Confidential **PAPER TWO**

POST OFFICE LTD

RISK AND COMPLIANCE COMMITTEE

Project Zebra - Horizon review by Deloitte

1. Purpose

The purpose of this paper is to:

1.1 Summarise the work undertaken by Deloitte, their approach, key findings, and their recommendations; and

1.2 Outline POL management's proposed actions in light of the above.

2. Background

2.1 Deloitte were engaged by Chris Aujard General Counsel and Lesley Sewell, CIO, at the request of the Board, to conduct a desktop review of certain matters as part of project Sparrow. The terms of reference for the review were based around the following direction provided by the Post Office legal team:

- "POL is responding to allegations from Sub-postmasters that the Horizon IT system used to record transactions in POL branches is defective and that the processes associated with it are inadequate. POL is committed to ensuring and demonstrating that the current Horizon system is robust and operates with integrity within an appropriate control framework"

2.2 Over 100 items of documentation were reviewed by the Deloitte's team who also interviewed management from Atos, Fujitsu, IT, Information Security, Legal and the Finance Service Centre. (Internal Audit was not involved at this stage)

2.3 A detailed (72 page) report has been issued but subject to legal privilege. Management reviews and discussion have since followed. A summary Board Briefing paper has also been issued.

3. Approach

3.1 Deloitte structured its work around a number of key control assertions made by POL over the environment prior to 2010, the changes made to Horizon in 2010 (HNG – X) and the transactions and control environment operating today.

The review considered the risks and controls in the following three areas.

- System Baseline Assurance- original Horizon implementation and 2010 activity.
- IT provision assurance – current IT management activities (security, IT operations, system changes)
- System Usage assurance – Controls around the business processes, their design and operation.

The assertions they considered included the following:

- The system was fit for purpose and worked as intended when first put in.
- Major changes since implementation have not impacted the design features adversely
- Supporting IT processes are well controlled
- Transactions from the counter are recorded completely, accurately and on a timely basis
- Directly posted "Balancing Transactions" are visible and approved
- The Audit Store is a complete and accurate record of Branch Ledger transactions
- Information reported from the Audit Store retains original integrity
- Database administrators (DBAs) or others granted DBA access have not modified Branch Database nor Audit Store data.
- Data posted from other systems and teams is visible to and accepted by sub-postmasters

3.2 The work was desktop and interview based using information that was available to POL and the parties involved. No direct testing of control assertions were made. Deloitte did not test any of the relevant Horizon features and were not required to revalidate the assurance work supplied to them. The exceptional use of the Balancing Transaction process event in 2010 was noted and verbal assertions from Fujitsu relied upon.

3.3 The documentation review included considerable technical information provided by Fujitsu plus third party work assurance undertaken by E&Y (ISAE 3402 report on the Horizon managed service), Bureau Veritas (PCI DSS compliance report on Horizon and ISO 27001) and Royal Mail Internal Audit (Security controls, 2011, 2012. The POL IA team was not in place until June 2013).

4 Key Observations and Findings

4.1 The table below summarises the observations documented on pages 4-5 and 25-26 of the full report.

Strengths	**Areas for attention**
Technical Horizon system documentation is extensive	Documentation is not in a risk and controls perspective
Audit Store integrity maintained through digital seals and signatures and verification processes during extraction of data from the store.	POL reliance on Horizon features to operate as described limited to the IT provision areas of ISAE3402, PCI DSS and ISO27001. These may be sufficient for the purposes of those standards but may not be enough for full POL reliance over operation of Horizon Features and additional testing may be needed.
Governing controls over key day to day IT management activities independently	Business use of documentation not complete or up to date.

Strengths	**Areas for attention**
tested.(ISAE 3402)	
Independent reviews (ISAE, 27001, PCI) provide good coverage for Information Security, fair coverage for Information Systems and Change Management	Pre-2010 baseline assurance work not available.

4.2 Recommendations proposed by Deloitte

Deloitte provided detailed recommendations across three areas:

- Actions that may assist project Sparrow.
- Actions for Future Systems requirements.
- Actions for more holistic approach to risk and assurance over Horizon
  - These are detailed in appendix 1.
  - They centre upon improved documentation, specific review of the privileged access controls around Balancing Transactions, detailed analytical testing of historic transactions, system requirements for any new system and a proposal for a holistic programme of risk and assurance for POL's overall risk and control framework.

4.3 These recommendations should be considered by management to consider in light of:

- Overall business risk.
- Risk Appetite.
- Future of the Horizon System
- Current POL Assurance capacity (1st, 2nd and 3rd lines)
- Legal imperatives
  - The work should also be considered in light of POL senior management commitments to 10 priority actions and behaviours (The 10 Accelerators). Whilst these should not take precedence over key risks to information and the Post Office reputation, management will need to judge priorities, capacity and financial resources.
  - Regard should be given to other initiatives being undertaken across the business. (E.g. the risk and change assurance work with PwC).

