POL00294440

Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

HNG-X: Review of Assur[illegible]c[illegible] Sources

Executive Summary [illegible]

Emerging findings at 29/04[illegible]mpletion of Deloitte work

POL00294440

Executive Summary

Context

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 2009/10, 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 such key controls.

In the context of helping POL to assess responses to recent allegations made by sub-postmasters, Deloitte has been recently 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 (that published by The Committee of Sponsoring Organisations of the Treadway Commission – the "COSO framework").

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

Overall Comments

A significant amount of work has been performed relating to key risks and the HNG-X processing environment.

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

Significant work has also been performed in certain areas of key risk too, though not structured under a formalised risk assessment nor independently assured.

Subject to the provision of documentary evidence by POL to support information gathered in interviews, governance controls over change management designs to expected practises.

Furthermore, in areas 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 context, and thus contain significant, though unstructured (in the context of a formalised risk assessment and control framework), information relating to controls that response to these specific risks within HNG-X.

Our main recommendation for potential improvement in the assurance provision 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 in project and specific risk areas. This exercise would provide a fully encompassing, more "cohesive" risk and control framework for the HNG-X processing environment, and give a platform from which POL can deliver efficient and sustainable comfort that key processing environment risks are being managed on an ongoing basis.

Such an enhanced, cohesive approach would also enable POL to formally optimise the design of the control framework against POL's emerging risk appetite definitions and take forwards our more detailed suggestions for improvement (below). For example, the need for POL to formalise its response to the ISAE 3402 "End User Control Considerations".

POL00294440

Key Emerging Findings

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

Project Change Risks:

Project Change Risks relate to very significant IT changes that require formal project governance structures, which are governed and controlled outside of day to day system operating procedures. Controls which mitigate these risks are often referred to as "Project Controls". Our work focussed on the implementation of HNG-X in 2009/10.

Subject to the provision of evidence to support verbal assertions made by POL, the design and operation of project governance and control procedures for the HNG-X implementation appears comparable to what we see at other organisations and what we would expect, though no independent assurance has been provided in this area.

Assurance over project change risks could be further strengthened through both gre[illegible]ndependent scrutiny during project activities and through post-implementation assessments. We also [illegible]at such significant change projects are an opportunity to efficiently capture and create the control and as[illegible]meworks for Specific Risks (see below), and to help clarify descriptions of controls and their opti[illegible]sti[illegible]changes are live.

IT Environment Risks:

IT Environment Risks relate to the policies and procedures w[illegible]the day to day running of the system, such as security management, change control management and [illegible]operations management. Controls which mitigate these risks are often referred to as "General Computer [illegible]s". Our work focussed on assurance provided over Fujitsu's activities in these areas.

Formally structured and independent assurance wor[illegible]be[illegible]d relating to these risks, in excess of the benchmark we typically see in non-outsourced IT envi[illegible]en[illegible]-line with benchmarks for an outsourced IT processing environment such as HNG-X.

POL's assurance over key risks in thi[illegible]a c[illegible]be stre[illegible]ened by more formally responding to "end user control considerations", reference[illegible]tic[illegible]E 3402 report and suggesting some refinements to the narratives within the ISAE 3402 to p[illegible]ther cla[illegible]y in certain, potentially ambiguous, areas (examples are noted below).

Specific Risks:

Specific Risks relate[illegible]se m[illegible]granular or unique matters, specific to and as applied to POL's HNG-X processing environmen[illegible]e inherent features within the application design, required end user activities and application enforced b[illegible]rs Controls which mitigate these risks are often referred to as "Inherent System Controls", "End User Contro[illegible]"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. 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 through a formal risk assessment and control framework, as the IT Environment risks are above. Our work relating to both the DVLA interface and the Audit Store, found that whilst the level of understanding demonstrated through documentation was excellent, and key controls, such as the use of 'tamper proof' IT infrastructure are highlighted, evidenced based, independent work to verify these key control features and attestations has not been performed.

POL00294440

Such an exercise 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 an[illegible]ered in our work:

- Fujitsu, who designed, built and now operate HNG-X.
- Bureau Veritas, who perform ISO 27001 certification over Fujitsu's [illegible]works, includi[illegible]t of HNG-X.
- Information Risk Management (IRM) who accredit HNG-X to P[illegible]ent C[illegible]d Industry Data Security Standards.
- Ernst & Young, who produce an ISAE 3402 service auditor r[illegible]he HNG-X processing environment.
- Internal audit, who perform risk based reviews within POL.

Footnote: Examples of ISAE 3402 Clarific[illegible]

Clarifying certain text in the ISAE 3402 report will help [illegible]ternal ambiguity for its interpretation. For example:

- clarify data sources for sampling [illegible]for [illegible]ge cont[illegible]testing);
- improve alignment to POL pol[illegible]d [illegible]g: requirement for unique usernames);
- state sample sizes used (eg: to u[illegible]understanding of the frequency of the control activity); and
- verify that all controls ar[illegible]d to e[illegible](eg: control test 6.5 in section 7 appears to have relied on verbal assertions from Fuji[illegible]

POL00294440

STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.