsu provide administration services, and hold service and super user account privileges within the system.

Horizon supports the processing of a multitude of different transactions including:

- Purchases of goods;
- Purchases of services (for example Lottery tickets or tax discs);
- Payments to discharge customer debts (payment of mobile phone bills for example);
- Refunds; and
- Transaction corrections.

Several transaction mediums are accepted, for example:

- Cash;
- Credit and debit cards; and
- Cheques.

A number of controls are in place to support the integrity of transactional processing including:

- The Audit Store, a secure area of Horizon which pertains to store all transactional information in sequentially numbered records, along with key system events;
- Monitoring controls facilitated by Tivoli Workflow Scheduler and associated exception handling processes;
- Handshakes and call offs between systems include various controls around the integrity of transmitted data (such as digital signatures); and
- Backup communication routes between branches and the central data centre (mobile technology).

Reconciliations are performed regularly both in branch and centrally. Key reconciliation processes carried out include:

- Daily branch cash declaration and reconciliation to Horizon balances;
- Weekly balance of cash and stock and reconciliation to Horizon balances;
- Monthly trading period roll over (including resolution of any suspense account issues rolling over from weekly or daily reconciliations); and
- Central finance processes to reconcile central records to cash remitted to POL, cheques remitted to POL etc.

In response to discrepancies as a result of these reconciliation processes investigations may be conducted by the Finance Service Centre, and if required transactional corrections processed. These corrections are subject to significant investigation and are subject to approval by Sub-postmasters in the first instance.

POL00222758

Workarounds are not usually required, the main workaround being in relation to mobile connections from branch to data centre in the event that the main connection to the central data centre cannot be utilised.

In producing the diagram on page 9, we have considered the primary System Usage risks in the context of the questions posed within the scope of our work, and refined these risks into the following control assertions:

- Transactions from the Counter are recorded completely, accurately and on a timely basis centrally;
- Transactions processed to Branch Ledgers are recorded completely and accurately in the Audit Store;
- Directly posted "Balancing Transactions" are visible and approved;
- Information reported from the Audit Store retains its original integrity;
- Data posted from other systems and teams is visible to and accepted by sub post-masters; and
- Database Administrators (DBAs) or others granted DBA access do not modify data directly.

POL00222758

5 Assessment of Assurance Sources

IT Provision Risk Assurance Sources / Gap Analysis

For the IT Provision risks the existing assurance sources appear to provide a good level of coverage over the risk universe associated with this area of the Horizon processing environment.

Our high-level analysis of this coverage against the three core risk areas is as follows:

Area	Information Security	Information System Operations	Change Management
ISO27001 Statement of Applicability	Good coverage	Fair coverage	Fair Coverage
ISAE3402 Report	Good coverage	Good coverage	Good coverage
PCI DSS Report	Good coverage	Limited coverage	Fair coverage

Detailed analysis at an objective level is included within Appendix 1.

In considering this assessment, POL management should be cognisant of the inherent limitations of each report, given the purpose for which it was written:

Report	Limitations / Factors to Consider whilst Utilising
ISO27001 Statement of Applicability	This document has been produced by Fujitsu, limiting its value from an independence perspective. It should be noted however that it is supported by an independent assessment of ISO27001 compliance by Bureau Veritas, an accredited certification provider. The main focus of ISO27001 is on security, although it does also focus (to a lesser degree) on the other core IT Provision risk areas, Change Management and Information System Operations.
ISAE3402 Report	This document has been produced by an independent third party, Ernst and Young. It has good coverage of all three IT Provision risk areas, and is produced according to testing standards stipulated within the ISAE3402 standard. In relying on this report management has considered 'Section 6 Complimentary User Entity Controls' which stipulates the controls that POL should be operating in addition to the controls at Fujitsu in order to complete the control environment over Horizon.
PCI DSS Report	The scope of the PCI DSS report is the narrowest of the three assurance reports. It is focused exclusively on the security of cardholder data, and does not span the other two IT Provisioning risk areas to the degree of the other assurance sources. It provides minimal coverage in particular of the Information Systems Operations System Provisioning risk.

Of note when considering coverage of IT Provision assurance sources is that the majority of the focus is over Information Security, whereby based upon the historical issues and allegations being levelled at the system,

POL00222758

Information System Operations and Change Management would appear to be higher risk areas in the context of this particular piece of work.

Peer Comparison of IT Provision Assurance Available to Similar Organisations

Our comparison to peer organisations yielded the following results:

Organisation Sector	Sources of Assurance	Regulatory Focus
Print Media	External Audit Ad-hoc Risk Consultancy	N/A
Retail	External Audit Internal Audit	FCA (CCA)
Retail	External Audit Internal Audit PCI DSS	FCA (CCA) Loan Loss Provisioning Reporting
Retail and payments processing	External Audit Internal Audit	FCA
Government	External Audit Internal Audit PCI DSS Risk	Data Protection

This highlights that the level of IT Provision Assurance Work that POL has performed is comparable to that in other similar organisations which are not subject to risk and control regulatory requirements.

This should however also be interpreted in the context of the allegations being made against the Horizon processing environment which may suggest that a higher level of assurance is warranted compared to these similar organisational benchmarks.

POL00222758

Baseline Risk Assurance Sources / Gap Analysis

Our assessment of Baseline Risk was based upon three core scope areas:

- Horizon Project;
- Data Strategy Foundation Project; and
- Audit Store Changes.

For each of these scope areas we queried relevant POL and Fujitsu personnel in order to understand the project and change governance documentation available, and form an assessment as to the project controls applied to these change events, compared to Deloitte's Project Management methodology.

Our findings are as follows:

Baseline Risk Area	Assurance Work Information Provided
Audit Store	Changes to Horizon, such as the migration to HNG-X in 2010 involved minimal changes to the operation of the Audit Store. As a result these large scale projects are of minimal interest with regards to establishing a Baseline Risk position in relation to the design and functioning of Horizon Features relating to Audit Store. Some small changes have been made to the Audit Store in more recent years. Samples of documentation correlating to changes throughout the years the Audit Store had been in place were requested in order to understand whether these changes to the system had been managed to good practise standards. Further at the point of implementation of the Audit Store verbal representation was provided that a 'Security Report' was produced which pertained to demonstrate that the functionality of the system was as designed. This would be a key piece of Assurance Work, demonstrating the correct functionality of the Audit Store at that point in time, but it could not be located by POL and thus could not be reviewed as part of our work.
HNG-X Implementation (2010)	Detailed business and technical design documents have been verbally represented to have been created during the delivery of the project life cycle. Detailed test plans, MI, Defect Management and other key testing artefacts were produced during the course of the project. Several acceptance criteria related to the closure of testing defects. Examples of testing documentation have been provided to our review team during the course of our work. Migration checklists and instructions have been provided. These illustrate that site visits would be conducted during the migration to support the Sub-postmaster with the migration and support the resolution of any queries. We have been provided with verbal representation that detailed project acceptance criteria were agreed between Fujitsu and POL, and then signed off during the lifecycle of the project. An example of such acceptance criteria in relation to Non-Functional Requirements has been provided to us to support this verbal representation.
Data Strategy Foundation Project	Detailed business and technical design documents have been verbally represented to have been created during the delivery of the project life cycle. Assurance Work was provided to demonstrate business scoping and approval of changes to be applied (including a benefits realisation and costings map), requirements tracker document, testing strategy plan, testing report plan and migration summary documents. We were also provided with an example of the weekly reporting process at project close which demonstrated the level of governance and oversight the project had from senior stakeholders.

POL00222758

Summarising the work we have performed against Baseline risk we conclude that for each sampled change, Assurance Work has been produced in accordance with defined change management or project methodologies. We have not however been furnished with all key items of documentation we would have liked to review, due to the availability of such documentation to POL, and much of the Assurance Work provided to us were confirmations of verbal representations made during our work.

Further work will be required to perform a 'deep dive' review of project and change documentation on particular high risk areas (for example the original implementation of the audit store, and acceptance criteria sign off for the Branch Database commissioning as part of the Horizon HNG-X Implementation project), in order to provide assurance that the system baseline position were appropriately implemented and tested (timeframes of such positions varying depending on the component of the system under investigation).

Assessment of Assurance against System Usage Risk Areas

Our assessment in each of these areas is based upon information contained within system documentation from Fujitsu and operational policy and procedure documentation from the finance service centre, as well as emails confirming verbal assertions we received during the course of our work.

No testing or independent sources of assurance were identified over these System Usage risk areas.

Our understanding of the design of Horizon Features responding to key risks is a core output of our work and is outlined within Appendix 2 where we have provided a documentary listing of all of the Horizon features.

POL00222758

6 Matters for Consideration

In this section we set out our key matters for management consideration, further to the work we have performed above.

We have structured this section as follows:

- Key Matters for Consideration, by Risk Area reviewed;
- Factors to Consider in Formulating an Action Plan; and
- Proposed Action Plan.

Key Matters for Consideration

Risk Area	Key Matters for Consideration	Nature of Assurance Work
(1) General	a. ***Risk Appetite:*** During our work, only occasional linkage of work to the risk appetite of POL was noted. Whilst not unusual in the consumer business sector, such articulation and embedding of risk appetite assists with the delivery of better optimised and prioritised key controls and assurance activities. b. ***Holistic Risk and Assurance Framework:*** A holistic, risk intelligent assessment relating to the identification and mitigation of key risks to the integrity of processing should be considered in order to validate the completeness of the Horizon Features referred to in our work and thus provide a complete schedule of key controls that require assurance. Whilst Assurance Work has been provided demonstrating the use of key forums for tracking the risk environment surrounding Horizon (such as the Information Security Management Forum and Fujitsu Services Security Reports), these arent set up to specifically consider the holistic risk and assurance framework necessary to enable an overall comment on the design, implementation and operating effectiveness of the Horizon Features.	N/a
(2) System Baseline	a. ***Project Governance:*** Governance procedures described to us (verbally) suggest that the expected levels of business involvement in pre-go live system and user acceptance testing is performed as part of system implementation projects over the Horizon IT system; and that business users would be appropriately involved in signing off of system requirements and readiness to go-live (full system reconciliations). To supplement these verbal assurances, management has provided us with samples of documentation from the three sampled change areas (Horizon Implementation, Data Strategy Foundation, and Audit Store changes). Despite these sources of evidence, management should consider whether further investigations into sources of assurance from the original Horizon implementation would be worthwhile, given the importance of establishing a well-founded baseline position over the Horizon Features. b. ***Audit Store Baseline:*** The implementation of Horizon HNG-X in 2010-11 was asserted to not have had a significant impact on the Horizon Features. In particular no changes were made to the Audit Store as a result of the implementation. Therefore the 'baseline' position for the Audit Store was established as being at the original implementation of the Horizon IT system. Key documentation around the baseline positon for the Audit Store has not been able to be provided to us during the course of our work. We note that a security report was verbally represented to us to have been commissioned during the original implementation of the Audit Store, although this report could not be located and provided to us.	Verbal representations Limited documentation

POL00222758

Risk Area	Key Matters for Consideration	Nature of Assurance Work
(3) IT Provision	a. ***End User Entity Control Considerations:*** The ISAE3402 report requires interpretation in the context of these controls at POL. They are outlined in section 6 of the ISAE3402 report. Without such analysis, the assurance provided by the ISAE3402 is weakened. We are aware that POL has nearly completed work in order to address such considerations. b. ***Assurance Clarifications:*** In the context of detailed testing and assurance procedures, there are areas of the ISAE3402 report which would benefit from further clarification, in order to remove the risk of ambiguity from its interpretation, and overlaps with other sources of assurance that may be performed. For example: o the report does not state from where populations of data tested in samples were obtained and thus how exposed conclusions may be to internal fraud or deliberate override of control (e.g. for change management testing, were samples picked from the population in the secure Audit Store, or from another source?); o the report does not draw out certain key features in the control design, which we would assume are present, for example, control objective 4.8.11 (relating to access to the system being restricted to appropriate users) does not explicitly state and test that users must have and use their own unique username, thus underpinning audit trail integrity; and controls relating to the management of administator access could be more specific as to the extent and nature of the design of contrds and testing performed. o the report is not explicit in the sample sizes used for testing; and o the report contains tests which could be strengthened, for example, control test 6.5 in section 7 appears to test through discussion with personnel only, without clarifying if anything was done to corroborate such verbal assertions. c. ***Internal* Audit Work –** Internal audit work conducted highlights progress in responding to and closing down issues in relation to internal audit risks, but a number of issues remain outstanding. Internal audit have also not done anyspecific assurance work over the allegations being raised on the Horizon system andPOL's response to the issues raised.	Extensive documentation Independent testing
(4) System Usage	a. ***Risk Driven Considerations:*** The current documentation over System Usage Risks has been largely written in response to key incidents or events, by non-independent parties and from operational perspectives. Whilst detailed, itis also not written from a risk and assurance perspective and is rarely evidential in its content. b. ***Risk and Control Framework:*** There are areas where an understanding of the design and nature of operations relating to System Usage Risksis available, but the design, implementation and operating effectiveness of **key controls** has not been aggregated into a risk driven framework nor formally assured through evidence based testing. Further, the ability of documentation to fully support information relating to the detailed design of controls relating to System Usage Risks is unclear (e.g. whilst JSNs are sequential is there a systems operations control which checks the completeness of this sequence proactively?). The Schedule of Assurance over Horizon Features we have formulated as part of our work (and documented in Appendix 2) provides a basis forsuch a risk and control framework, as well as targeted testing over key controls. Management should consider enhancing their assurance provision by verifying the completeness of this schedule, and conducting implementation and operating effectiveness testing of the key controls there-in. c. ***Interfaces - DVLA:*** Whilst environmental risk relating to system operatons is largely assured in the ISAE3402, we note that no evidence of specific or detailed testing or assurance work has been carried out over System Usage Risks relating to the DVLA interface (both IT and business in nature). We note that many interfaces observed do not relate directly with the Horizon Features in scope for this review, but we recommend that such activities be considered for inclusion in theoverall risk and control framework relating to the Horizon processing environment. d. ***Audit Store:*** We observed the following: o It is not clear from the documentation we have been provided whether POL has agreed that the current capturing of certain, key system events, is complete and appropriate for potential governance and investigation needs; o We have not identified controls which formally report, review and consider the impact and resolution of any exceptions identified duringthe Audit Store extraction process, nor reconcile the data from other reporting systems inthe business to those data sets contained within the Audit Store ;	Partial Documentation

