POL00138271

Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

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

Executive Summary

DRAFT – Emerging findi[illegible]pletion of Deloitte work.

POL00138271

Executive Summary

Context

POL is committed to ensuring and demonstrating that the Horizon system ("HNG-X") is robust and operates with integrity, within an appropriate control framework. Since its implementation in 2010/11, POL has commissioned a number of pieces of assurance work relating to HNG-X and recently appointed Deloitte to consider whether this work appropriately covers key risks.

We have also been requested to raise suggestions for improvement in the assurance provision over the HNG-X processing environment, leveraging our experience at other organisations and knowledge of best practises.

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

Sources of Assurance Reviewed

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

- Fujitsu, who designed, built and now operate HNG-X.
- Bureau Veritas, who perform ISO 27001 certification over Fujitsu 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.

We structured our work around 3 main areas of risk, and our emerging findings below are aligned to these:

- Project Change Risks – relating to significant IT changes that require formal project governance structures. Our work focussed on the implementation of HNG-X in 2010/11.
- IT Environment Risks – relating to the procedures supporting the general running of the system. Our work focussed on assurance provided over Fujitsu's activities.
- Specific Risks – relating to more particular or unique matters, specific to features of HNG-X. Our work focussed on the interfaces with other systems (DVLA) and the preservation of HNG-X audit trail (Audit Store).

Key Emerging Findings

Project Change Risks:

Whilst no independent assurance has been provided over these risks, 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.

Subject to validation, assurance over project change risks could be further strengthened through both greater independent scrutiny during project activities and through post-implementation assessments.

We also note, for potential future reference, that such significant change projects are an opportunity to efficiently capture and create the control and assurance frameworks for Specific Risks (which we refer to below), as well as help to clarify key control descriptions to avoid potential downstream ambiguity.

POL00138271

IT Environment Risks:

Formally structured and independent assurance work has been performed relating to these risks, in excess of the benchmark we typically see in non-outsourced IT environments and in-line with benchmarks for an outsourced IT processing environment such as HNG-X.

We identified one key area where we consider the assurance provision needs improvement – relating to the "end user control considerations", referenced in Section 6 of the ISAE 3402 report by Ernst & Young. Such matters are important to consider, ensuring that the assurance provided by the ISAE 3402 is interpreted in the appropriate context of controls within POL. We are not aware of such work being performed.

There are also opportunities for further enhancement in the quality and clarity of the assurance activities, including:

- *Assurance Clarifications:* clarifying certain text in the ISAE 3402 report will help remove potential ambiguity for its interpretation. For example, clarifying data sources for sampling (eg: for change control testing); improving alignment to POL policies and procedures (eg: requirement for uni[illegible]ernames); stating sample sizes used (eg: to underpin understanding of the frequency of the control a[illegible]); and verifying that all controls are tested to evidence (eg: control test 6.5 in section 7 appears [illegible]elied on verbal assertions from Fujitsu staff).
- *Assurance Focus:* a significant proportion of the assurance activi[illegible] are weighte[illegible]ds security management risks. Once risk appetite is defined (see below) [illegible]ould recommend that the balance of assurance between this area and other important areas, s[illegible]s sys[illegible] operations and change control, be considered. This will help give confidence that optimal lev[illegible]ance are being provided across risks.

Specific Risks:

Substantial work has been performed over risks in th[illegible]a, [illegible]rgely by Fujitsu. They have produced extensive and detailed documentation relating to the k[illegible]si[illegible]perating features of the HNG-X system, using technically competent professionals, familiar with [illegible]em.

However, despite this significant provi[illegible]of [illegible]nation, [illegible]consider this area to be where POL's assurance sources would benefit most from f[illegible]atte[illegible]isk driven, independent challenge by risk assurance professionals to key Specific Risk a[illegible] wor[illegible]ing to both the DVLA interface and the Audit Store, found that whilst the level of understanding d[illegible]ated through documentation was excellent, evidenced based, independent work to verif[illegible]cont[illegible]ures and attestations has not been performed.

To support the app[illegible]unders[illegible]g of these risks, and to support prioritisation of assurance activities, we would recommend tha[illegible]xten[illegible] IT Environment Risk and Control framework (used in the ISAE 3402 above) to cover more Specific R[illegible]ntrols. Such an exercise would also enable a more automated and thus efficient control design to be [illegible]idered (for example, more proactive monitoring and 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 little use of Internal Audit appears to have been made in key IT Risk areas – which may present opportunity for POL to strengthen your response to Specific Risks, noted above.

POL00138271

STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.