Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

HNG-X: Review of Assurance Sources

Executive Summary - Draft

Emerging findings at 29/04/14, subject to completion of Deloitte work

Deloitte Ref: Board Summary v5
SUBJECT TO LEGAL PRIVILEGE

Executive Summary

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 ("HNG-X") is robust and operates with integrity, within an appropriate control framework.

Since its implementation in branches in 2010, POL has commissioned or has received an increasing number of pieces of work relating to HNG-X to provide comfort over the design and operation of key controls. Deloitte has been appointed to consider whether this assurance work appropriately covers key risks relating to the HNG-X 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 (for example, the COSO framework, as published by The Committee of Sponsoring Organisations of the Treadway Commission).

Our work is near completion and thus this summary outlines our emerging conclusions as at 29th April 2014. Our report, containing final conclusions, additional detail and recommendations for next steps, will be issued in May.

Overall Comments

A significant amount of work has been performed relating to key risks across the HNG-X processing environment. This work is comparable to that typically seen in other, similar organisations.

Specifically, the assurance provision relating to HNG-X's general control environment risks at Fujitsu adopts best practises, where the risk assessment and control framework have been formalised and is independently assured under a recognised assurance standard (ISAE 3402).

The significant work performed in the areas of implementation and specific risk is consistent with that typically undertaken in organisations comparable to POL, where such risks are not required to be formally documented and assured to comply with external governance requirements. POL could obtain greater assurance from this work if it were aligned to a formalised, independently assured, risk assessment.

Governance and controls over change risks relating to the HNG-X implementation align to expected practices (subject to the provision of documentary evidence by POL to support the verbal assertions of interviewees).

Relating to more specific risks (including responses to reported errors), extensive and detailed documentation has been produced by technically competent professionals, familiar with the system, at Fujitsu. These documents include descriptions of the key design and operating features of the HNG-X system in more specific areas and thus contain significant information relating to controls within HNG-X. We note that the documents produced are of system and operational nature, and, whilst consistent with organisations like POL that are not subject to external compliance requirements in this area, would provide greater comfort over the complete coverage of key risks if supplemented from a risk assessed lens.

Our main recommendation for improvement in the assurance provision therefore would be for POL to extend the formal risk and control framework, already in place for general controls, to also embrace key risks and controls holistically across the HNG-X processing environment. For example, to include controls in specific risk and thus more operational areas of the business, such as the Finance Service Centre.

This exercise would provide a fully encompassing and coherent risk and control framework for the HNG-X processing environment, and give a platform from which POL can deliver more comprehensive, efficient and sustainable comfort that key processing environment risks are being managed on an ongoing basis.

Such an enhanced approach would also enable POL to formally optimise the design of the control framework against POL's emerging risk appetite definitions and take forward the more granular improvement suggestions contained in our report. For example, the need for POL to formalise its response to the ISAE 3402 "User Entity Control Considerations", which POL has recently started to document.

Key Emerging Findings

We structured our work around 3 main areas of risk and have aligned our more detailed, emerging findings to these:

IT Environment Risks:

IT Environment Risks relate to the policies and procedures which support the day to day running of the system, such as security management, change control management and system operations management. 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.

Formally structured and independent assurance work has been performed relating to these risks, in line with benchmarks for an outsourced IT processing environment such as HNG-X.

POL's assurance over key risks in this area could be strengthened by POL completing its formal response to "user entity control considerations" of the ISAE 3402 report and by suggesting some refinements to the narratives within the ISAE 3402 to provide further clarity in certain, potentially ambiguous, areas (examples are in our final report)).

HNG-X Implementation Change Risks:

HNG-X Implementation Change Risks relate to the very significant IT changes that required formal project governance structures when HNG-X was implemented. 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".

The design and operation of project governance and control procedures for the HNG-X implementation appears comparable to what we see at other organisations (this is subject to the provision of evidence to support verbal assertions made by POL in this area). No independent assurance has been provided in this area.

Assurance over these implementation risks could be further strengthened through both greater independent scrutiny and through post-implementation assessment. We also note, for future reference, that such significant projects are an opportunity to efficiently capture and create the control and assurance frameworks for Specific Risks (see below), and to help clarify descriptions of controls and their optimal testing once changes are live.

Specific Risks:

Specific Risks relate to those more granular or unique matters, specific to and as applied to POL's HNG-X processing environment, for example inherent features within the application design, required end user activities and application enforced behaviours. ` Controls which mitigate these risks are often referred to as "Inherent System Controls", "End User Controls", "Application Embedded Controls" and "Process Controls". Our work focussed on the interfaces with other systems (DVLA) and the preservation of HNG-X audit trail (Audit Store).

Substantial work has been performed over risks in this area, delivered largely by Fujitsu, in particular in areas where reported issues have occurred in system processing. Based on the areas we have been provided, Fujitsu have produced extensive and detailed documentation relating to the key design and operating features of the HNG-X system, using technically competent professionals, familiar with the system.

In order to provide greater comfort that this work addresses all key risks, this area would benefit from being managed, and documented, through a risk lens, potentially extending the formal risk assessment and control framework already in place for IT Environment risks (above).

Our work relating to both the DVLA interface and the Audit Store found that the level of understanding demonstrated through system documentation appeared comprehensive, and that key controls were referenced within that documentation (such as the use of ‘tamper proof’ IT infrastructure). The documentation has not however been produced from a risk assessed perspective, that would then support more evidenced based, independent verification of these key control features and attestations.

Such a formalisation exercise would not only give greater assurance over specific risks, but would also enable a more automated and thus efficient control design to be considered (for example, more automated controls and further proactive monitoring / alerting to key risk events).

Other matters:

We observed that the risk appetite of POL is yet to be defined, though we understand that an exercise is underway with the ARC to achieve this. We consider this to be an important exercise for POL to perform, as it will help underpin and better optimise the design of your control and assurance landscape (above) in the future.

We also note that POL’s use of Internal Audit could be extended to support the provision of further comfort over specific risk areas. Internal Audit have covered some aspects of these risk in parallel with their work on IT Environment risks, for example, the operation of interfaces to POL SAP, but there is opportunity for this to be extended – for example, system interfaces to Credence and controls relating to adjustment postings.

Sources of Assurance Reviewed

Sources of assurance from the following organisations have been identified and considered in our work:

- Fujitsu, who designed, built and now operate HNG-X.
- Bureau Veritas, who perform ISO 27001 certification over Fujitsu’s networks, including that of HNG-X.
- Information Risk Management (IRM) who accredit HNG-X to Payment Card Industry Data Security Standards.
- Ernst & Young, who produce an ISAE 3402 service auditor report over the HNG-X processing environment.
- Internal audit, who perform risk based reviews within POL.

POL00304160

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.