POL00222758

Risk Area	Key Matters for Consideration	Nature of Assurance Work
	○ Investigatory work on the Audit Store has all been performed by Fujitsu who, whilst technically qualified, do not constitute an independent or risk experienced party for assurance driven purposes. POL could consider doing more independent analysis of Audit Store historic data to verify that it is recorded in line with expected characteristics; and ○ From the documentation we have reviewed, controls to assess that the digital signature is valid and verify that there is a complete sequence of JSNs are retrospective. No proactive checks were documented which describe the performance of such verifications prior to the copying of data to the Audit Store. e. ***Proactive monitoring of key System Usage Risks:*** The current assurance environment appears to be "reactive" in nature, with exceptions in processing triggering diagnostic and remediation activity only when reported. It would appear that no use is being made of the Audit Store, for proactive monitoring of unusual or exceptional system events potentially worthy of further investigation and action. f. ***Hardware controls over the Audit Store:*** The Centera EMC devices used to host Audit Store data have not been configured in the most secure EC+ configuration. As a result system administrators on these boxes may be able to process changes to the data stored within the Audit Store, if other alternative software controls around digital seals, and key management are not adequately segregated from Centera box administration staff. Privileged access to the cryptographic solution around digital signatures, and publically available formulas on MD5 hashed digital seals would potentially allow privileged users at Fujitsu to delete a legitimate sealed file, and replacement with a 'fake' file in an undetectable manner. g. ***Branch Database:*** We observed the following in relation to the Branch Database being: ○ A method for posting 'Balancing Transactions' was observed from technical documentation which allows for posting of additional transactions centrally without the requirement for these transactions to be accepted by Sub-postmasters (as 'Transaction Acknowledgements' and 'Transaction Corrections' require). Whilst an audit trail is asserted to be in place over these functions, evidence of testing of these features is not available; ○ Processes around Transaction Acknowledgements and Transaction Corrections are subject to out of date documentation, or in the case of Transaction acknowledgements, no documentation at all. Such documentation should be produced or brought up to date; ○ For 'Balancing Transactions', 'Transaction Acknowledgments', and 'Transaction Corrections' we did not identify controls to routinely monitor all centrally initiated transactions to verify that they are all initiated and actioned through known and governed processes, or controls to reconcile and check data sources which underpin current period transactional reporting for Subpostmasters to the Audit Store record of such activity; ○ Security on the Branch Database around the 'Messaging Journal table' is a key area of risk due to branch transactional data being held on this table for up to a day before being written to the Audit Store. It was unclear from the documentation reviewed whether specific assurance work had been carried out in this area; and ○ Controls that would detect when a person with authorised privileged access used such access to send a 'fake' basket into the digital signing process could not be evidenced to exist.	

POL00222758

Recommendations

We have identified three areas where POL should consider further actions to strengthen the quality and nature of assurance in place over the Horizon system.

These are actions that may:

- Further support Project Sparrow;
- Integrate knowledge obtained from this work into the Future System Requirements project; and
- Help POL to move towards a more holistic Programme of Assurance.

We have aligned each of the actions we would recommend to POL management to one of these areas, and we present these below.

Actions that may further support Project Sparrow

A1 **Investigation of Balancing Transactions Use in 2010**	***Perform a detailed review of Balancing Transaction use:*** Instruct a suitably qualified party (independent of Fujitsu) to carry out a review of the circumstances leading up to the need to use the Balancing Transaction functionality in Horizon, including an assessment of the communications with the relevant Sub-Postmaster prior to any adjustment being made to their ledgers. This work should include a more detailed walkthrough of the current day "Balancing Transaction" policies, procedures and key controls, making recommendations for improvement
A2 **Verification Work that Horizon Features are Implemented as Described**	***Perform implementation testing of Horizon Features:*** Instruct a suitably qualified party (independent of Fujitsu) to carry out implementation testing of the Horizon Features (or a selection of key Horizon Features) identified in this report. The work should aim to provide POL with comfort that the Horizon Features extracted from documentation are actually designed and implemented exactly as described in that documentation.
A3 **Analytical Testing of Historic Transactions**	***Analytical Testing of Historic Transactions:*** Audit Store documentation asserts that the system contains seven years of Branch transactions, and a number of system event activities. In addition, a number of assertions relating to data integrity, record / field structure and key control features (such as sequencing of JSN) are made in documentation, but have never been validated by parties outside of Fujitsu. With modern day technologies, the analytic profiling and testing of such Big Data sets is likely to be feasible, thus POL should consider instructing a party independent of Fujitsu to perform independent risk analytics on an extract of all Audit Store data to verify that (a) key characteristics are seen in the data as expected and (b) what other matters / exceptions / insights can potentially be derived. This exercise would also provide valuable insight into those Horizon Features that could be automatically monitored as part of the optimised risk and control environment described below.
A4 **Documentation of all Horizon adjustment and reporting processes in the FSC**	***Update / Create documentation formalised all key adjustment and reporting processes in operation over Horizon in the FSC:*** Identify and document all key activities in the FSC relating to both adjustment processing to Sub-Postmaster ledgers and to the control activities that ensure that transactional data visible to Sub-Postmasters is fully reconciled to the Audit Store's 'high integrity' copy of Branch Ledger transactions. Use this exercise to verify the completeness and appropriateness of Horizon Features so far identified from verbal assertions, and then perform implementation testing (per A2 above) of such controls.

POL00222758

Actions that will integrate knowledge obtained from this work into the Future System Requirements project.

B1 **Produce baseline requirements for future replacement of the Horizon System**	***Produce Future System Requirements Document:*** Produce a schedule of key system requirements that any future Horizon replacement platform should deliver against, as an underpinning baseline for the integrity of processing. This schedule would outline key control objectives, with current day control activities /Horizon Features and /or other examples cited to show how such control objectives could be addressed in any future system. The schedule should include matters that will support the delivery of such design confidence in efficient ways, and providing foundations for preventative, detective and monitoring control activities. It could also highlight key questions for POL to consider, such as the longevity of data head in the Audit Store and the type of cryptographic mechanisms applied to the system.

Actions that may help POL move towards a more holistic programme of Assurance

This area is the more significant piece of work recommended in a broad context for POL to consider as a result of our assessment.

The development of such a holistic assurance programme should be seen as a 'strategic' response to the issues raised. If delivered successfully it will bring assurance benefits beyond the confines of assuring the integrity of processing within Horizon.

Whilst not raised specifically below, such an exercise would first require the appointment of a role in POL who would be responsible for the coordination of assurance across the whole organisation and the reporting of key areas where assurance provision could be improved (a "Head of Assurance"). This would ensure that POL Management and the Board have the ability to map, coordinate and assess assurance sources (and their quality) on an ongoing basis for the organisation.

C1 **Risk Workshop**	***Risk Workshop[1]:*** Conduct an exercise with key stakeholders in POL, including those in charge of Governance, to create a baseline understanding of risk and risk management concepts; share examples of how similar organisations manage, define and control key risks; and obtain suggestions and consensus as to if, where and how POL could become a more "Risk Intelligent" organisation and reporting of risk and assurance matters could be improved.
C2 **Construct Risk and Control Framework**	***Construct Risk and Control Framework:*** Extend and confirm the completeness of the Horizon Features which are designed to exert control over the Horizon processing environment. The framework can be used to prioritise key areas for improvement (including clarifications / the removal of ambiguity in existing sources) and embed agreed changes in current assurance sources. A key component for the construction of this risk and control framework is the initial information produced as part of our analysis and reproduced in Appendix 2. This Framework could be extended to cover POL's overall risk and control framework, not just those areas relevant to Horizon processing.
C3 **Test Controls**	***Test Controls:*** Once the framework is verified as complete, key controls can be identified and evidence based testing performed to validate that they are operating effectively. Such operating effectiveness work could be performed on a sustained basis and could be delivered by an independent party in line with a recognised assurance standard. In addition, this exercise can be used to feedback on the design of the control environment so that it can be optimised (i.e. maximise coverage of key risks, with minimal duplication).
C4 **Optimise ongoing testing**	***Sustain Assurance Delivery and Implement More Proactive Monitoring[2]:*** The longer term assurance map can be designed to sustain assurance delivery for POL over key risks. This may include a transition to a more proactively monitored control environment ("continuous controls monitoring"), where automated alerts are generated if certain key behaviours in the system are identified.

POL00222758

Notes:

[1]**Risk Workshop:** Risk appetite statements may be considered as part of this exercise, but are typically found by key stakeholders to be a different area to understand. Such statements are effectively matters which help an organisation to avoid imprecise or open statements relating to risk, which do not assist with the effective management of responses to such risks. Statements are mechanisms that also help management to define parameters relating to risk, against which key decisions and escalation activities can be performed.

'Key risk indicators' are often a tool used by management, and those in charge of Governance, in these areas. Whilst POL needs to consider their own risk statements and indicators, some examples of those that may be worthy of consideration in relation to the integrity of processing in Horizon could include:

- The number of allegations or concerns raised by Sub-postmasters during a defined period;
- The number and value of adjustment postings being performed by FSC
- The use of balancing transactions
- The number of security incidents on the Horizon system during a defined period;
- The value of unreconciled differences between systems / ledgers
- The number and nature of errors or exceptions in processing; and
- Key controls found to not to be operating effectively in a period.

The above are not exhaustive and key risk indicators need to be considered thoroughly in response to the particular risks and controls which are required in response to the risk universes formulated over the Horizon processing environment.

[2]**Sustain Assurance Delivery and Implement more Proactive Monitoring:** Benefits of these activities could include:

- Minimising duplication in the control framework, and the assurance activities there-on;
- Support targeted assurance provision in the context of existing or potential future allegations;
- Provide more measureable benchmarks of performance against other organisations;
- Underpin further efficiencies in the assurance provision, for example the automation of existing manual controls;
- Incentivise ongoing improvement in both the processes and the assurance provision, by highlighting deficiencies on a timely basis and reporting these directly back to those business or outsourced owners who need to take a remediation or corrective action; and
- Support the maintenance of the completeness of documentation over the Horizon Features.

POL00222758

Appendix 1: IT Provision Assurance Source Mapping and Gap Analysis

The mapping below outlines the more detailed IT Provision assurance mapping against IT Provision risks, as summarised in Section 4:

Area	Environmental Risk	ISO27001 Statement of Applicability	Coverage Rating	ISAE3402 Section	Coverage Rating	PCIDSS	Coverage Rating
Change Management	Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data.	A.10 Communications and Operations Management A.12 Information Systems Acquisition, Development and Maintenance		4.8.10 Change Management		Requirement 6: Develop and maintain secure systems and applications.	
Change Management	Inappropriate changes are made to system software (e.g., operating system, network, change-management software, access-control software).	A.10 Communications and Operations Management A.12 Information Systems Acquisition, Development and Maintenance		4.8.10 Change Management		Requirement 6: Develop and maintain secure systems and applications.	
Change Management	Inappropriate changes are made to the database structure and relationships between the data.	A.10 Communications and Operations Management A.12 Information Systems Acquisition, Development and Maintenance		4.8.10 Change Management		Requirement 6: Develop and maintain secure systems and applications.	
Operations	Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	A.10 Communications and Operations Management A.14 Business Continuity Management		4.8.2 Backup 4.8.5 Incident Management 4.8.6 Major Incident Process 4.8.7 Security Incident Process		Information System Operations not within scope for PCIDSS review.	

