This document contains confidential information relating to Post Office Limited. It is intended for the named recipients only and should not be disseminated further.

Horizon
System
Controls

Review of Key System Controls in Horizon

Post Office Limited

Legally Privileged & Strictly Confidential

Assurance Review

March 2012

Internal Audit & Risk Management

Context and Objectives

The Post Office Limited (POL) network of approximately 11,000 branches processes client and business transactions in excess of £100 billion annually. The majority of transactions are conducted on behalf of third parties, for example, receiving payment for domestic utility bills and paying out from National Savings accounts.

Customer transactions are captured on the Horizon (HNGX) electronic point of sale system in branches and transmitted to central systems (utility payment, external banking and POL finance systems) throughout the day. Overnight, daily summaries are transferred into the central accounting system, POL SAP. The translation process between the two systems is enabled by the Reference Data System (RDS). An overview of the component parts of the HNGX system is provided at Appendix A.

The overall objective of the review was to provide assurance that appropriate IT management disciplines provide a stable IT platform, and that suitable internal controls operate over HNGX transactions and the extraction of these for central systems. In the area of management disciplines the review assessed controls over: access to software; change management; capacity monitoring; and system resilience and disaster recovery. With regards to internal controls over transactions the review covered: master data controls; transaction data; SAP Middleware; and batch updates.

The review also assessed the degree to which actions to address the issues raised in the 2011 Ernst & Young (E&Y) Management Letter regarding the HNGX control environment have been progressed by management.

Key Findings and Conclusion

IT Management Disciplines and HNGX Transaction Controls

The following control weaknesses were identified:

1. **System access:** Access to HNGX in branches is by means of individual user accounts and passwords. However, particularly in sub-post offices, the same user accounts and passwords are often shared between branch staff. The use of individual user accounts is not always practical, e.g. in the case of single terminal branches where time would be lost continually switching between user accounts, and the number and geographical spread of sub-post offices makes it difficult for POL management to ensure access controls are enforced.

   Implication: The ability to identify an individual user responsible for inputting a transaction may potentially be compromised.

2. **Resilience and Disaster Recovery:** Fail-over from the live data centre to the back-up has not been tested since June 2009, although disaster recovery arrangements were tested during the migration to the new system in October 2009. Testing of the business continuity plan has been scheduled for the 24th and 25th of March 2012.

   Implication: The period of any inability to trade as a result of a major system outage may be greater than anticipated.

Internal Audit & Risk Management

Key Findings and Conclusion - Continued

3. **Master data:** No audit trail exists for change requests received by Fujitsu from the Network Business Support Centre (NBSC). Not all 'approved' requesters are documented or referred to on receipt of a change request. The membership of the Lotus Notes email groups, which are used to authorise the Master Data Teams to make changes to standing data, is not known and has not been subject to recent review. One of a sample of 10 change requests was found to have been handled via the "Fast track" process when it should have come through the normal process, resulting in reduced oversight of the change.

   Implication: It is difficult to detect and prevent inappropriate changes being made to master data.

4. **Transaction data:** One of a sample of 5 monthly reconciliations between HNGX generated client transaction summaries and those created by the clients themselves was found not to have a second level review signature. Period-end Senior Management review is not formally signed-off, although it appears to be undertaken.

   Implication: Transaction discrepancies may not be identified resulting in third party clients being undercharged or overcharged for transactions.

Conclusion: IT disciplines around functional changes and capacity monitoring were found to be appropriately designed and also operating effectively. However, access to the system in branches, particularly sub-post offices, can be by means of shared accounts. In addition, fail-over from the live data centre to the back-up centre has not been tested since June 2009. This requirement is of particular importance, as highlighted by an outage in the system in December 2011. Testing of the business continuity plan has been scheduled for March 2012. Controls designed to maintain the completeness, accuracy and integrity of transactional data flows within HNGX were effective, with minor weaknesses noted around manual processes for the validation of master data and transaction data. No evidence was found of material discrepancies arising from these issues.

Control Environment: Some improvement required.

E&Y Management Letter 2011

The 2011 E&Y Management Letter identified a number of areas for improving HNGX and other POL IT system controls. This current Internal Audit & Risk Management (IA&RM) review assessed the degree to which management action plans have progressed to address the issues which related to HNGX. Progress has been made in completing the actions arising from the E&Y Management Letter. The E&Y recommendations that require most additional work relate to: inappropriate access to software change management duties (incomplete segregation between software development and migration roles); the process for the identification and resolution of incidents; the recommendations that POL undertakes an architectural review, configure passwords in line with policy and perform periodic scan of passwords as part of a penetration testing schedule. The penetration testing originally planned for January 2012 has been postponed to March 2012 as the business had to prioritise a test to meet Payment Card Industry (PCI) compliance during January.
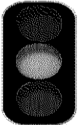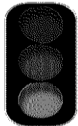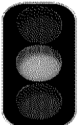
The findings, summarised in Appendix B on page 9, have been shared with E&Y and reflect our assessment as at the end of January 2012.

