Deloitte.

HNG-X: Review of Assurance Sources

Phase 1 - Board Update at 13/5/14

Subject to completion and delivery of our final report on 16th May 2014

Board Update at 13/5/14

Context

Post Office Limited ("POL") is responding to allegations that the "Horizon" IT system used to record transactions in Post Office 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.

Since its implementation in branches, POL has commissioned or has received an increasing number of pieces of work relating to Horizon to provide comfort over its integrity. Deloitte has been appointed to consider whether this assurance work appropriately covers key risks relating to the integrity of the processing environment and raise suggestions for potential improvements in the assurance provision.

Our work was performed in the context of activities we see in other, similar organisations, as well as guidance offered by recognised, best practise control frameworks. Our work has been performed as a desktop review and thus has not tested the quality or accuracy of any of the assertions made in documentation provided to us.

This part of our work ("Phase 1") is now complete and will report in full to management on Friday 16th May 2014. Our work has been extended in certain specific areas ("Phase 2"), the scope of which we also summarise below. This Phase 2 work will report in summary on Friday 16th May 2014 and in full on Friday 23rd May 2014.

Phase 1 – Approach and Findings

Our work considered three main areas where we would expect assurance sources to be available for the Board, in order to fulfil your objective of being provided with comfort that the Horizon system is fit for purpose and operating with integrity:

1. **Assurance over the system "Baseline"** – this provides comfort that the original implementation project and other changes performed under formal projects were conducted in line with good project management practices, and that detailed testing was performed against agreed business requirements. Such activity verifies that the system was, at that point in time, fit for purpose and implemented as intended.

2. **Assurance over the system "Provision"** – this provides comfort that the underlying IT activities, necessary to providing a system that can run and be used with integrity, are designed and operating effectively. Such activity verifies that key day to day IT management activities, for example, relating to security, IT operations and system changes are appropriately governed and controlled.

3. **Assurance over the system "Usage"** – this provides comfort that key features in the system, designed to prevent or detect matters that would impact the integrity of processing, are in place and operating as intended. This area of assurance often requires detailed underlying work hence is typically conducted under a prioritised ("risk intelligent") approach.

Overall a significant amount of work has been performed, producing significant volumes of documentation relating to the Horizon processing environment. This type of work is comparable to that typically seen in other organisations, where formal risk and control frameworks are not mandated and some IT activities outsourced.

Our key findings relating to each of the three areas of assurance provision are included in the table below, including our recommendations for POL to consider in order to provide further key areas of assurance to the Board.

PHASE 1 – BOARD UPDATE AT 13/5/14
STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.

1

Assurance Area	Key Findings	Recommendations
System Baseline	The implementation of HNG-X in 2010 adopted Royal Mail's "Harmony" project governance methodology. Wipro provided independent assurance that this Project's strategy and delivery of testing, relating to system performance, was effective. However, the 2010 changes did not significantly impact the design features of the system which underpin the integrity of processing by the system - hence this assurance should not be relied on by the Board to provide such Baseline comfort. Provision and examination of further Project documentation has not yet identified a source of comfort for the Board which we consider reasonably delivers "Baseline" Assurance. We note that Fujitsu were planning an independent review in this area in July 2012, but did not progress this when POL appointed Second Sight for purposes understood to be similar.	We recommend that POL complete their investigation of further Project documents that evidence testing has been performed at those points in time and thus demonstrates Horizon was fit for the intended business purposes. In addition, we recommend that the 'baseline' design features, which we will report as part of our extension work, be: ∞ Validated by POL and Fujitsu as a holistic schedule of those key 'baseline' features of the processing environment that must operate effectively for the system to run with integrity. ∞ Formally tested to evidence effective implementation and operation.
IT Provision	The assurance provision relating to the current day activities of IT and Fujitsu in this area adopts and delivers good practise. A formal IT risk assessment has been performed and an IT control framework produced and independently assured, under a recognised assurance standard (ISAE 3402). Some areas of documentation would benefit from further detail or clarification of the extent and nature of testing performed under this standard. Such improvement would also help avoid potential duplication, if additional assurance work is performed.	We recommend that POL work with the ISAE 3402 providers to clarify, in those areas we will highlight in our final report, the extent and nature of testing performed to support their opinion. This will help to ensure that POL's assurance provision is both complete, sufficiently granular and avoids potential duplication of effort in its delivery.
System Usage	Extensive and detailed documentation relating to the system has been produced by technically competent professionals, familiar with the detailed design of Horizon. However, documentation relating to wider business use activities, relevant to the integrity of processing, does not always exist. Documentation available typically includes good descriptions of the key design features that underpin the integrity of processing, but would benefit from enhancement and clarification in certain detailed areas. No work could be demonstrated that provides independent validation and testing of key assertions contained in this documentation and thus we conclude that the Board has minimum assurance in this area. Our extension work (below) is designed to provide suggestions on where such further assurance activity could be prioritised.	We recommend that POL extend the formal risk and control framework, already in place for areas of assurance above, to include these more holistic areas of risk relating to the integrity of processing. For example, assurance over adjustment posting processes, balance transfer processes and transfer acknowledgement activities, operating in the Finance Service Centre, should be considered. This exercise would provide a fully encompassing and coherent framework and a platform from which POL can deliver more comprehensive, efficient and sustainable comfort that the integrity of system processing is being managed appropriately on an ongoing basis.