POL00222758

Area	Environmental Risk	ISO27001 Statement of Applicability	Coverage Rating	ISAE3402 Section	Coverage Rating	PCIDSS	Coverage Rating
Operations	Production systems, programs, and/or jobs result in inaccurate, incomplete, or unauthorized processing of data.	A.10 Communications and Operations Management		4.8.3 Job Scheduling 4.8.4 Availability and Capacity Management 4.8.5 Incident Management 4.8.6 Major Incident Process 4.8.7 Security Incident Process		Information System Operations not within scope for PCIDSS review.	
Security	Inappropriate changes are made directly to financial data through means other than application transactions.	A.11 Access Control		4.8.12 Access to databases, data files, and programs		Requirement 3: Protect stored cardholder data. Requirement 6: Develop and maintain secure systems and applications.	
Security	Inappropriate changes are made to Application systems or programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) and/or report logic.	A.10 Communications and Operations Management A.12 Information Systems Acquisition, Development and Maintenance		4.8.10 Change Management		Requirement 6: Develop and maintain secure systems and applications.	
Security	Individuals gain inappropriate access to equipment in the data centre and exploit such access to circumvent logical access controls and gain inappropriate access to systems.	A.8 Human Resources Security A.9 Physical & Environmental Security		4.8.1 Physical and Environmental Controls		Requirement 9: Restrict physical access to cardholder data.	
Security	Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.	A.11 Access Control		4.8.10 Change Management		Requirement 6: Develop and maintain secure systems and applications.	
Security	The network does not adequately prevent unauthorized users from gaining inappropriate access to information systems.	A.11 Access Control		4.8.9 Networks 4.8.10 Change Management 4.8.11 Security		Requirement 6: Develop and maintain secure systems and applications. Requirement 11: Regularly test security systems and processes.	

POL00222758

Area	Environmental Risk	ISO27001 Statement of Applicability	Coverage Rating	ISAE3402 Section	Coverage Rating	PCIDSS	Coverage Rating
Security	Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	A.8 Human Resources Security A.11 Access Control		4.8.11 Security 4.8.12 Access to databases, data files, and programs		Requirement 7: Restrict access to cardholder data by business need-to-know. Requirement 12: Maintain a policy that addresses information security for employees and contractors.	

POL00222758

Appendix 2: Assurance Schedule over Horizon Features

We present below a schedule of the Assurance Work and sources we have identified which relate to certain groups of Horizon Features.

We have structured these in line with our three areas of assessment (System Baseline, IT Provision and System Usage), as defined in our report.

We have also recorded our assessment of the level of comfort that POL has over that Horizon Feature, defined as:

- **"Significant"** means we have seen Assurance Work that delivers comfort through evidence based testing by independent parties.
- **"Partial"** means we have seen Assurance Work in the form of descriptions in formal documentation, but no testing of implementation or operating effectiveness.
- **"Limited"** means we have seen Assurance Work that documents verbal assertions we received during our work.
- **"None"** means that Assurance Work has not yet been provided to us.

POL00222758

System Baseline

Area	Key Assertion re. Processing Integrity	Description of feature	Assurance Work Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Baseline	The system was fit for purpose and worked as intended when first put in?	The design of key elements of the Horizon system relevant to the integrity of auditing and capturing transactions was formally agreed and signed off prior to systems deployment.	No information provided.	Preventative	Manual	None
Baseline	The system was fit for purpose and worked as intended when first put in?	Traceability Matrices have been documented, implemented and periodically reviewed to ensure that business requirement documents have been regularly reviewed against project progress.	No information provided.	Preventative	Manual	None
Baseline	The system was fit for purpose and worked as intended when first put in?	During the initial implementation of the software, Key Project Governance mechanisms were put in place to ensure the: Working Group Steering Group/Project board Requirements Review Group	No information provided.	Preventative	Manual	None
Baseline	Major changes since implementation have not impacted the system.	Traceability Matrices have been documented, implemented and periodically reviewed to ensure that business requirement documents have been regularly reviewed against project progress.	No information provided.	Preventative	Manual	None

POL00222758

Area	Key Assertion re. Processing Integrity	Description of feature	Assurance Work Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Baseline	Major changes since implementation have not impacted the system.	Key Project Governance mechanisms have been enacted and operated over significant changes to the system since implementation. Examples of such mechanisms include: - Working Group - Steering Group/Project board - Requirements Review Group	No information provided.	Preventative	Manual	None
Baseline	The system was fit for purpose and worked as intended when first put in.	Prior to implementation into the live environment (and in some cases post) acceptance criteria in relation to key system elements important for auditing and capturing transactions were formally agreed and signed off.	For Audit Store Baseline: Example acceptance criteria document entitled Acceptance Report 20070917BL01.13WIP (note no sign off of acceptance criteria is included within this document). For 2011 Horizon Implementation (BRDB Baseline): Testing plans were provided in the document 'Copy of IT Health Check 23-07-2009.xls', a Risk Assessment of the project has been provided in 'Security All Risk Extract 090928 v2.xls' and Migration instructions have also been provided in the document 'Migration_ Instructions.pdf'. Also a report by third party consultancy firm Wipro has	Preventative	Manual	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description of feature	Assurance Work Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
			been provided to demonstrate the project was delivered as planned in the document 'Horizon : Performance Test Audit Post Office Limited (POL)'. For 2012 Data Strategy Foundation (External Feeds Baseline): - Example acceptance criteria document entitled CFD New Requirements v1.11.xls (note no sign off of acceptance criteria is included within this document). Additionally, an example of a designed, and reviewed Migration Strategy, titled 'Migration Strategy CFD v0.4', was provided, in addition to a Test Report, 'POLTSTREP0010 - CFD E2E Test Report v0 1'.			
Baseline	The system was fit for purpose and worked as intended when first put in?	The testing of key elements of the system important for the auditing and capturing of transactions was formally agreed and signed off and then delivered against.	For 2011 HNG-X Implementation: For 2012 Data Strategy Foundation: - Test Strategy Document entitled 'Acceptance Testing Strategy' - authorised version	Preventative	Manual	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description of feature	Assurance Work Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
			dated 10/11/2011. - Test Exit Report entitled 'Client File Delivery Report E2E - Exit Test Report', draft version 0.1 dated 06/01/2012.			
Baseline	Major changes since implementation have not impacted the system.	Sign off for design of significant change is formalised and documented.	2005 Design Proposal ASDPR027.doc 2005 Audit Centera API Implementation DELLD026.doc 2002 Change Proposal CP3240.rtf 2004 Change Proposal CP4021.rtf	Preventative	Manual	Partial
Baseline	Major changes since implementation have not impacted the system.	Acceptance criteria related to key areas such as the branch database and audit store.	2002 Acceptance Test Specification IAACS002.doc	Preventative	Manual	Partial
Baseline	Major changes since implementation have not impacted the system.	Test Strategy and Execution have been documented and signed off, and provide an adequate audit trail for the testing of key system features such as the Audit Store and Branch Database.	2003 Acceptance Test Report IAACR003.doc	Preventative	Manual	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description of feature	Assurance Work Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Baseline	Major changes since implementation have not impacted the system.	Independent Assurance over design of HNG-X system by Gartner.	No information provided.	Preventative	Manual	Low
Baseline	Major changes since implementation have not impacted the system.	Programmes and projects affecting the Horizon system are controlled and governed using an established change methodology.	Harmony Delivery Lifecycle document	Preventative	Manual	Partial
Baseline	Major changes since implementation have not impacted the system.	Independent Assurance report over testing procedures has been obtained.	Wipro performance testing report.	Preventative	Manual	Significant

POL00222758

IT Provision Assurance

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Provision	IT supporting processes are well controlled.	Management have established forums to oversee the performance of third party IT providers.	ISMF Minutes FJS Security Report	Preventative	Manual	Partial
Provision	IT supporting processes are well controlled.	POL has documented end user control considerations to supplement third party service provider controls assurance reports	POL End User Considerations Document	Preventative	Manual	Partial
Provision	IT supporting processes are well controlled.	Third party assurance reports are in place to ensure the overall control of the IT environment, including: ISAE 3402 reports, PCIDSS compliance report and ISO27001 certified accreditation.	ISAE3402 Report PCIDSS Report	Preventative	Manual	Significant

POL00222758

Usage Assurance

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	Only baskets that balance to £0 can be accepted by the central database (double entry concept exists).	Horizon Online Data Integrity_POL document.	Preventative	Automated	Partial
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	Digital Signature is applied to each transaction basket at the point of counter inception to prevent downstream tampering.	Horizon Online Data Integrity_POL document.	Preventative	Automated	Partial
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	Transactional Acknowledgement and manual review process.	Verbal confirmation from Rod Ismay and Jane Smith in Finance Shared Services.	Detective	Automated	Partial
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	Sequential numbering is applied to each counter basket prior to digital signature application to provide a 'baked in' sequence check.	Horizon Online Data Integrity_ POL document.	Preventative	Automated	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	Oracle commit and roll-back process is atomic (i.e. either a complete transaction is posted or nothing is posted).	Horizon Online Data Integrity_ POL document.	Preventative	Automated	Partial
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	A fall back mobile link is in place to ensure that if transactions are still processed in a timely manner	Horizon Online Data Integrity_ POL document.	Preventative	Automated	Partial
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally.	A private cryptographic key is securely established for each transmitted basket.	Horizon Online Data Integrity_ POL document.	Preventative	Automated	Partial
Usage	Directly posted transactions, such as "Balancing Transactions", are visible and approved.	Formalised change control approval and monitoring process over the usage of Balancing Transactions	Email communication from John Simpkins dated 15/05/2014, articulating control design around this process.	Preventative	Manual	Partial
Usage	Directly posted transactions, such as "Balancing Transactions", are visible and approved.	An audit trail log is in place to monitor the use of balance transactions. The log is monitored by an independent department that does not have access to the function.	Email communication from John Simpkins dated 15/05/2014, articulating control design around this process.	Detective	Manual	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Branch Ledger transactions are recorded accurately in the Audit Store.	JSNs are processed into the audit store and reviewed when users access audit store information. The Audit Store will automatically detect non-sequential files that are then processed by the Tivoli monitoring tool and investigated where appropriate.	Technical Design Document for Audit Extract Process - DESAPPHLD0029.	Preventative	IT Dependent Manual	Partial
Usage	Branch Ledger transactions are recorded accurately in the Audit Store.	Digital seals are in place to ensure that files are not amended following load to the Audit Store	Technical Design Document for Audit Extract Process - DESAPPHLD0029	Preventative	Automated	Partial
Usage	Branch Ledger transactions are recorded accurately in the Audit Store.	The digital seal applied to the batched digital signatures ensures that any amendments to data leaves a traceable audit trail	Security Architecture Document Network Architecture Document Cryptography Architecture Document	Preventative	Automated	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Branch Ledger transactions are recorded accurately in the Audit Store.	JSNs are processed into the audit store and reviewed when users access audit store information. The Audit Store will automatically detect non-sequential files that are then processed by the Tivoli monitoring tool and investigated where appropriate.	BRDB Technical Design Document Audit Technical Design Document		Automated	Partial
Usage	Branch Ledger transactions are recorded accurately in the Audit Store.	Formalised change control approval and monitoring process over the usage of Balancing Transactions	Email communication from John Simpkins dated 15/05/2014, and articulating control design around this process.	Preventative	Manual	Partial
Usage	Branch Ledger transactions are recorded accurately in the Audit Store.	Audit trail monitoring the usage of balance transactions	Email communication from John Simpkins dated 15/05/2014	Preventative	Manual	Partial
Usage	Information from the Audit Store retains original integrity.	Logical access controls in place over user management to ensure that only appropriate staff have access to extract information from the audit store	Audit Store Procedures	Preventative	Automated	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Information from the Audit Store retains original integrity.	Hardware controls are in place to prevent the modification of data in the Audit Store	Audit Store Procedures	Preventative	Automated	Partial
Usage	Information from the Audit Store retains original integrity.	JSNs are processed into the audit store and reviewed when users access audit store information. Audit store will automatically detect non-sequential files that are then processed by the Tivoli monitoring tool and investigated where appropriate.	Audit Store Procedures	Detective	Automated	Partial
Usage	Information from the Audit Store retains original integrity.	The digital seal applied to the batch on data transfer is checked back to the initial seal to ensure that hash value has not been altered.	Audit Store Procedures	Detective	Automated	Partial
Usage	Information from the Audit Store retains original integrity.	The integrity of the digital signature is checked for all baskets used in the extracts.	Audit Store Procedures	Detective	Automated	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Information from the Audit Store retains original integrity.	Exceptions identified in integrity checks on digital seals or signatures or in the sequence check are formally raised and handled as part of day-to-day IT operational processes within the Tivoli Monitoring tool.	Audit Store Procedures	Detective	Automated	Partial
Usage	The system used by the Finance teams for control contains all records	3 way match between Branch Database, Transaction file and POLSAP load file	Data Flow Diagram provided by Finance (Jane Smith)		IT Dependent Manual	Partial
Usage	Data posted from other systems and teams is visible to and accepted by sub post-masters	Amendments posted centrally via transactional corrections must be approved by sub-Post Masters must be approved before they can be applied to the Branch Database	Transactional Corrections Procedural Evidence	Preventative	Automated	Partial
Usage	Data posted from other systems and teams is visible to and accepted by sub post-masters	Amendments posted centrally via transactional acknowledgements must be approved by sub-Post Masters must be approved before they can be applied to the Branch Database	Branch Database Procedures	Preventative	Automated	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Data posted from other systems and teams is visible to and accepted by sub post-masters	For any outstanding (non-accepted) Transaction Acknowledgement or Transaction Corrections 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.	Rod Ismay	Preventative	Manual	Partial
Usage	Data posted from other systems and teams is visible to and accepted by sub post-masters	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 reconciliation, and their monthly trading period roll over activities.	Branch Database Procedures	Preventative	IT Dependent Manual	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Data posted from other systems and teams is visible to and accepted by sub post-masters	All processes create an identifiable transaction in Horizon, with an audit trail to the originator in the Finance Services team. This transaction ID is protected by the JSN, digital signature and digital seal features.	Branch Database Procedures	Preventative	IT Dependent Manual	Partial
Usage	DBAs or others granted DBA access have not modified Branch Database data.	Sub post-master must functionally approve the Transactional Acknowledgement file produced by the POLSAP system before items can be processed through to the branch database.	Branch Database Procedures	Preventative	IT Dependent Manual	Partial
Usage	DBAs or others granted DBA access have not modified Branch Database data.	Formalised change control approval and monitoring process over the usage of Balancing Transactions	Email communication from John Simpkins dated 15/05/2014, and articulating control design around this process.,	Preventative	Manual	Partial
Usage	DBAs or others granted DBA access have not modified Branch Database data.	Audit trail monitoring the usage of balance transactions	Email communication from John Simpkins dated 15/05/2014	Preventative	Manual	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	DBAs or others granted DBA access have not modified Branch Database data.	Hardware controls are in place to prevent the modification of data in the audit store	Audit Store Procedures	Preventative	Automated	Partial
Usage	DBAs or others granted DBA access have not modified Branch Database data.	Database access privileges that would enable a person to delete a digitally signed basket are restricted to authorised administrators at Fujitsu.	ISAE3402	Preventative	Automated	Partial
Usage	DBAs or others granted DBA access have not modified Branch Database data.	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.	ISAE3402	Preventative	Automated	Partial
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally?	TWS scheduler and monitoring processes are defined and formalised. Any issues or errors are reported and responded to by Fujitsu as part of day-to-day IT Operational activities.	ISAE3402	Detective	Automated	Significant

