POL00105635

Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL

Project Zebra – Phase 1 Report

HNG-X: Review of Assurance Sources

Contents and Key Extracts

DRAFT - For validation in advance of Board discussion on Wednesday 30th April.

POL00105635

Contents

(Note – only key extracts are presented below for the purposes of validation and the Board meeting on 30th April 2014, below).

POL00105635

Executive Summary

Summary Introduction, Terms and Scope

In response to Post Office Ltd's (POL's) desire to demonstrate that your current day Horizon Next Generation ("HNG-X") system is robust and operates with integrity, within an appropriate control framework, POL has commissioned and been provided with work relating to the HNG-X processing environment.

POL has appointed Deloitte to independently produce, based upon the information made available to us by POL, a summary of this work undertaken, raising key matters for your consideration which we consider relevant to POL's objectives above.

This report introduces the concept of the "risk universe" over the HNG-X processing environment. As part of our work we have created a high level risk universe, based on the recognised COSO (Committee of Sponsoring Organisations) model. We have then used this model to consider where we would expect assurance over key risks to have been obtained by POL. For the purposes of our reporting, we have grouped these risks into 3 main areas:

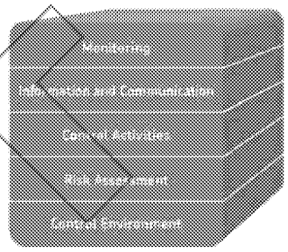

Fig 1: Simplified COSO Model

- Project Risks – those risks relating to very significant changes to the processing environment that require formal project governance structures to be setup and deployed. Controls which mitigate these risks are often referred to as "Project Controls".
- Environmental Risks – those risks applicable 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".
- Specific Risks – those risks that are more granular or unique in nature, as applied to POL's HNG-X processing environment, specific to matters such as application enforced behaviours; unique system design and interaction features; required end user activities , and . Controls which mitigate these risks are often referred to as "Inherent System Controls", "End User Controls", "Application Embedded Controls" and "Process Controls".

As per best practises, we also recognise the need for the response to the risk universe to be driven by the risk appetite of the Board; and to be delivered through risk intelligent and balanced controls. Our report makes reference to these terms, which we define in this context as:

- Risk Appetite – is the level of residual risk which is acceptable to those in charge of governance, around which the internal control environment and be designed and operated.
- Risk Intelligence – is the ability of management to take risk appropriately into consideration when making decisions, to underpin conformance with risk appetite. 'Monitoring',' Information and Communication' and 'Risk Assessment' are dimensions of COSO that are all relevant to management's ability to be risk intelligent.
- Control balance – is the ability to shape optimally efficient responses to risk, balancing control activities which are preventative, detective and monitoring in nature.

To further assist with understanding our work in appropriate context, we note that:

- We have only considered assurance sources relating to the current day HNG-X processing environment, and we have not looked at any assurance sources relating to POL's legacy Horizon system(s).
- We have relied on information provided by POL and, other than the approved contact we had with Fujitsu, we have not met nor spoken to any third parties during our work.
- We have not verified or tested the information provided, and thus we cannot comment on its quality, accuracy nor the completeness of any documents or matters there-in included.
- We have not reviewed nor considered any contractual provisions in place between you and any third parties.

POL00105635

Summary Understanding of the Processing Environment

The Horizon system has been used by POL since 1995. Designed, built and operated in conjunction with Fujitsu, it has processed many millions of transactions across thousands Post Office branches during this time, and has a significant number of interfaces to manage and control data-flows, both internally and externally with third party systems. HNG-X is currently used by more than 68,000 users across 11,500 Post Office branches.

In 2010/11 the system underwent a significant upgrade, through the branch by branch implementation of the HNG-X solution. The key purpose of this project was to enhance the infrastructure on which system was operating, for example, removing data stores from local branch environments and providing the ability for POL to better secure key data assets. Our report is thus only relevant to the processing environment from this point forwards.

A key feature of the HNG-X system is its audit trail. The system has an "Audit Store", which is a secure area containing digitally signed (tamper proof) copies of all completed branch transactions and other key operational events. All records in this store have a unique, sequential identifier (assigned at the Counter) which not only provides evidence of completeness of the store, but also links the audit trail record permanently to its original source – at both branch and counter (and therefore user) levels.

