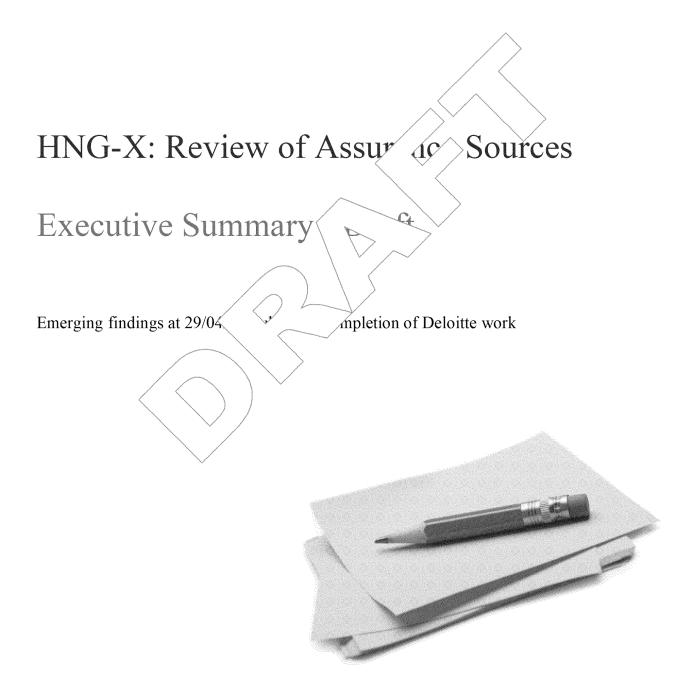
# Deloitte.

STRICTLY PRIVATE AND CONFIDENTIAL



Deloitte Ref: Board Summary v3 SUBJECT TO LEGAL PRIVILEGE

## **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 organis offered by recognised, best practise control frameworks (that published by The Organisations of the Treadway Commission – the "COSO framework").

Our work is near completion and thus this summary outlines our emerginal conclusions. April 2014. Our final report, containing additional detail as well as recommendations and thus this summary outlines our emerginal conclusions.

### **Overall Comments**

A significant amount of work has been performed relative key risks a embedding the HNG-X processing environment.

Of note, the provision relating to HNG-X's general control framework have been recognised assurance standard (ISAE 3402) and independently assured under a

Significant work has also been perfor in a large of areas of a risk too, though not structured under a formalised risk assessment nor independently and areas of a risk too, though not structured under a formalised risk assessment nor independently and areas of a risk too, though not structured under a formalised risk assessment nor independently and areas of a risk too, though not structured under a formalised risk assessment nor independently and areas of a risk too, though not structured under a formalised risk assessment nor independently and a risk assessment nor independently a risk too, and a risk assessment nor independently a risk too.

Subject to the provision of documental ce by POL to support information gathered in interviews, governance controls over the total support information gathered in interviews, governance controls over the provision of documental ce by POL to support information gathered in interviews, governance controls over the provision of documental ce by POL to support information gathered in interviews, governance controls over the provision of documental ce by POL to support information gathered in interviews, governance controls over the provision of documental ce by POL to support information gathered in interviews, governance controls over the provision of documental ce by POL to support information gathered in interviews, governance controls over the provision of the provision of documental controls over the provision of the provision

Furthermore, in are ore specific context, and thus control framework), information relating to controls that response to reported errors), extensive and detailed echnically competent professionals, familiar with the system, at Fujitsu. These documents including the system in more specific context, and thus 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 forgeneral 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".

#### **DRAFT FINDINGS**

## **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 greduring project activities and through post-implementation assessments. We also projects are an opportunity to efficiently capture and create the control and assessments are like.

#### IT Environment Risks:

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

Formally structured and independent assurance work benchmark we typically see in non-outsourced IT environment such as HNG-X.

POL's assurance over key risks in thit control considerations", reference tip (a) be street ened by more formally responding to "end user control considerations", reference tip (a) 2402 report and suggesting some refinements to the narratives within the ISAE 3402 to p (a) in certain, potentially ambiguous, areas (examples are noted below).

#### Specific Risks:

Specific Risks relate em granular or unique matters, specific to and as applied to POL's HNG-X processing environment inherent features within the application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application enforced by inherent features within the application design, required end user activities and application enforced by inherent System Controls, "End User Control which mitigate these risks are often referred to as "Inherent System Controls", "End User Control which mitigate these risks are often referred to as "Inherent System 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.

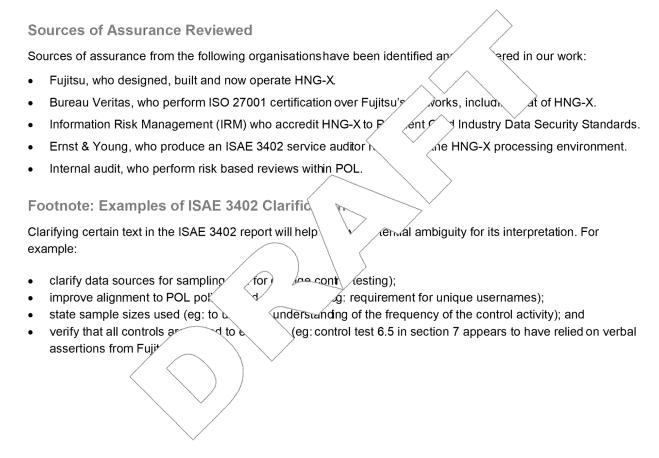
## DRAFT FINDINGS STRICTLY PRIVATE AND CONFIDENTIAL. SUBJECT TO LEGAL PRIVILEGE.

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.





Other than as stated below, this document is confidential and prepared solely for your informationand 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 paty. 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 thedetails of that arrangement (for example, for the purpose of discussion with tax authorities). In any event, no 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 numberOC303675 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. Pleasesee www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.