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Counter transactions are recorded completely, accurately and on a timely basis centrally	Logical security access controls in place to minimise the risk of inappropriate access to the counter software within branch.	Security Architecture Document reference - ARCSECARC0003 section 6.2 and ISAE3402, PCIDSS and ISO27001 reports as well.	Preventative	Automated	Significant
Usage	Branch Ledger transactions are recorded accurately in the Audit Store	Logical security access controls are in place in relation to the Branch Database and audit store to ensure that only appropriate staff members have access. Key transactions and tables are monitored and activity is verified by an independent third party.	ISAE3402 report.	Preventative	Automated	Significant
Usage	Branch Ledger transactions are recorded accurately in the Audit Store	Database access privileges that would enable a person to delete Audit Store data are restricted to authorised administrators at Fujitsu.	ISAE3402	Preventative	Automated	Partial

POL00222758

Area	Key Assertion re. Processing Integrity	Description	Source	Control Type (Preventative / Detective / Monitoring)	Control Method (Manual / Automated / IT Dependent Manual)	Level of Comfort
Usage	Branch Ledger transactions are recorded accurately in the Audit Store	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.	ISAE3402	Preventative	Automated	Partial

POL00222758

Appendix 3: Inventory of Documentation Reviewed

The following documentation was reviewed during the course of our review:

Document Number	Document	Document Type
1	Horizon Core Audit Process (Powerpoint)	Other sources of comfort
2	Fact file (updated with SS comments)	Other sources of comfort
3	ISAE3402 Report over Fujitsu managed service on Horizon	Assurance
4	Centrally Generated Transactions document	Other sources of comfort
5	POL Summary of Horizon Anomalies Referred to in Second Sight Report	Assurance
6	Report on Local Suspense (14 Branch) Issue	Other sources of comfort
7	Report on Receipts Payments (62 Branch) Issue	Other sources of comfort
8	Spot Review Bible	Other sources of comfort
9	Horizon Data Integrity Document	Other sources of comfort
10	Horizon Data Integrity Document	Other sources of comfort
11	Fujitsu ISO27001 Certificate	Assurance
12	ISO27001 Statement of Applicability produced by Fujitsu	Assurance
13	PCI DSS Attestation of Compliance	Assurance
14	PCI DSS Report by Bureau Veritas	Assurance
15	ISMF Minutes for three months	Other sources of comfort
16	Fujitsu Security Reports for three months	Other sources of comfort
17	Fujitsu Information Security Management System (ISMS) Scope	Other sources of comfort
18	Horizon Solution Architecture Outline	Other sources of comfort
19	Post Office to Driving & Vehicle Licensing Agency Automated Payments Client File Interface document	Other sources of comfort
20	DVLA Internal Web Service High Level Design document	Other sources of comfort
21	Security All Risk Extract	Other sources of comfort
22	Migration Overview Document for Horizon system	Other sources of comfort
23	Horizon Technical Security Architecture	Other sources of comfort

POL00222758

Document Number	Document	Document Type
24	Solution Architecture Document	Other sources of comfort
25	Batch Processing Overview Document	Other sources of comfort
26	EMC Centera Acceptance Test Report - IAACR003	Other sources of comfort
27	Centera Accepting Testing Specification - IAACS002	Other sources of comfort
28	Application Interface Design - DELLD026	Other sources of comfort
29	Audit Server Specification Design -TDDES071	Other sources of comfort
30	Configuration Design - TDMAN006	Other sources of comfort
31	Configuration Design - TDMAN009	Other sources of comfort
32	Centera star OS upgrade to version 2.4 design proposal	Other sources of comfort
33	Centera star OS upgrade to version 2.4 design proposal Amendment -CP4021	Other sources of comfort
34	Centera star OS upgrade to version 2.4 design proposal Amendment -CP3241	Other sources of comfort
35	Exception and Event Guide - TDMAN007	Other sources of comfort
36	Functional Separation - CRFSP006	Other sources of comfort
37	High Level Design - SDHLD001	Other sources of comfort
38	Audit Data Retrieval - SDHLD002	Other sources of comfort
39	Centera Migration HLD - TDION039	Other sources of comfort
40	Centera - High Level Test Plans - VIHTP014	Other sources of comfort
41	Horizon System Audit Manual - IAMAN005	Other sources of comfort
42	Low Level Design Document	Other sources of comfort
43	Centera Operational Procedures - TDMAN008	Other sources of comfort
44	Centera - Performance Test Specification - TDLLT008	Other sources of comfort
45	Centera Support Guide - TDMAN017	Other sources of comfort
46	Centera Support Guide - TDMAN018	Other sources of comfort
47	Centera Test Report - VITRP029	Other sources of comfort
48	Centera User Guide - TDMAN005	Other sources of comfort
49	Data Strategy Foundation - 04 - G149 Data Strategy Foundation - Client File Transfer - PODG Closure v2 0	Other sources of comfort
50	Data Strategy Foundation - CFD New Requirements v1.11	Other sources of comfort
51	Data Strategy Foundation - Data Strategy Foundation Test Strategy V1 0	Other sources of comfort
52	Data Strategy Foundation - Migration Strategy CFD v0.4	Other sources of comfort
53	Data Strategy Foundation - POLTSTREP0010 - CFD E2E Test Report v0 1	Other sources of comfort

POL00222758

Document Number	Document	Document Type
54	Data Strategy Foundation - Revised business case CFD 24 11 10	Other sources of comfort
55	Horizon Technical Network Architecture - ARCNETARC0001	Other sources of comfort
56	Horizon Crypto Services High Level Design -DESSECHLD0002	Other sources of comfort
57	E2E data flows	Other sources of comfort
58	idocs involving settlement	Other sources of comfort
59	Process Management Systems Diagram (Version 14 - 24.10.2011)	Other sources of comfort
60	AR11.005 - Horizon controls	Other sources of comfort
61	AR12.050 - Horizon follow up	Other sources of comfort
62	AR12.050a -Follow-up Horizon May2013	Other sources of comfort
63	Horizon Counter Application High Level Design - DESAPPHLD0047	Other sources of comfort
64	COMPONENT TEST PLAN FOR Horizon COUNTER INFRASTRUCTURE: SERVICE AND PROCESS CONTROL	Other sources of comfort
65	Horizon Operational and Support Services Requirements	Other sources of comfort
66	ACCEPTANCE REPORT FOR DESIGN WALKTHROUGH EVENT DW03 - SECURITY	Other sources of comfort
67	Draft Deloitte Phase 2 Instructions (RDW 07 05 14)2	Other sources of comfort
68	Phase 2 - Areas of Focus diagram (DRAFT v1)	Other sources of comfort
69	Project Zebra - Phase 2 Potential Next Steps v3	Other sources of comfort
70	REQAPPAIS1392v3.2.PayStation.ETL	Other sources of comfort
71	REQAPPAIS1391v2.1.PoGo.ETL.	Other sources of comfort
72	Acceptance Report 20070917BL01.13WIP	Other sources of comfort
73	All Streams Plan vsn 0.98	Other sources of comfort
74	BC PLA 001 v 0.3	Other sources of comfort
75	BC020 HNG PD Potential Risks and Issues Register v1.0	Other sources of comfort
76	Change Management Assessment Template	Other sources of comfort
77	DES SEC HLD 0010 v 1.0	Other sources of comfort
78	Engagement Meeting Log Notes v1.2	Other sources of comfort
79	Gartner Report Findings 1.1 with Appendix	Assurance
80	HARMONY Full Guide 1.1a	Other sources of comfort
81	HARMONY Full Guide 1.1a	Other sources of comfort
82	HNG Benefits Tracking in confidence May 08 final	Other sources of comfort
83	HNG Board Report 080408	Other sources of comfort

POL00222758

Document Number	Document	Document Type
84	HNG PID v1.3	Other sources of comfort
85	HNG Reqts Team Meeting 050606	Other sources of comfort
86	HNG Risk and Issues 070424LY	Other sources of comfort
87	Horizon Testing Strategy - HXTSR001	Other sources of comfort
88	In Touch report for HNG 080418a	Other sources of comfort
89	In Touch Report for HNG 081205	Other sources of comfort
90	POL HNG IMP 002 v 1.0	Other sources of comfort
91	POL HNG REQ 014	Other sources of comfort
92	QRH031 HNG Reqts PID v0.1f	Other sources of comfort
93	ACCEPTANCE REPORT FOR Horizon ACCEPTANCE GATEWAY 1 & 2 - REQ GEN ACS 0001 v0.2	Other sources of comfort
94	Horizon GENERIC ACCEPTANCE PROCESS -REQGENPRO0735	Other sources of comfort
95	Stakeholder Engagement Log_091218	Other sources of comfort
96	Test Report for the Integrity Testing of Horizon Data-centre Disaster Recovery – Week Commencing 1st September 2008 - SVMSDMREP0005	Other sources of comfort
97	Wipro - Horizon : Performance Test Audit Post Office Limited (POL)	Assurance
98	DVLA Internal Web Service High Level Design - DESAPPHLD0012	Other sources of comfort
99	Audit Data Retrieval High Level Design - DESAPPHLD0029	Other sources of comfort
100	Audit Data Collection & Storage High Level Design - DESAPPHLD0030	Other sources of comfort
101	Horizon Counter Application High Level Design - DESAPPHLD0047	Other sources of comfort
102	COMPONENT TEST PLAN FOR Horizon COUNTER INFRASTRUCTURE: SERVICE AND PROCESS CONTROL -DEV CNT CTP 0068 v 2.1	Other sources of comfort
103	DVLA AP Client File AIS	Other sources of comfort
104	Product Branch Accounting - Issuing Process for Transaction corrections v0.1	Other sources of comfort
105	Audit Data Collection and Storage High Level Design	Other sources of comfort
106	Data Flow - Transaction Processing for client file delivery	Other sources of comfort
107	Data Flow - NBSC Miskey Process - Network Banking	Other sources of comfort

POL00222758

With the prior permission of POL, the following individuals were interviewed or consulted during the course of our review:

Contact Name	Job Title / Role	Organisation
Dave King	Senior Technical Security Assurance Manager	POL
Julie George	Head of Information Security and Assurance Group	POL
Rod Williams	Litigation Lawyer	POL
James Davidson	Fujitsu Primary Point of Contact	Fujitsu
Pete Newsome	Quality responsibility	Fujitsu
Will Russell	Regional Network Manager NT - South	POL
Phil Norton	Horizon Requirements responsibility	Atos
James Brett	Senior Test Manager – Post Office Account	Atos
Bill Membery	Requirements/Testing responsibility on Horizon	Fujitsu
Gareth Jenkins	Distinguished Engineer	Fujitsu
Neil Crowther	Senior Business Analyst	POL
Matthew Lenton	Document Management responsibility	Fujitsu
Rod Ismay	Head of Finance Service Centre	POL
Jane Smith	AP Enquiry Team Leader, Finance Service Centre	POL
Dave King	Senior Technical Security Assurance Manager	POL

POL00222758

Appendix 4: Engagement Letter

Deloitte.