Since its implementation, a number of organisations (in addition to POL's own business and IT resources) have been involved in performing work over the HNG-X processing environment. These include:

- Fujitsu, who designed, built and now operate the system for POL.
- Bureau Veritas, who perform ISO 27001 certification over Fujitsu's networks, including that of HNG-X.
- Information Risk Management (IRM) who accredit to the Payment Card Industry Data Security Standard.
- Ernst & Young, who produce an ISAE 3402 service auditor report.
- Post Office internal audit.

When considering the work performed by these organisations, we refer to it in one of two ways:

- Assurance work – work provided by an independent organisation, suitably qualified in the subject matter and experienced in the provision of conclusive assurance statements. In the context of HNG-X sources, we consider the ISAE 3402 report, PCI DSS accreditation and work of internal audit to be examples of 'assurance work'.
- Other work – work not provided by an independent party, and/or who is unlikely to be experienced in the provision of risk driven assurance work. We consider work such as that from POL's outsourcers, peer reviews and the diagnostic investigations / spot reviews that have been performed, to be examples of 'other work'.

Summary of Work Performed

Our detailed scope of services is outlined in our Engagement Letter (Appendix 2). To summarise, we have:

- Reviewed the documents listed in Appendix 1 and clarified certain matters with POL and Fujitsu.
- Created a high level risk universe, based on our experience of computer processing environments.
- Considered the documents POL has shared relating to work done over project and environmental risks.
- Considered the documents POL has shared relating to work done over specific risks, and looked further at work to do with specific risks relevant to the:
    - Interfaces with DVLA systems;
    - Implementation of and migration to HNG-X; and
    - Integrity of the HNG-X Audit Store.
- Mapped key assurance work and other work to the risk universe, highlighting key potential gaps or areas of potential ambiguity.

POL00105635

Key Matters for Consideration

Risk Area	Key Matters for Consideration	Nature of Work Done
(1) General	a. ***Risk Appetite:*** During our work, only occasional linkage of work to the risk appetite of POL was noted. Whilst not unusual in the consumer business sector, such articulation and embedding of risk appetite assists with the delivery of better optimised and prioritised key controls and assurance activities. b. ***Internal Audit:*** During our work we have not been furnished with any examples of Internal Audit assurance over key HNG-X risks on behalf of those in charge of governance. We find it unusual that a risk driven internal capability such as internal audit have performed no work on the HNG-X processing environment over the time period considered by our review.	N/a
(2) Project	a. ***Project Governance:*** Governance procedures described to us (verbally) suggest that the expected levels of business involvement in pre-go live system and user acceptance testing was performed as part of the implementation; and that business users were appropriately involved in signing off of system requirements and readiness to go-live (full system reconciliations). The quality and nature of this testing is key to the 'baseline' or 'inherent' assurance that the system has operated in line with intentions since go-live. However, we have not yet been provided with documentation that supports these verbal assertions (which we understand is being recovered by POL). b. ***Post Implementation Assurance:*** Project assurance relating to post implementation assessment, incident reporting and lessons learned is outstanding to be reviewed by Deloitte. c. ***Control Framework:*** The ability of documentation to fully support information relating to the detailed design of controls relating to specific risks is unclear (eg: whilst JSNs are sequential is there an systems operations control which checks the completeness of this sequence proactively?).	Other work only, no assurance work noted.
(3) Environmental	a. ***Risk Appetite and Assessment:*** Whilst work performed is comparable to that which we see at other organisations, POL has not yet performed an exercise to assess coverage of key controls and assurance work against their own risk appetite. b. ***End User Control Considerations:*** The ISAE 3402 report requires interpretation in the context of these controls at POL. They are outlined in section 6 of the ISAE 3402 report. Without such analysis, the assurance provided by the ISAE3402 is weakened. We are not aware of any such work being performed by POL or other organisations. c. ***Assurance Focus:*** There is significant, potentially duplicated, assurance (from multiple sources) relating to certain security management risks. However, only one source of assurance (the ISAE 3402 report) is available relating to non-security related "system operations" and "change management" risks. This leads to significant reliance on the quality and nature of assurance provided by that source. d. ***Assurance Clarifications:*** In the context of detailed testing and assurance procedures, there are areas of the ISAE 3402 report which would benefit from further clarification, in order to remove ambiguity from its interpretation. For example: ○ the report does not clarify from where populations of data tested in samples were obtained and thus how exposed conclusions may be from internal fraud or deliberate override of control (eg: for change management testing, were samples picked from the population in the secure Audit Store, or from another source?). ○ the report does not draw out certain key features in the control design, which we would assume are present, for example, control objective 4.8.11 (relating to access to the system being restricted to appropriate users) does not explicitly state and test that users must have and use their own unique username, thus underpinning audit trail integrity. ○ the report is not explicit in the sample sizes used for testing. ○ the report contains tests which appear 'weak' in nature, for example, control test 6.5 in section 7 appears to test through discussion with personnel only, without clarifying if anything was done to corroborate such verbal assertions.	Both assurance work and other work