4.4 The actions that should be taken with respect to these recommendations have been discussed by Legal, Risk, Information Security, Finance Service Centre and Internal Audit.

Ref	**Summary of recommendation**	**Business View**
A1	Perform a detailed review of Balancing Transactions use and controls.	Yes.
A2	Perform implementation testing of Horizon features.	Only if resources are available and on agreement of scope.

Ref	Summary of recommendation	Business View
		Consider if can be done by E&Y as part of 3402 testing.
A3	Analytical Testing of Historic Transactions	No. Considered to be a large exercise for which the benefit is questionable.
A4	Update/Create documentation for adjustment and reporting processes at FSC	Yes - but see proposed scope from Head of FSC in appendix.
B1	Produce Future Systems Requirements Document.	At appropriate time when new system is considered.
C1-C4	Risk Workshop, Construct risk and control framework, Test Controls, Ongoing Assurance delivery and pro-active monitoring across Horizon and full POL business.	Head of Risk recommends that C1-C4 should be carried out within the confines of the Horizon system to establish a robust control framework. The wider organisational piece is already being addressed through the existing work of the Risk & Compliance team, and the partnership for strategic assurance activity with PwC. Head of ISAG recommends that current Information Security Assurance activity should also be considered.

5. Required Action

5.1 The Risk and Compliance Committee is required to note the activity that has taken place and support the proposed actions, namely;

- Test of controls around the Balancing Transactions,
- FSC documentation, and
- Risk and control framework around Horizon.

Chris Aujard
General Counsel

Appendix 1

Further details of Recommendations from Deloitte.

Ref	Details
A1	**Perform a detailed review of Balancing Transactions use:** Use suitably qualified party independent of Fujitsu to review controls around the need to use the Balancing Transactions functionality, communications with Sub – post masters, reasons for making adjustments and full review of procedures and policies.
A2	**Perform implementation testing of Horizon Features** Use party independent of Fujitsu to conduction implementation testing of Horizon features. Use the review to confirm features are operating as described from documentation.
A3	**Analytical Testing of Historical Transactions** Audit Store documentation asserts the system holds seven years of branch transactions and system event activities. In addition assertions over data integrity, record and field structure and key controls such as JSN sequencing. Not validated by parties outside of Fujitsu. Analytical techniques using modern technology for Big Data sets could allow POL to conduct detailed risk analytics of Audit Store data to verify that the data is as expected and derive other insights or exceptions. This may identify Horizon features that could be automatically monitored.
A4	**Update / create documentation formalised for all key adjustment and reporting processes in operation over Horizon in the FSC.** Identify and document all key activities in the FSC for adjustments to Sub Postmaster ledgers, control activities that reconcile transaction data visible to the Sub-Postmasters to the Audit Store's "High Integrity" copy of Branch Ledger transactions. This can be used to verify the completeness of the Horizon Features in place that have been verbally asserted and perform implementation controls verification in A2.
B1	**Produce Future Systems Requirement Document** Produce system of requirements for any future Horizon platform to deliver against. This should include Key Control objectives, current day control activities. Schedule to include matters that help design preventative, detective and monitoring control activities. Longevity of data retention in Audit Store and cryptographic requirements should be applied.

Ref	Details
C1	**Risk Workshop.** Conduct an exercise with Key Stakeholders in POL to create baseline understanding of risk and risk management concepts, share examples of other companies, and determine how POL can become more risk intelligent organisation.
C2	**Construct a risk and control framework** Extend and confirm the completeness of the Horizon Features and use the framework to prioritise areas for improvement. Extend the framework to POL's overall risk and control framework, not just those areas relevant to Horizon
C3	**Test Controls.** Use the framework to test controls across POL's risk environment. Use a third party to operate against a recognised assurance standard.
C4	**Sustain Assurance Delivery and Implement more proactive monitoring.** Longer term assurance map to sustain assurance delivery for POL over key risks. Consider continuous controls monitoring using automated alerts if key behaviours in the system are identified.

Proposed alternative actions for A4 – Rod Ismay Head of FSC

Ensure comprehensive documentation of:

- Key processes in FSC which identify or respond to accounting issues in branches
- Key controls in the data pipeline from point of sale to central finance systems

This can then be used to provide assurance as to the processes and controls around data transmitted from Horizon and around corrections notified to Sub postmasters.

Reasons for revised proposals:

The FSC does not directly make adjustments to Sub-postmaster ledgers. Instead it identifies or responds to issues and then sends Transaction Corrections to branches such they are able to see and satisfy themselves about changes.

Data is held in very different structures in different places which would make the reconciliation proposed by Deloittes a challenge and may not be beneficial or time efficient

The branch has data in a trial balance list. The audit store has individual transactions. The FSC will have data batched by client to drive the settlement runs.

- Therefore an action can be to update documentation of the data harvesting and interface checks down the pipeline and control testing down that pipe. That could help test the completeness, timeliness and accuracy of data moving down the pipe.