Deloitte LLP
P.O. Box 500
2 Hardman Street
Manchester M60 2AT
Tel: GRO
Fax:
www.deloitte.co.uk

Mr Chris Aujard
Post Office Ltd
148 Old Street
London
EC1V 9HQ

9th April 2014

Dear Sirs

STRICTLY PRIVATE AND CONFIDENTIAL
PRIVILEGED IN CONTEMPLATION OF LITIGATION

We are pleased to set out for your approval the arrangements under which we propose to assist Post Office Ltd ("POL" or "You"). We understand that You are responding to allegations that the "Horizon HNG-X" IT system, used to record transactions in Post Office branches, is defective and/or that the processes associated with it are inadequate (the "Allegations").

In order to respond better to the Allegations, You require services from us, as outlined in paragraph 2(b) below. These arrangements are set out in this letter together with the enclosed Terms of Business and appendices.

So that we are able to assist You effectively, please ensure that You have considered fully all of the terms and conditions set out in this letter and its enclosures and that You are satisfied that the scope of our Services described below is sufficient for Your needs.

1 Scope and objectives

In order to respond better to the Allegations (which have been, and will in all likelihood continue to be, advanced in the courts), You want to demonstrate that the Horizon HNG-X system is robust and operates with integrity, within an appropriate control framework. In response to this, You have either been provided with or commissioned a number of independent assurance reviews into matters relating to Horizon HNG-X's operating environment and processing integrity.

The purpose of seeking input from Deloitte LLP (UK) ("Deloitte") is to provide, based upon the information made available to us by You, an independently produced summary of the assurance and other work undertaken, over your current day Horizon HNG-X system, for presentation to and discussion with the POL Board ("Part 1 work").

We understand that the input provided by Deloitte will inform Your decisions relating to potential areas of additional work that You may choose to commission to respond better to the Allegations, and that we may be involved in the delivery of such additional work ("Part 2 work") under either a Change Order or separate Engagement.

You have asked us to provide the Services set out in Section 2 below and to prepare the report described in Section 2(d). (the "**Purpose**").

official professional services provider to the Olympic and Paralympic Games

Deloitte.

We understand that any work being undertaken by us in accordance with this engagement letter is being undertaken in relation to ongoing litigation and/or potential future litigation, and hence is subject to legal professional privilege.

In addition, this matter is strictly confidential. Save as permitted under Section 4 of our terms of business, no information relating to this matter, or our work for it, will be disclosed to any third party without mutual written consent.

You have advised us that all correspondence and all preparatory papers for any report we might make are legally privileged, as they are being prepared in relation to ongoing litigation and linked to the provision of legal advice. Outside of the Engagement Team, or other Deloitte Partners and employees necessary for us to deliver our work, we will therefore take reasonable skill and care to identify papers, memoranda, correspondence and other materials prepared by us as being "Legally Privileged and Confidential" (or bear equivalent wording) and that they are circulated through Rodric Williams, Your Litigation Lawyer.

2 Our Services and responsibilities

(a) Our Engagement Team

It is our intention that Gareth James will be the Partner responsible to You for the Services described in this letter, unless otherwise agreed with You (such agreement not to be unreasonably withheld or delayed). David Noon, our Service Line Leader with overall responsibility for the services we provide to You, will also be available as required.

Chris Lauder, a Director within our Governance and Controls team, will lead the delivery of our Services to You, together with Mark Westbrook and Charlotte Desourdy, both Senior Managers. They will establish direct working relationships with the appropriate people working on the Client Team. Gareth, Chris, Mark and Charlotte will be supported by Tom Scampion, Partner, who has particular experience in performing work and preparing reports under similar circumstances; and other members of our team as required.

We understand that You do not require any of our team to be available to act as a named expert witness. Should this be required, we would need to agree a separate engagement letter for those Services and Deliverables.

Together they comprise the "**Engagement Team**".

For the purposes of this engagement, we are advised that the client team at POL will consist of Lesley Sewell, Chief Information Officer; Chris Aujard, General Counsel; Belinda Crowe, Programme Director; Julie George, Head of Information Security (deputising for Lesley Sewell if absent); and Rodric Williams, Post Office Ltd Litigation Lawyer. The client team will report on this engagement to Paula Vennells, Chief Executive. We note that we will be advised of any future changes to the client team.

Together they comprise the "**Client Team**".

(b) Services

Part 1 of our Services will provide the following:

- Obtain an understanding of the Allegations; the key risks in and internal controls over the Horizon HNG-X processing environment relevant to the integrity of processing; the measures in place to record and preserve the integrity of system audit trails and other background matters that we may deem necessary to complete our Deliverable.

POL00222758

- Obtain an understanding of the key differences between the current Horizon HNG-X processing environment, and the system which this replaced (here-to referred to as the "legacy Horizon system").
- Review, understand and consolidate the corresponding investigations, assurance activities and remediation actions which You or third parties have undertaken (see Appendix 1 for the "Sources of Information" known to be within scope at this stage) focussing on three primary areas:
    - Work that has been performed to assure the design and operation of key control activities that created and preserve the integrity of processing across the Horizon HNG-X environment (the Audit Store);
    - Work that has been performed to assure the design and operation of key control activities that created and preserve the integrity of interfaces with the DVLA third party system and the Horizon HNG-X environment;
    - Investigations and actions that have been taken in response to the thematic findings of Second Sight, as outlined in Your supplied document "POL Summary of Second Sight anomalies" (see Appendix 1).
- Hold discussions with relevant members of Your staff and other key stakeholders as pre-agreed with You, to deliver the work outlined above;
- Prepare the Deliverable outlined in section 2(d) below;
- Attend twice weekly meetings or conference calls with Your Client Team, to explain our approach, status of work and the commentary within our Deliverable; and
- Carry out any other work required by You which is reasonably incidental to the above.

You do not require Deloitte to comment on or test the quality of the assurance work performed, nor opine on its adequacy, sufficiency or conclusions, or the integrity of the Horizon HNG-X processing environment (nor the legacy Horizon system).

As engagement requirements are discussed, clarified and agreed further, we will outline the additional scope and timeline for such work via the Change Order process as set out in Appendix 2. Any Part 2 work You require us to perform will be agreed under these Change Order processes. This may include, but will not be limited to:

- Testing on data held within the system audit trails, to assess (for example) conclusions previously drawn by Fujitsu into the extent of known deficiencies;
- Assessment and profiling of system audit trails, to look for characteristics of and trends in unusual behaviours in the system transactional core;
- Enquiry into and testing of the nature and extent of unit, system and user acceptance testing of the Horizon HNG-X processing environment, during its implementation;
- More detailed consideration as to any aspects of the internal control environment which operate over the current Horizon HNG-X processing environment which were not in place or operating over the legacy Horizon system.
- Understand the nature and extent of interfaces with other third party systems and test the operating integrity of dataflows to and from certain of these systems; and

- Testing of responses to thematic concerns raised by other independent reviews.

The scope of our services and any deliverables will be limited solely to the Services and Deliverables set out in this Contract. We will make no representations in respect of and will not consider any other aspect.

Our work will be performed through a combination of desk based inspection of documentation, corroborative enquiry and through third party provided evidence or contact, as agreed between You and us.

(c) Our responsibilities

In performing the Services, we will be responsible for:

- undertaking the procedures as necessary to produce our deliverables; and
- confirming the factual accuracy of our report with You.

You agree that other than as set out in the Services section above, we will not audit or otherwise test or verify the information given to us in the course of the Services. In particular, unless otherwise instructed by You to do so, we will not perform or re-perform any assurance work that has tested and concluded on the design, implementation and operational effectiveness of any internal controls over the Horizon processing environment.

Our work will be limited by the time and the information available. Whilst we will report our findings in accordance with the agreed scope of work having considered the information provided to us in the course of carrying out the Services, additional information that You may regard as relevant may exist that is not provided to (and therefore not considered by) us. Accordingly, our Deliverable(s) and our work should not be relied upon as being comprehensive in such respects. We accept no responsibility for matters not covered by or omitted from our Deliverable(s) due to the specific nature of our work instructions from You.

In particular, we note that, in certain respects, we will be reliant on the integrity of those people whom we interview, and that our ability to corroborate and test what we have been told may be limited by the available information.

We shall discuss with You any difficulties we encounter with completing our work should any problems arise.

You acknowledge that You are responsible for establishing and maintaining an effective internal control system that reduces the likelihood that errors or irregularities will occur and remain undetected; however, it does not eliminate that possibility. Nothing in our work guarantees that errors or irregularities will not occur, nor is it designed to detect any such errors or irregularities should they occur.

The scope of our Services and our responsibilities will not involve us in performing the work necessary for the purpose of providing, neither shall we provide, any assurance on the reliability, proper compilation or clerical accuracy of any plan, budget, projection or forecast ("prospective financial information") nor the reasonableness of the underlying assumptions. Since any prospective financial information relates to the future, it may be affected by unforeseen events. Actual results are likely to be different from those projected because events and circumstances frequently do not occur as expected, and those differences may be material.

POL00222758

Deloitte.

(d) Format and use of the Deloitte Deliverables

The format and timing of the reports (the "Deliverables") issued by us will be agreed with You. The content of such Deliverables is expected to be an executive summary and a written report, as follows:

Executive Summary:

- A summary of our objectives, approach, work performed and observations, suitable for Board presentation and discussion in their meeting on the 30 April 2014 (noting any key outstanding points, if applicable, and subject to the accuracy of our assumptions and the fulfilment of Your responsibilities, below);

Written Report:

- Introduction – reconfirming the context of our appointment and the scope of work performed.
- Our Approach – outlining the procedures we have adopted in the delivery of our work, those documents reviewed and the individuals we have interviewed;
- Understanding the Horizon HNG-X Processing Environment – based on the documentation provided to us, provide an overview:
  - Relating to the Technical processing environment – envisaged to be a description of technical matters of the Horizon HNG-X system, consisting of, where information is provided to us:
    - key statistics relating to the processing environment and its range of functions (as stipulated by Fujitsu), including the design and operation of the data integrity protocols (the Audit Store);
    - key matters relating to its network architecture, internal and external interfaces, software components, hardware components;
    - key matters relating to its history, including the timing of its implementation, the nature of Governing responsibilities over this project and the key enhancements that Horizon HNG-X delivered compared to the legacy Horizon system; and
    - key responsibilities relating to the current operation of the Horizon HNG-X processing environment, including change control, security management, system operations (including error handling procedures, follow-up and resolution), end-user support and system recovery, and assurance responsibilities over these key controls.
  - Relating to the User environment – envisaged to be a description of the usage environment of the Horizon HNG-X system, consisting of, where information is provided to us:
    - a description of the types of users in the system and the physical environments in which Horizon HNG-X is accessible;
    - the types of transactions processed by the system and, at a reasonable level, how the integrity of these transactions is verified and preserved;
    - how more than daily, weekly, monthly, quarterly and annual reconciliation processes operate and how variances and/or errors are handled;
    - the nature of key workarounds and other ad hoc processes that are commonly adopted by users; and
    - a summary of the categories of the alleged defects in Horizon HNG-X.
- An Assurance Map - showing those sources of Your assurance which You have shared with us and the areas of key risk relating to the integrity of processing that these were designed to assure;

Deloitte.

- Matters for Consideration - an assessment of Your Assurance Map in the context of Your objectives and significant matters we have observed during our work that we recommend You consider further.

Any Deliverable should not be copied, referred to or quoted to any other party, except in the context of Your defence of the Allegations, or be used for any other purpose. We draw Your attention to clause 5 of the enclosed Terms of Business that sets out the conditions under which the Deliverables will be provided to You.

In the event that You wish to share our Deliverable with third parties, we may consent to such a course subject to us receiving 'hold harmless' undertakings (or their equivalent). These procedures notify them that:

- the disclosure to them will not create any duty, liability or responsibility whatsoever to them in relation to our Deliverable or any of its contents;
- the Deliverable was not prepared for their use or with their needs or interests in mind; and
- they should keep our Deliverable confidential and not copy or circulate our Deliverable, or any extracts of them, to any third party without our express written permission.

