POL00031384

Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

HNG-X: Review of Assurance Sources

Discussion Areas re: Phase 2

DRAFT - For discussion only.

Deloitte Ref: Project Zebra - Phase 2 Potential Next Steps v2 – Discussion document
SUBJECT TO LEGAL PRIVILEGE

Phase 2: Objectives for Discussion

Context to Phase 2

On the 30th April 2014, the Board raised 2 specific questions, and requested thoughts from Deloitte:

1. In the context of specific allegations regarding non-traceable, "phantom" transactions existing in Horizon – what assurance could be provided over how the system records and maintains the transaction logs;
2. In wider context, what further assurance could be given both pre and post 2010 (when there was a change in Horizon system in use).

In this context, and considering potential downstream public statements that POL may make, we propose further work which will:

- Complete the assessment of assurance sources relating to the 'current day', updating improvement suggestions as further work is performed and focussing on the supporting POL to identify and respond to specific risk areas where further assurance work should be considered to strengthen key risk coverage;
- Perform a series of deep dive assessments into areas of acknowledged specific risk;
- From the foundation of the current day risk framework and assurance map, look back and construct a timeline of variances from this known position.

Potential Areas of Further Work:

Phase 2 (a) – Deep Dive re: Implementation Risks - Assurance Sources (<2wks)

Goal – to be able to complete commentary to the Board on sources of comfort that were in place during the HNG-X implementation in 2010 (which have been verbally asserted to us so far). Using project governance and testing specialists, activities being to:

- Review design of HNG-X Project Governance versus Deloitte Project Governance Framework;
- Review assurance sources relating to business requirements gathering, documentation and signoff;
- Review assurance sources relating to unit, system and user acceptance testing, including an assessment of the 'coverage' of any risk assessment (eg: comms failure) and testing with respect to other deep dive areas of concern being:
  - The Audit Store,
  - Third Party Interfaces and
  - Other key themes of allegations (as provided by POL).

Hypothesis – that a public statement could be supported relating to the scope of testing and the assurance over that testing, as part of the HNG-X implementation.

Phase 2 (b) – Deep Dive re: IT Environment Risks - Assurance Sources (<2wks)

Goal – to be able to complete commentary to the Board on sources relating to IT Environment Risks since HNG-X implementation. Using the existing team, activities being to:

- Perform assurance map timeline analysis to show how the sources of assurance have evolved during and since 2010 relating to the IT Environment Risks;
- Review external and internal audit findings since implementation in 2010 and assess responses re: mitigating controls, remediation and follow-up actions;

- Review the documentation that POL produces regarding 3402 “User Entity Compliance Considerations”;
- Prioritise key areas for ISAE 3402 improvement (including clarifications / the removal of ambiguity).

Hypothesis – that a public statement could be supported relating to assurance activities over the current day supporting IT environment through which Horizon is provided (and this may be extendable to ‘since its implementation in 2010’ if the assurance map timeline support this).

Phase 2 (c) – Deep Dive re: Specific Risks - Audit Store Control Design (< & >2wks)

Goal – to be able to comment further on the design and operation of the Audit Store (not just its documentation). The Audit Store is key to their first specific question relating to Horizon’s ability to record and then maintain an accurate and complete (“tamper proof”) record of system transactions. Using data governance, integrity and analytics specialists, activities being to:

Focussing on the current day Audit Store:

- Based on documentation provided, create a risk framework relating to the Audit Store, the data recorded there-in and its integrity, identifying preventative, detective and monitoring controls designed to mitigate these risks (<2wks);
- Validate this risk and control framework with Fujitsu and POL, agreeing any potential gaps in the control response and mapping sources of independent assurance as a control activity level (<2wks);
- Link to Phase 2(a) assurance and commentary above (<2wks);
- Perform testing of controls, to Deloitte sample size requirements, where no source of independent assurance is already available (>2wks);
- Conduct tests of detail to verify the completeness of certain key control features (>2wks) – including:
  - Full reconciliation (Period X) of Audit Store transactional content to the Branch Database and follow-up of any variances in this reconciliation;
  - Profiling of the Audit Store records by document type, vouching completeness of documentation;
  - Inspection of ‘2nd degree’ Audit trail matters (eg: tracing of non SPM initiated records);
  - Rebuilding, from underlying data, of key reports used for monitoring or key control purposes;
  - Trend analysis and multi-variant cluster analytics on Audit Store data.
- Produce a timeline of historic changes to functionality relating to the audit store, inspecting key change control documentation for each historic change (business reasons, design impacts and control impacts w.r.t to the risk and control framework above).