PHASE 1 – BOARD UPDATE AT 13/5/14
STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.

2

Phase 2 - Scope

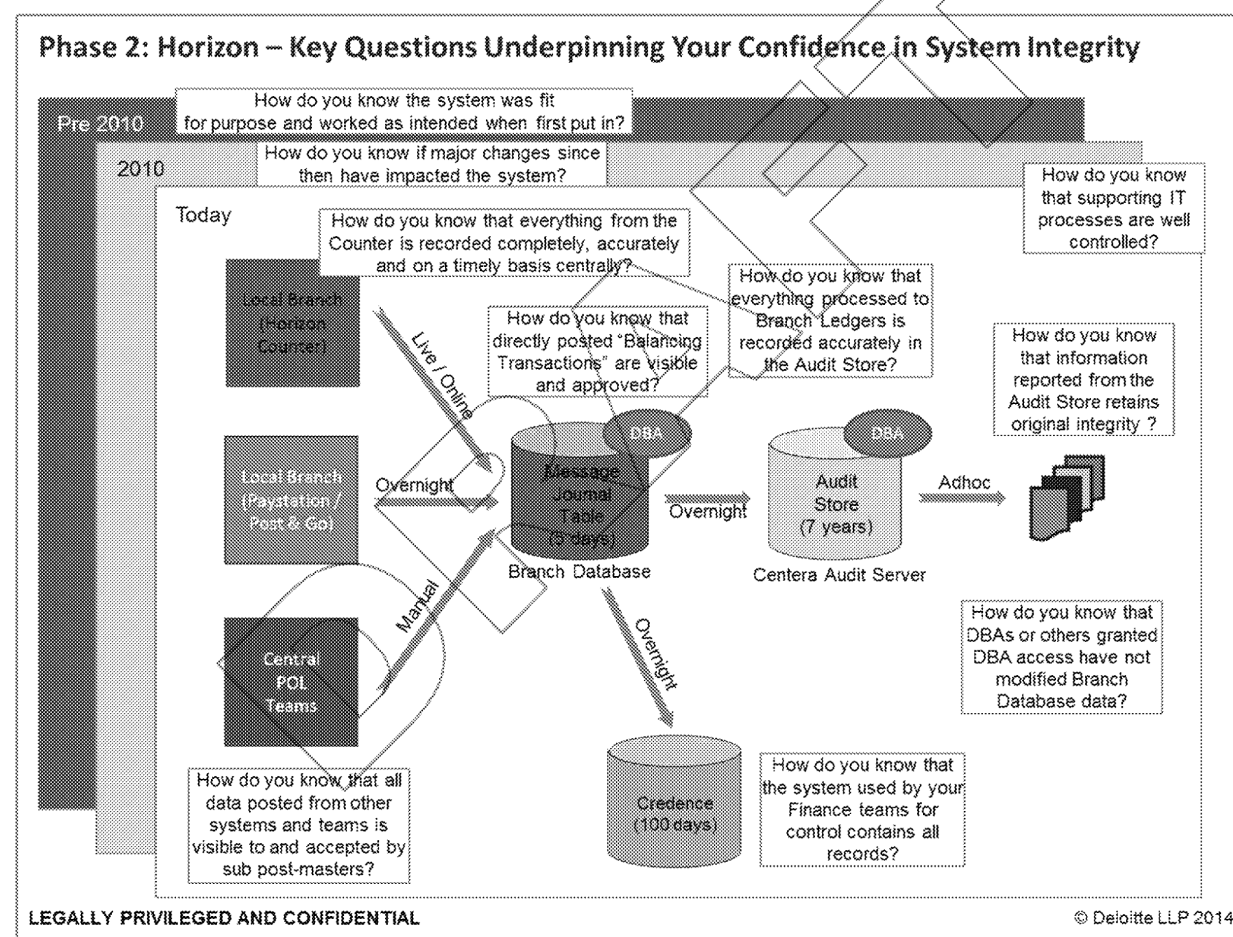POL has extended our work to perform a desktop review of those detailed features of Horizon which:

• ensure that the sub-post master has full ownership and visibility of all records in their Branch ledger; and

• ensure that these Branch ledger records are kept by the system with integrity and full audit trail.

Our extension includes a technical validation of the Audit Store's tamper proof mechanisms and we will also consider, based on supplied documentation, where key events in the past could have impacted these features.

We will structure our work around the further key questions shown in the diagram below (supplementing those key questions from Phase 1), identifying high priority features of Horizon which help manage such risks to system integrity and assessing the extent to which such key features are both documented and assured.

We will then make recommendations on how the Board could prioritise and deliver further assurance in these specific areas.

Our Phase 2 work will report in full by Friday 23rd May 2014.

Phase 2: Horizon – Key Questions Underpinning Your Confidence in System Integrity

LEGALLY PRIVILEGED AND CONFIDENTIAL   © Deloitte LLP 2014

PHASE 1 – BOARD UPDATE AT 13/5/14
STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.

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

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

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

STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.