We understand that You are unlikely to make any public announcements which would refer to our work. If this situation changes however, You agree that You will not make any such public announcement(s) on this matter referring to Deloitte or our work in any way without providing prior notification of the wording of any public announcement to us and without our prior written consent to such wording, such consent will not be withheld unreasonably.

3 Client Responsibilities and Assumptions

(a) Client Responsibilities

In connection with the provision of the Services, we refer You to clause 3 of the enclosed Terms of Business. These confirm Your responsibility for the provision of information and decision-making in connection with the Services we are to provide. In addition, our delivery of the Services is dependent upon Your completion of the following:

- You acknowledge and agree that our performance of the Services is dependent on the timely and effective completion of Your own activities and responsibilities in connection with this engagement, as well as timely decisions and approvals by You;
- You agree to making available to us all information You deem relevant to this review;
- You agree to providing timely access to relevant personnel in order for us to obtain sufficient information to inform our understanding and report;
- Unless we are otherwise instructed, You agree to carrying out all contact with third parties;
- You agree to providing a nominated point of contact for us throughout the work;
- You agree to provide a room for our team and secure storage facilities for paperwork, if required, at 148 Old Street, London; and
- You agree to assess the Deliverable we provide to You, to determine the most appropriate courses of action for You.

POL00222758

Deloitte.

You acknowledge and agree that our performance of the Services is dependent on the timely and effective completion of Your own activities and responsibilities in connection with this engagement, as well as timely decisions and approvals by You.

The responsibilities set out above and those contained in clause 3 of the Terms of Business are together referred to in this Contract as the "**Client Responsibilities**".

(b) Assumptions

The Services, Charges (as set out in Section 4 below) and timetable are based upon the following assumptions, representations and information supplied by You ("**Assumptions**").

- Horizon HNG-X is also knows as Horizon Online in Your organisation. We will refer to the processing environment as Horizon HNG-X through-out our work. The system which Horizon HNG-X replaced will be referred to as "the legacy Horizon system".
- Only matters relating to the Horizon HNG-X processing environment will be considered in our review. We will not consider any information relating to the legacy Horizon system, with the exception of that necessary for us to obtain an understanding of key enhancements that the Horizon HNG-X delivered when it was implemented,
- Deloitte will not provide a legal or any other opinion at any point throughout the work;
- That sufficient information is available on a timely basis regarding the scope of Services and Deliverables for us to be able to carry out our work;
- That all pertinent information relating to the nature of the Allegations against You has been provided to us such that we are fully aware of the detail of the Allegations;
- Unless otherwise instructed, that Deloitte staff will have no direct contact with any third parties other than named Fujitsu contacts that You provide to us;
- The individuals we may need to interview will be available to us for sufficient time for us to perform our work during the period of our assessment and third parties can be contacted on a timely basis by You to request further information should this be required;
- Deloitte will not verify or test any information provided directly by You, or indirectly by third parties via You;
- Deloitte will adopt a time limited approach to our work, operating to key milestone dates dependent on the accuracy of our assumptions and the fulfilment of Your responsibilities, above; and
- Deloitte will not review any contractual provisions in place between You and third parties.

(c) Client contacts

We understand that Rodric Williams, Litigation Lawyer, will be Your nominated point of contact and that requests for information and documentation should be copied to Belinda Crowe.

Deloitte.

4 Our Charges

We will base our charges upon the actual time and materials incurred, plus out-of-pocket expenses and applicable value added tax. The billing rates we will apply match those of previous specialist advisory work which we have performed for You in 2013.

We estimate that the Part 1 work will take 15 days of senior time to deliver. To provide some certainty over our fees, we will cap our total fee for Part 1 work at £50,000 (plus VAT and out of pocket expenses). Charges for work done under a Change Order will be based on the rate card below (in addition to this fee cap for the Part 1 work), unless otherwise agreed.

Grade	Advisory Rate /hr
Partner	£630
Director	£540
Senior Manager	£430
Manager	£400
Senior Consultant	£310
Consultant	£185
Analyst	£145

If during the course of our work, or Change Order there-under, a need for ancillary specialist services not specified in this Contract is identified, agreement to their use and related charges will be obtained before any expenditure is incurred.

5 Terms of Business and Liability Provisions

The enclosed Terms of Business form an integral part of the Contract between us and Your attention is drawn to them. You agree that for the purpose of clause 6 of these Terms of Business, our aggregate liability arising from or in any way in connection with the Services shall not exceed £750,000.

6 Variations

If You or we wish to request or recommend any addition, modification or other change to the Services or performance required under this Contract, we each agree to follow the change control procedures described in Appendix 2.

POL00222758

Deloitte.

Acknowledgement and acceptance

We appreciate the opportunity to be of service to You and look forward to working with You on this assignment. You can be assured that it will receive our close attention.

If, having considered the provisions of this Contract You conclude that they are reasonable in the context of all the factors relating to our proposed appointment and You wish to engage us on these terms, please let us have Your written agreement to these arrangements by signing and returning to us the enclosed copy of this letter.

Yours faithfully,

GRO

Deloitte LLP

Post Office Ltd agrees to the appointment of Deloitte LLP on and subject to the terms of the Contract set out in this Engagement Letter and its enclosures.

Signed: GRO

Duly authorised for and on behalf of Post Office Ltd

Printed Name: Chris Aujard

Position: General Counsel

Date: 25/4/2014

Enclosures:
Appendix 1 – Sources of Information
Appendix 2 – Change Control Procedures
Appendix 3 – Template Change Order
Appendix 4 - Deloitte LLP Terms of Business, Consulting and Advisory Services

Deloitte.

APPENDIX 1

ENGAGEMENT LETTER DATED 9 APRIL 2014
SOURCES OF INFORMATION

For Part 1 work, we will use the following sources of information which have been provided by You:

1. "Horizon Core Audit Process" which outlines how Horizon HNG-X has been designed to operate;
2. "Draft Factfile" which deals with how POL uses Horizon HNG-X in the branch network;
3. "Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications" which outlines the environment in which Horizon operates;
4. "Table of the deficiency themes" which outlines areas that underlie some of the allegations that Horizon HNG-X is deficient;
5. "POL Summary of Second Sight anomalies" which is an internal POL summary of the anomalies within Horizon HNG-X referring to para's 6.4 to 6.10 of Second Sight's July 2013 Report;
6. Fujitsu's response on the "Local Suspense" / 14 Branch anomaly;
7. Fujitsu's response on the "Receipts Payments" / 62 Branch anomaly;
8. The "Spot Review Bible", which contains the ten "Spot Reviews" sent to POL and POL's responses (cf para 2.7 of Second Sight's July 2013 Report);
9. Fujitsu's "Horizon Data Integrity" document, which provides a technical description of the measures built into Horizon HNG-X to ensure data integrity, including a description of several failure scenarios, and descriptions as to how those measures apply in each case;
10. Fujitsu's "Horizon Online Data Integrity for Post Office Ltd" document, which provides a technical description of the measures that are built into Horizon HNG-X to ensure data integrity and descriptions as to how those measures apply in each case;
11. Current Fujitsu POA ISO27001 certification;
12. The associated Fujitsu POA ISMS Statement of Applicability;
13. The Post Office Horizon PCI DSS certificate;
14. The Post Office Horizon PCI DSS signed AOC;
15. The Post Office Horizon PCI DSS ROC;
16. The last 3 published Post Office ISMF minutes with Fujitsu; and
17. The last 3 Fujitsu Security Ops Reports

Additional documents may be provided by You as part of our engagement. The full list of information sources will be disclosed in our Deliverable.

POL00222758

Deloitte.

APPENDIX 2

ENGAGEMENT LETTER DATED 9 APRIL 2014
CHANGE CONTROL PROCEDURES

1 If at any time either party wishes to request or recommend any addition, modification or other change to the Services or performance required under the Contract (a "**Change**"), the party proposing the Change will submit a written request for the Change (a "**Change Request**") to the other party.

2 All Change Requests will require the authorisation in writing by the named person who has signed the Engagement Letter for and on behalf of the Client, in the case of Change Requests initiated by the Client or the Deloitte client service partner as specified in the Engagement Letter in the case of Change Requests initiated by Deloitte.

3 Deloitte will investigate the implications for the Contract of implementing each Change Request, and prepare and submit to the Client a proposed Change Order, in the form attached as Appendix 3, in respect of such Change Request. If in a party's judgement, the time to evaluate and respond to one or more Change Requests, because of their magnitude, complexity or frequency, may result in a delay in the Services, that party will notify the other party. The parties will then need to agree an appropriate course of action.

4 The Client will notify Deloitte in writing of its decision as to whether or not it wishes to implement the proposed Change as soon as reasonably practicable but in any event no later than 5 days (or such other period agreed by the parties) after receipt of the Change Order submitted by Deloitte. Should the parties wish to proceed with the proposed Change, the Change Order shall be signed by the named person who has signed the Engagement Letter for and on behalf of the Client and the client service partner, or other authorised representatives (such signed document being referred to as a "**Change Order**").

5 Neither party is obliged to proceed with any proposed Change (and the related changes) and no Change (and related changes) will be effective and enforceable against a party, unless and until a Change Order for that Change is signed on behalf of both parties. Until the Change Order for any proposed Change is signed, Deloitte will continue to perform and be paid for the Services as if the Change had not been proposed.

6 Deloitte shall be entitled to charge for all reasonable costs and expenses incurred in connection with investigating the implications of a Change Request, whether or not a Change Order is signed in respect of such Change Request.

Deloitte.

APPENDIX 3

ENGAGEMENT LETTER DATED 9 APRIL 2014
CHANGE ORDER NUMBER ___

Date

<Client Name and Address>

For the attention of < >

Dear Sirs

This Change Order (including any appendices, schedules, and/or attachments), records agreed changes to the Contract between Deloitte LLP ("Deloitte" or "we") and < > dated < >, as amended by prior agreed Change Order(s) or amendments thereto. This Change Order constitutes the entire understanding and agreement between the Client and Deloitte with respect to the changes set out in this document, supersedes all prior oral and written communications with respect to such changes (including, but not limited to Change Requests), and may only be amended in writing, signed by authorised representatives of both parties.

The section(s) of the Engagement Letter set forth below [and any earlier Change Order(s) or amendments thereto] is/are hereby amended, effective as of [effective date of changes], by the following text:

1 **Scope and objectives**

2 **Our Services and responsibilities**

3 **Client Responsibilities and Assumptions**

4 **Our Charges**

5 **Consequential changes to the Contract**

POL00222758

Deloitte.

Except as expressly modified herein, all other terms and conditions of the Contract remain unchanged. Please indicate Your agreement to the terms of this Change Order by signing and returning to Deloitte the enclosed copy of this Change Order.

Yours faithfully,

Partner
Deloitte LLP

Agreed by Post Office Ltd:

Signed: _____

For and on behalf of Post Office Ltd

Printed Name: _____

Position: _____

Date: _____

Deloitte.

APPENDIX 4

ENGAGEMENT LETTER DATED 9 APRIL 2014
DELOITTE LLP - TERMS OF BUSINESS

DELOITTE LLP
TERMS OF BUSINESS

Consulting and Advisory Services

1 THE CONTRACT BETWEEN US

1.1 The whole of the contract between you (the "Client", or "you") and the UK limited liability partnership of Deloitte LLP ("Deloitte" or "we") is described in the covering engagement letter, proposal and/or statement of work and any appendices and enclosures thereto other than these Terms of Business ("Engagement Letter"), and these Terms of Business, (together the "Contract"). Nothing we discussed prior to your signature of the Engagement Letter induced, nor forms part of, the Contract (including but not limited to any confidentiality agreements which, if any, you agree are terminated hereby) unless it is specifically set out in this Contract. No-one is authorised to agree any variations to the Terms of Business or the Contract unless any variations are documented and agreed in writing between us.

1.2 If we have already started work (e.g. by gathering information, project planning or giving initial advice) then you agree that this Contract applies retrospectively from the start of our work.

1.3 The definitions set out in these Terms of Business, the Engagement Letter and any appendices or enclosures shall have the same meaning throughout this Contract. If there is a conflict between these Terms of Business and the Engagement Letter, these Terms of Business govern.

1.4 If any provision of this Contract is determined to be illegal, void or unenforceable in whole or in part, such provision or the affected part shall be deemed not to form part of this Contract but all other provisions together with the remainder of the affected provision shall remain in full force and effect.