Focussing on the history of the Audit Store:

- Perform assurance map timeline analysis to show how the risk and control framework relating to the Audit Store (as defined above) has changed both since 2010 and pre 2010.

Hypothesis – that a public statement could be supported relating to the integrity of Horizon’s design regarding the recording and maintenance of its transaction logs (extendable back to X period?).

Phase 2 (d) – Deep Dive re: Specific Risks – Adjustment Postings (<2wks)

Goal – to be able to comment further on transactions in the Branch database which are initiated outside of the Branch / Counter environment, verifying data flow design, control / approval requirements, reconciliations and enquiring into ‘unusual’ events and handling. Using risk and control specialists, activities being to:

- Visit the Finance Service Centre, inspect documentation and hold interview to establish current day policies and procedures relating to adjustment postings, including typical sources if issue for which centrally initiated adjustment postings are created;
- Review existing sources of assurance over the end-to-end process, linking to implementation requirements and testing in 2(a) above and how the transactions are recorded in the underlying Audit Store;
- Identify key risks and controls and how these are monitoring / logged and/or assured;

- Enquire into other matters which may impact the integrity of the adjustment posting process, including:
    - adhoc issues and responses experienced in the FSC,
    - access controls over adjustment posting functionality,
    - appeal processes and resolution activities.
- Perform analytics on the underlying branch database to confirm that only items posted or approved by the local Branch are recorded; and consider how the branch database ‘rolls up’ into Branch ledgers and reconciliations.

Hypothesis – that a public statement could be supported relating to the control and oversight of local branches transactional activities.

Phase 2 (e) – Deep Dive re: Specific Risks – Database Administrator Controls (<2wks)

Goal – to be able to verify the depth of control relating to database administration over both the branch database of Horizon and the Audit Store. Using existing team, activities being to:

- Perform a deep dive into control activities assured in the ISAE 3402 relating to database administration;
- Perform a risk assessment over database administration capabilities, and if/how such access permissions could enable the underlying database structure, records or fields to be added to, amended or deleted in circumvention of change control procedures.

Hypothesis – that a public statement could be supported relating to the integrity of the underlying database.

Phase 2 (f) – Deep Dive re: Specific Risks – What is out there that’s “key”? (>2wks)

Goal – to give confidence that other, potentially key, specific risks, outside of those in 2(c),(d),(e) above, should not be reviewed in greater depth to provide further evidence relating to the integrity of Horizon system. Using risk specialists, activities being to:

- Conduct an exercise with key POL (and potentially Fujitsu) stakeholders to define key risks (across all Horizon processes) relating to the completeness, accuracy and timeliness of processing within Horizon and perform risk clustering and prioritisation to form the basis of a Specific Risk framework.
- Consider ranking each of the risks by significance and likelihood, to produce a specific risk heat map relating to the usage of the Horizon system.

Hypothesis – that a public statement could be supported relating to a risk assessment over the use of the Horizon system.

Phase 2 (g) – Deep Dive re: Specific Risks – Manual Data Entry Risk (<2wks)

Goal – to assess assurance sources over “manual” transactional data entry by Branches (end of day totals / transactions performed in batch – such as ATM, Post & Go?). Using risk and control specialists, activities being to:

- Work with Horizon specialists to identify all sources of ‘batch total’ data entry performed by Branches on a repeated basis;
- Review the risk and control framework governing these processes and identify and review sources of assurance;
- Understand how adjustments, due to error and/or fraud are processed, in line with Phase 2 (d) above.

Hypothesis – that a public statement could be supported relating to the control and oversight of local branches transactional activities.

Phase 2 (h) – Deep Dive re: Specific Risks – Third Party System Interfaces (>2wks)

Goal – to validate documentation. Using the existing team, activities being to:

- Seek sources of evidence that relate to 3P system interface logs;
- Examine contents of such logs to advise on potential next steps.

Note: Before investment in this stage, further verification of implementation testing scenarios and the data flows from third party systems into the branch database should be considered, as the mitigating counter-database messaging protocol may mean that third party systems are a step further removed from the risks of complete/accurate data recording (ie: additional work here in automated interfaces may not be a high priority area to look at).

Hypothesis – that a public statement could be supported relating to interfaces to third party systems

POL00031384

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.