POL00105635

(4) Specific	a. ***Risk Driven Considerations:*** The current documentation over specific risks has been largely written in response to key incidents or events, by non-independent parties and from operational perspectives. Whilst detailed, it is also not written from a risk and assurance perspective and is rarely evidential in its content. b. ***Control Framework:*** There are areas where an understanding of the design and nature of operations relating to specific risks is available, but the design, implementation and operating effectiveness of **key controls** has not been aggregated into a risk driven framework nor assured by independent parties in detail. c. ***Interfaces - DVLA:*** Whilst environmental risk relating to system operations is largely assured in the ISAE 3402, we note that no evidence of specific or detailed testing or assurance work has been carried out over specific risks relating to the DVLA interface (both IT and business in nature). d. ***Audit Store:*** This records all transactional activity and certain (key) system events. Work we have seen performed on this store has been performed by Fujitsu and is not 'evidence based', as the documentation provides a description of the process they have performed only. It is also not clear from the documentation we have been provided whether: ○ POL has agreed that the current capturing of certain, key system events, is complete and appropriate for potential governance and investigation needs; and ○ Investigatory work on the Audit Store has all been performed by Fujitsu who, whilst technically qualified, do not constitute an independent nor experienced party for risk driven assurance purposes, or what risk analytic tools were used for these purposes. e. ***Proactive monitoring of key specific risks:*** The current assurance environment appears to be "reactive" in nature, with exceptions in processing triggering diagnostic and remediation activity only when reported. It would appear that no use is being made of the Audit Store, for proactive monitoring of unusual or exceptional system events potentially worthy of further investigation and action.	Other work only, no assurance work noted.

Key Potential Next Steps

We recommend that POL consider the following actions to further strengthen the quality and nature of assurance:

1	***Risk Appetite Workshop:*** Conduct an exercise with the POL Board and those in charge of Governance to define Risk Appetite relating to the HNG-X processing environment.
2	***Risk and Control Framework:*** Extend and confirm the completeness of the HNG-X processing environment risk universe and create a more detailed internal control framework which responds to these risks (in particular at Specific Risk levels). Prioritise key areas for improvement (including clarifications / the removal of ambiguity in exist sources) and embed agreed changes in existing assurance sources. This will include the areas already identified below:
	2(a) End User Control Considerations Testing: POL controls called out in the ISAE 3402 as being 'key' to supporting those controls in operation at Fujitsu should be identified and tested;
	2(b) Audit Store Testing: An independent party should review and test the Audit Store functionality, as described within the technical documentation provided by Fujitsu. This should include certain data analytic tests on underlying Audit Store data, to better understand, profile and examine the operation of the Store, and, potentially, use historic characteristics of incidents and errors to analytically search for like characteristics and trends within the audit records
	2(c) Interfaces: An independent party should review and test key interfaces, as described within the technical documentation provided by Fujitsu. This should include certain data analytic tests on transactions flowing through interfaces, to better understand, profile and examine the operation of those data-flows.
3	***Review Project Documentation:*** Assess evidence that business requirements, testing and post implementation assurance were performed sufficiently and adequately as part of the 2010/11 HNG-X implementation project.
4	***Implement More Proactive Monitoring of Key Risks:*** Key risks and the operation of key mitigating controls should be proactively monitored, with automated alerts generated when certain key behaviours in the system are not in line with expectations or intended outcomes (eg: ongoing verification of sequential JSN records in the Audit Store).
5	***Sustainable Assurance Delivery:*** Once the design of the assurance requirements is concluded, an exercise should be performed to optimise the assurance map, to ensure full coverage of key risks, with minimal duplication.

POL00105635