1.5 Deloitte LLP is the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"). For the purpose of this Contract, "Deloitte Parties" means all entities that are members of the DTTL worldwide network and each of their subsidiaries, predecessors, successors and assignees, and all partners, principals, members, owners, directors, employees and agents of all such entities. Deloitte LLP (which for these purposes includes reference to its subsidiaries) uses the word "partner" in respect of its members and certain of its senior employees in its dealings with you to describe, respectively, a member and senior employee of Deloitte LLP in their capacity as such. Deloitte LLP gives a number of its employees the title of "director", which denotes that they are senior employees and not that they hold the office of director for the purposes of the Companies Act 2006.

Contracting parties and assignment

1.6 This Contract is between you and Deloitte. You agree that your relationship is solely with Deloitte as the entity contracting with you to provide the Services. Notwithstanding the fact that certain Services under the Contract may be carried out by personnel provided to Deloitte from other Deloitte Parties through service or other agreements, you agree that none of the Deloitte Parties (except Deloitte) will have any liability to you and that you will not bring any claim or proceedings of any nature (whether in contract, tort, breach of statutory duty or otherwise and including, but not limited to, a claim for negligence) in any way in respect of or in connection with this Contract against any of the Deloitte Parties (except Deloitte) or any subcontractors that we may use to provide the Services. The foregoing exclusion does not apply to any liability, claim or proceeding founded on an allegation of fraud or other liability that cannot be excluded under English law.

1.7 This Contract does not make either of us an agent or legal representative of the other, nor does it create a partnership or joint venture.

1.8 Neither of us may assign or otherwise transfer the benefit of this Contract without the prior express written consent of the other, save that we may assign the benefit of this Contract to any of the Deloitte Parties, including any successor to our business. Further, neither of us will directly nor indirectly agree to assign or transfer any claim against the other arising out of this Contract to any other person.

Third party rights

1.9 No person who is not a party to this Contract other than the Deloitte Parties and our subcontractors, if any, shall have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms.

1.10 This Contract can be varied without any third party's consent.

2 OUR SERVICES AND RESPONSIBILITIES TO YOU

2.1 The scope of our services and any Deliverables to be provided under this Contract together with our responsibilities for them (together the "Services") are as described in the Engagement Letter. We will use all reasonable efforts to supply the Services in accordance with any timetable referred to in the Engagement Letter or otherwise specified by the parties. However, unless both parties specifically agree otherwise in writing, all dates given by Deloitte or specified by you for the supply of the Services are intended for planning and estimating purposes only and are not contractually binding.

Engagement Team

2.2 Whilst we will attempt to comply with your request for specific individuals, the appointment of all personnel to perform the Services and the nature and duration of their assignment shall be made as Deloitte considers appropriate. We may at any time replace or reassign any personnel assigned by us to the Services; in such circumstances we will endeavour to give you reasonable notice.

2.3 You will be responsible for ensuring that your staff involved with this Contract have the appropriate skills and experience. If any of your staff fail to perform as required, you will provide additional or replacement staff as we may reasonably request.

Data Protection

2.4 In providing the Services to you or otherwise in connection with the Services, we may:

(i) need to collect, hold and use information (e.g. contact details) about identifiable individuals ("Data Subjects"). We may also use such information as part of our client account opening and general administration process (e.g. in order to carry out anti-money laundering, conflict and financial checks or debt recovery). Information about a Data Subject may be transferred to or accessible from DTTL or DTTL member firms' offices around the world for these purposes or for the purposes identified in the following paragraph. Should your officers or employees enquire, please inform them that we may hold information relating to them for these purposes; and

(ii) occasionally contact a Data Subject with details of events/seminars we are holding, or we may send a Data Subject publications or newsletters, which we believe may be of interest to him or her. If a Data Subject does not wish to

POL00222758

Deloitte.

receive this information, please let us know by informing the partner responsible for the Services.

2.5 We reserve the right to monitor telephone calls and electronic communications for the purposes of ensuring compliance with our legal and regulatory obligations and internal policies.

2.6 In providing some of the Services to you we may be processing information about Data Subjects on your behalf and thus act as a "Data Processor" for the purposes of the Data Protection Act 1998. In these circumstances, we will (i) only process personal data in accordance with your lawful and reasonable instructions; and (ii) comply with security obligations equivalent to those imposed on you, as Data Controller, by the seventh principle of that Act.

3 YOUR RESPONSIBILITIES

3.1 You are responsible for determining that the scope of the Services is appropriate for your needs.

3.2 Our performance of the Services, the timetable, the level of our Charges and any fee estimates each depend on the accuracy and completeness of any assumptions set out in the Engagement Letter. Please tell us if you believe any of these assumptions are unrealistic for any reason.

3.3 You will give us all the information that is necessary for the performance of the Services. In this context, you agree we shall not be treated as being on notice of information given to us in the course of previous engagements and so all information that is relevant to the Services must be given directly to the engagement team even if the same information has been given to us previously in the course of a different contract or engagement. Please note that, other than as set out in the Engagement Letter, we will not audit or otherwise test or verify the information provided to us in the course of the Services. You agree that we shall be entitled to rely on all information provided to us and on your decisions and approvals in connection with our Services and to assume that all such information provided to us from whatever sources is true, complete and not misleading. We will not be responsible for the consequences of any information provided to us in the course of the Services not being complete, accurate or current.

3.4 Where needed to assist us in performing the Services, you will (i) take decisions and obtain management approvals promptly; (ii) give us full and prompt access to your people and premises and those of your affiliates and to your other advisors associated with the engagement, together with all necessary administrative support; (iii) obtain any approvals, licences and security clearances promptly (including any relating to third parties, our personnel and any subcontractors); and (iv) keep us promptly informed of any proposals or developments in your business relevant to the Services.

3.5 You agree that you remain solely responsible for managing all aspects of your business, for taking all decisions and operating all accounting, internal control or management information systems. This includes applying your independent business judgement to evaluate any advice or recommendations that we give you. You will be responsible for deciding whether our recommendations make sense in the context of your business, and whether you wish to rely on, implement or act on them, including the actions necessary to realise any expected benefits.

3.6 Where you are using third parties to provide information, materials or other assistance in support of the Services, or you are employing other suppliers whose work may affect our ability to deliver the Services, you will be responsible for the management of such persons and their performance, including the timeliness and quality of their input and work.

3.7 You will also be responsible for paying the Charges in accordance with this Contract.

Legal advice

3.8 Our Services may be conducted alongside your legal advisers, acting separately for you. To the extent they relate to our performance of the Services, we may need to review sections of draft agreements prepared by your legal advisers but we are not qualified to provide legal advice. Any agreement is the product of negotiation between its parties and you agree that it is your responsibility to obtain appropriate legal advice and to decide whether in all the circumstances you are prepared to accept any proposed agreement.

4 RESPONSIBILITIES TO EACH OTHER

Confidentiality

4.1 We each agree that where either of us is in possession of information about the other that is by its nature confidential, or is designated as such by the other (whether in writing or orally), including this Contract ("Confidential Information"), we each undertake to (i) keep it confidential; (ii) use it only in connection with providing and receiving the Services; and (iii) not to disclose it to any other person without the other's prior written consent. These undertakings will not apply to any information that otherwise becomes generally publicly available, was possessed prior to the commencement of the Services (or prior to being designated as Confidential Information), or is lawfully acquired from a third party who is under no obligation of confidence or information which is or has been independently developed by the recipient.

4.2 We each will be entitled to disclose Confidential Information to our legal advisors to protect our legitimate interests and to comply with any legal, professional or regulatory requirement. You agree to reimburse any costs we may incur in complying with any such disclosure requirement relating to any of our Services to you imposed in any proceedings or regulatory process not involving any substantive claim or proceeding against us, provided that we notify you promptly and, where reasonably or legally possible, prior to disclosure.

4.3 You agree that we may share Confidential Information with any Deloitte Party and any subcontractors we use to provide the Services (or more generally to support our office administration) on the understanding that they will treat the information as Confidential Information in accordance with the provisions of this Contract.

4.4 Unless you tell us otherwise, we may in the performance of the Services attend meetings to discuss your affairs with your other advisers and may do so openly, free from any obligation to you of confidentiality.

4.5 When offering our services to others we may disclose to them that we have acted for you unless you instruct us to the contrary.

4.6 Nothing in this Contract will prevent or restrict any Deloitte Party from providing services to other clients (including services which are the same or similar to the Services) or using or sharing for any purpose any knowledge, experience and skills used in, gained or arising from performing the Services subject to the obligations of confidentiality set out in clause 4.1 even if those other clients' interests are in competition with your own. Equally, you agree that to the extent that we possess information obtained under an obligation of confidentiality to another client or other third party, we are not obliged to disclose it to you or make use of it for your benefit, however relevant it may be to the Services.

Conflicts of interest

4.7 It is our practice, in appropriate circumstances, to check for conflicts of interest before taking on engagements. Deloitte Parties provide many different professional services to clients and we cannot be certain that we will identify promptly all situations where there may be a conflict with your interests. Please notify us promptly of any potential conflict affecting this engagement of which you are, or become, aware.

Electronic communications

4.8 We each agree that where appropriate we may communicate with each other electronically over the internet (including by way of e-mail). Our personnel will also need access to our own systems and data. You agree that you will (at your discretion) i) allow our personnel to use a Deloitte Local Area Network at your premises; ii) and/or provide our personnel with analogue dial-up connections or an Ethernet connection to allow our hardware (typically Deloitte's laptop computers used by members of the engagement team) to connect to our network via your internet communications facilities. Further, in order for our personnel to operate effectively and efficiently they may

Deloitte.

need access to your electronic data and also to your internet communications facilities for the purpose of the engagement. We will only access your internal networks, applications, data or other systems through the terminal hardware or software you make available to us for the purpose.

4.9 Access to your systems by our personnel will be subject to such conditions as you at your sole discretion consider necessary to protect the security and integrity of your data and systems. We each recognise that the internet is inherently insecure and that data can become corrupted, communications are not always delivered promptly (or at all) and that other methods of communication may be appropriate. Electronic communications are prone to contamination by viruses. Each of us will be responsible for protecting our own systems and interests and neither of us will be responsible to the other on any basis (contract, tort or otherwise) for any loss, damage or omission in anyway arising from the use of electronic data (including e-mail) as a form of communication or from our personnel's access to your networks, applications, data or other systems. Nothing in this clause shall exclude any liability arising from the negligent addressing of an email.

Staff

4.10 We each agree not to offer employment to or solicit the other's personnel who within 6 months of such action has been involved directly in the Services or otherwise connected to this Contract (except where an individual responds directly to a general recruitment campaign) nor use the services of any such personnel (either independently or via a third party) for a period of 6 months from the date that the individual concerned ceases to be permanently involved with the Services.

5 DELIVERABLES

Drafts and oral discussions

5.1 In formulating our conclusions, we may discuss ideas with you orally or show you drafts of the Deliverables (as specified in the Engagement Letter) for your comment. We do this on the basis that you will not rely on any drafts or oral comments or advice unless their content is finalised and confirmed to you in writing in the final Deliverables. Accordingly, we will not be responsible if you choose to act, or refrain from acting, on the basis of any drafts or oral comments or advice. If you want to rely or act on oral comments, or advice, please let us know in order that we may deal with them in our final Deliverables. Furthermore, for your convenience, the Deliverables may be made available to you in draft or in electronic as well as hard copy format. Multiple copies and versions of documents may therefore exist in different media. In the case of any discrepancy, the signed hard copy of the final Deliverable is definitive.

5.2 Unless the Engagement Letter specifies other arrangements, you agree that each Deliverable will be deemed accepted by you (and our Services, or the relevant part of them, completed) when it is in its final form or when you first make use of the Deliverable, whichever first occurs.

Use of Deliverables

5.3 The Deliverables and any other advice we provide to you are for your exclusive use and must be used solely for the purpose described in the Engagement Letter. They must not be used for any other purpose, recited or referred to in any document, copied or made available (in whole or in part) to any other person without our prior written express consent. You acknowledge that were you to do so (and without limitation) this could expose us to a risk that a third party who otherwise would not have access to the Deliverable (and/or Confidential Information as defined in clause 4 above), might claim to have relied upon the Deliverable (and/or Confidential Information) to its detriment and might bring or threaten to bring an action, claim or proceedings against us.

5.4 Save as expressly provided by the Engagement Letter, no person other than you may rely on the Deliverables and/or information derived from them and we accept no responsibility to any other person to whom the Deliverables are shown or into whose hands they may come.

Post date events

5.5 We have no responsibility to update any Deliverable for events occurring after completion of this Contract (which, unless provided otherwise in the Engagement Letter, will be the date on which the final Deliverable is delivered or signed), nor to monitor its continuing relevance or suitability for your purposes.

Ownership and intellectual property

5.6 On payment of all of our Charges, you will acquire ownership of the Deliverables in their tangible form and the right to use them internally in your business. We will own and retain ownership of all intellectual and other proprietary rights of any kind in the Deliverables, our working papers (if any) and in all other reports, materials, documentation, software, system interfaces, templates, methodologies and processes and ideas and concepts and techniques that we may use or develop in connection with this Contract (other than materials provided to us by you in which you retain intellectual and other proprietary rights). In circumstances where we may hold certain documents on your behalf, you agree that we may destroy them (together with any other documents related to the engagement) at any time after 6 years from conclusion of the work to which those documents relate.

5.7 You and we agree that neither of us will use the other's name, trademarks, service marks, logos, trade names and/or branding without prior written consent.

6 LIABILITY PROVISIONS

6.1 We will perform the Services with reasonable skill and reasonable care.

6.2 Without prejudice to any defence which we may have, you agree that we will not be liable to you for any loss, liability, damage, cost, charge or expense of whatever nature and howsoever caused and including interest (together "Losses") unless and then only to the extent that such Losses are finally determined to have resulted from our breach of contract or negligence, subject always to the following provisions:

6.2.1 We will not be liable for any Losses arising out of your use of our Deliverables or our advice for a purpose other than as set out in the Engagement Letter.

6.2.2 We will not be liable for Losses arising from the acts or omissions of any person other than Deloitte or any subcontractor (including any Deloitte Party) that we may use to provide the Services.

6.2.3 We will not be liable for Losses arising as a result of the provision of false, misleading or incomplete information or documentation by, or the withholding or concealment or misrepresentation of information or documentation, by any person other than the Deloitte Parties unless and then only to the extent that detection of such defect in the information or documentation or such withholding, concealment or misrepresentation should reasonably have been expected because it was evident without further enquiry from the information or documentation provided to us and expressly required to be considered by us pursuant to the provision of the Services.

6.2.4 Any liability which we may have to you under or in connection with this Contract for Losses suffered by you shall (so far as permitted by law) be limited to such an amount as is finally determined to be just and equitable, having regard to the extent of responsibility for the Losses of us, you, (including your directors, officers, employees or agents), and any person other than us who is jointly or severally liable to you for all or part of the same Losses, provided always that Deloitte's liability to you shall not under any circumstances exceed in aggregate the amount set out hereunder. Any limitation or exclusion or restriction on the liability of any such other person under any jurisdiction, whether arising under statute or contract or resulting from death, bankruptcy or insolvency, or any settlement of such

POL00222758

liability agreed with you, shall be ignored for the purposes of determining whether that other person is liable to you and the extent of responsibility of that other person to you.

6.2.5 Our total liability of whatever nature, whether in contract, tort (including, without limitation, negligence), under statute or otherwise to you and to all other persons who we both have agreed may have the benefit of and rely on our work on the terms hereof, (you and they each a "Beneficiary"), for any and all Losses arising from or in any way in connection with this Contract shall not exceed the amount specified in the Engagement Letter or, if no amount is specified there, £500,000 (five hundred thousand pounds sterling).

6.2.6 Where there is more than one Beneficiary of the Services, the limitation in this clause 6.2 on our total liability to all Beneficiaries shall be apportioned by them amongst them. No Beneficiary shall dispute or challenge the validity, operation or enforceability of this clause on the grounds that no such apportionment has been so agreed or on the ground that the agreed share of the limitation amount so apportioned to any Beneficiary is unreasonably low.

6.2.7 In no event shall we be liable to you, whether in contract, statute, tort (including, without limitation, negligence) or otherwise for (i) loss or damage incurred as a result of third party claims; (ii) loss of profit, goodwill, business opportunity or anticipated savings, loss of or corruption to data, loss of revenues or wasted management or staff time; or (iii) incidental, special, punitive, exemplary, indirect or consequential loss or damage; (together, "Excluded Losses") which you may suffer, howsoever caused and whether or not you or we knew, or ought to have known, that the Excluded Losses would be likely to be suffered.

6.3 Deloitte neither owes nor accepts any duty to any person other than you. No Deloitte Party shall be liable for any Losses suffered by any other person caused by that or any other person's use of or reliance on our Deliverables or our advice.

6.4 Nothing in this Contract shall exclude, restrict (or prevent a claim being brought in respect of) any liability arising from fraud or other liabilities which cannot lawfully be limited or excluded.

6.5 Unless and then only to the extent they have been finally and judicially determined (including the conclusion of any appeal) to have been caused by the fraud of any of the Deloitte Parties, you agree to indemnify and hold harmless the Deloitte Parties against all Losses which they incur in the defence and settlement (including meeting any judicially determined award of damages) of any demand, action, claim or proceeding (a "Claim") brought by any third party in any way arising in connection with this Contract whether or not such Claim is founded upon an allegation of our negligence.

6.6 Any claim or action brought by you under or connection with this Contract must be brought within 24 months of the cause of action arising.

7 CHARGES

7.1 We will render invoices in respect of the Services comprising our fees, out-of-pocket expenses and any charges of specialists, subcontractors and advisers, plus applicable taxes including VAT (together our "Charges"). These will be in accordance with any schedules set out in the Engagement Letter. Our fees are generally calculated on the basis of the time and level of staff required to conduct the Services during normal office hours. Other factors may also be taken into account, including the use of our proprietary expertise, technology and know how, the need to act rapidly or exclusively or outside normal office hours or the importance, complexity or monetary value of the matter concerned. Out-of-pocket expenses will depend on the nature of the Services and where appropriate, staff travelling and subsistence will be reimbursable in accordance with our normal personnel policies.

7.2 Any estimate of the fees involved in the Services will be based upon our assessment of the work involved, taking account of any assumptions set out in the Engagement Letter. Unless we have agreed otherwise in the Engagement Letter, our fees may be adjusted if the Services prove more complex or time consuming than expected. We will let you know when we consider any estimate is likely to be exceeded.

7.3 A fee estimate assumes that we will have full and prompt access at all reasonable times to your premises, directors, staff and any advisers relevant to the Services. It also assumes that you will provide reasonable work space for our people without charge, as well as a suitable office environment and facilities including occasional secretarial support services, photocopying and computer facilities and access to telephone, fax and modem communications.

7.4 Unless otherwise specified in the Engagement Letter, we will invoice our Charges monthly in arrears and a final invoice on completion of the Services. These invoices are due for settlement within 14 days of receipt. You agree that we are entitled to charge you interest on overdue invoices at 2% over the prevailing Royal Bank of Scotland plc base rate.

7.5 We will be entitled to receive all charges incurred up to the date of termination of this Contract for any reason.

8 TERMINATION

8.1 We each may terminate this Contract without notice in the event that the other becomes the subject of insolvency proceedings or calls any meeting of its creditors. Alternatively, either of us may terminate this Contract at any time on 30 days' written notice to the other.

8.2 Should any action taken by you create a situation which amounts to a professional conflict of interest under the rules of the professional and/or regulatory bodies regulating the activities of the Deloitte Parties, we may terminate this Contract without penalty on written notice. We will inform you as soon as reasonably practicable of any situation that occurs that we become aware of that may create a professional conflict which could result in termination in accordance with this clause 8.2.

8.3 Any provisions of the Contract which either expressly, or by their nature, extend beyond the expiry or termination of this Contract shall survive such expiration or termination.

9 GENERAL TERMS OF BUSINESS

Quality of Service

9.1 If, at any time, you believe our service to you could be improved, or if you are dissatisfied with any aspect of our services you should raise the matter with the partner responsible for providing the Services to you. If you would prefer to discuss the matter with someone other than that partner, or if you wish to make a complaint, please call or write to Richard Pust, the firm's Managing Partner, Growth & Markets.

9.2 We will investigate all complaints. You have the right to take any complaint up with the Institute of Chartered Accountants in England and Wales (the ICAEW). You may obtain an explanation of the mechanisms that operate in respect of a complaint to the ICAEW at www.icaew.com/complaints or by writing to the ICAEW. To contact the ICAEW write to the Professional Standards Office, Level 1, Metropolitan House, 321 Avebury Boulevard, Milton Keynes, MK9 2FZ.

Negotiation / mediation

9.3 We each agree that we will attempt in good faith to resolve any dispute or claim arising out of or in connection with the Contract promptly through negotiations between your senior executives and our management. If the matter is not resolved through negotiation then, prior to the commencement of legal proceedings, we will each attempt in good faith to resolve the dispute or claim by participating in an Alternative Dispute Resolution (ADR) procedure which, if not otherwise agreed, will be as recommended to us by the Centre for Effective Dispute Resolution. If the matter has not been resolved by an ADR procedure within 45 days of such procedure being

commenced, then the matter may be dealt with through legal proceedings.

Legal and other obligations

9.4 Nothing in this Contract precludes us from taking such steps as are necessary in order to comply with any legal or regulatory requirement or any professional or ethical rules of any relevant professional body of which we or any of our partners or employees is, at the time, a member.

Force majeure

9.5 Neither of us will be liable for any delays or failures in performance or breach of contract due to events or circumstances beyond our reasonable control.

Governing law and jurisdiction

9.6 The Contract and our relationship (including all contractual and non-contractual rights and obligations arising out of or relating thereto) are governed by English law and the Courts of England and Wales shall have exclusive jurisdiction to settle any dispute that may arise in connection with this Contract and our relationship (including all contractual and non-contractual rights and obligations arising out of or relating thereto).

POL00222758

Appendix 5: Change Order 01

Deloitte.

ENGAGEMENT LETTER DATED 09 APRIL 2014
CHANGE ORDER NUMBER 01 (VERSION 2)

06 May 2014

Mr Chris Aujard
Post Office Ltd
148 Old Street
London
EC1V 9HQ

For the attention of Chris Aujard

Dear Sirs

This Change Order (including any appendices, schedules, and/or attachments), records agreed changes to the Contract between Deloitte LLP ("Deloitte" or "we") and Post Office Ltd ("POL" or "You") dated 09 April, 2014, as amended by prior agreed Change Order(s) or amendments thereto. This Change Order constitutes the entire understanding and agreement between the Client and Deloitte with respect to the changes set out in this document, supersedes all prior oral and written communications with respect to such changes (including, but not limited to Change Requests), and may only be amended in writing, signed by authorised representatives of both parties.

The section(s) of the Engagement Letter set forth below are hereby amended, effective as of 06 May 2014, by the following text:

1 Project scope and objectives

Your project scope and objectives remain as previously described within our engagement letter dated 09 April 2014.

2 Our Services and responsibilities

Our services within 2(b) of our contract dated 09 April 2014 will be amended to include the two following extension areas:

Extension Area 1:

Deloitte will continue to review further supplied documentation relating to the 2010 implementation of HNG-X and other key project documentation supplied by POL, in order to compare the nature and extent of project governance and documentation with the Deloitte methodology. The assessment will include a review of documents that outline if and how transactional branch dataflows and Audit Store features of the system were impacted by the implementation.

In addition Deloitte will assess documentation relating to signoff of business requirements as well as the project's testing strategies and testing assurance provision.

Deloitte will integrate a description of our approach, findings and recommendations from this work into our deliverable.

Deloitte.

Extension Area 2:

Deloitte will review further documentation relating to the specific design features of the processing environment which are asserted to be in place to underpin two key objectives:

1. That sub-post masters have full ownership and visibility of all records in their Branch ledger;
2. That the Branch ledger records are kept by the system with integrity and full audit trail.

Deloitte will produce a schedule of these specific design features, identified only through desktop review of documentation provided by Post Office, and use this to assess whether the existence of the specific design feature has been tested and/or assured. Deloitte will comment on the 2 point above in this context.

Deloitte will not comment on the quality of documentation and will not perform any implementation or operating effectiveness testing.

Deloitte's work, still based on desktop review procedures, will also include:

- Corroboration with an appropriate Deloitte specialist to validate the Audit Store's tamper proof mechanisms.
- Understanding key historic changes in order to assess if key events which could have impacted the control design features above.
- Highlighting those design features where further implementation or operating effectiveness testing should be considered by POL to provide further assurance to the Board.

Deloitte will integrate a description of our approach, findings and recommendations from this work into our deliverable.

In addition to the above areas of additional service, Deloitte will support the delivery of ongoing project update meetings with POL stakeholders prepare a Board Update document (marked as Draft) as at close of our work on the Tuesday 13th May 2014 and Friday 16th May 2014.

4 Our Charges

Our time charges for this additional work will be charged on a time and materials based, in line with the rate card shown in our original Engagement Letter.

5 Consequential changes to the Contract

Except as expressly modified herein, all other terms and conditions of the Contract remain unchanged.

Please indicate your agreement to the terms of this Change Order by signing and returning to Deloitte the enclosed copy of this Change Order.

POL00222758

Deloitte.

Yours faithfully,

GRO

Gareth James
Partner
Deloitte LLP

Agreed by Post Office Limited: GRO

Signed: GRO

For and on behalf of Post Office Limited:

Printed Name: CHRIS AUJARD

Position: GENERAL COUNSEL

Date: 15.04.2014

POL00222758

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 may exist or all improvements that might be made. Any recommendations made for improvements should be assessed by you for their full impact before they are implemented.

Deloitte LLP

London

May 2014