Management Response

We agree with this report and its findings, and will act to progress the action plan within the agreed timescales **– Lesley J Sewell**
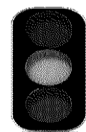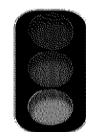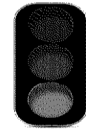
Internal Audit & Risk Management

Summary Findings - IT Management Disciplines

What was done	What was found	Rating
Access to Software: Walked through and sample tested access arrangements for branch, POL and Fujitsu technical support staff.	HNGX access in branches, particularly sub-post offices, is often via shared accounts. Access security controls over the "back end" HNGX environment (including Credence/ TI) were found to be effective, as were physical security controls.	
Change Management: Inspected testing and release management processes, walked through and sample tested completed changes.	Functional changes are initiated and progressed via agreed processes and appropriately approved and tested prior to migration to the live environment.	
Capacity Monitoring: Reviewed and sample tested arrangements for monitoring processing capacity.	Transaction processing capacity, including processor utilisation, disk space etc, is proactively managed and monitored by Fujitsu including forecasting of future requirements.	
Resilience and Disaster Recovery: Inspected, walked through and sample tested arrangements for ensuring resilience and disaster recovery.	System design resilience is high with frequent failure testing of individual components and sub-systems. "Warm" fail-over arrangements exist between the two data centres, although these have not been tested since June 2009.	

Note: For details of systems and data flows, see "HNGX System Overview" at Appendix A.

Internal Audit & Risk Management

Summary Findings - Internal Controls Over Transactions

What was done	What was found	Rating
Master Data: Inspected master data input process and data validation routines and tested via walkthroughs and sample testing of changes .	Minor weaknesses were found around: helpdesk-initiated change requests; documentation and verification of "approved" requesters; and use of "fast-track" requests. Data validation routines have been designed and implemented effectively.	
Transaction Data: Reviewed and sample tested arrangements for the reconciliation and validation of transaction data .	Client account reconciliations are reviewed by team leaders and balances >£400k are reviewed by second line management. However, no formal senior manager sign-off exists for month-end probity reviews.	
SAP Middleware: Inspected data validation controls and tested the reconciliation of inputs to and outputs from Middleware (which translates HNGX data to POL SAP readable format).	A detailed functional specification has been defined and agreed with Fujitsu, covering controls to validate the completeness / accuracy of the interface to POL SAP. Controls relating to data transfer between SAP Middleware and POL SAP appear to be designed and operated effectively.	
Batch Updates: Verified data flows across key interfaces to assess whether batch updates are completed accurately and on time by means of walkthroughs and sample testing.	Effective batch processing / interface monitoring controls are in place, automated and managed via Tivoli Workflow Scheduler (TWS). Automated error alerts are raised by TWS to the Service Management team who escalate to either the Logica Application Management team or Fujitsu for resolution .	

Note: For details of systems and data flows, see "HNGX System Overview" at Appendix A.

Internal Audit & Risk Management

What is Being Done

Access to software

1. Complete an analysis of the potential misuse of individual Horizon user accounts and passwords in branches. Communicate to branch staff the requirement that accounts and passwords must only be used in accordance with Post Office policy. **Priority 2 (Dave M King – May 12)**

Resilience and disaster recovery

2. Agree with Fujitsu a date for full fail-over testing. **Priority 2 (Lesley Sewell – Completed)**

Master data

3. Develop and deploy a formal process for change requests identified and communicated by the NBSC Helpdesk. **Priority 2 (Lesley Sewell – May 12)**

4. Confirm the current membership of Master Data Change and Property Projects Lotus Notes email groups, ensuring that only current team member addresses are included. **Priority 2 (Lesley Sewell – May 12)**

Importance	No of actions	Completed	by Jun 12
Priority 1	-	-	-
Priority 2	4	1	3

Internal Audit & Risk Management

Circulation List

Susan Crichton, Legal and Compliance Director

Christopher Day, Finance Director

Kevin Gilliland, Network and Sales Director

Andy J Jones, Quality and Standards Manager

Dave M King, Senior Security Programme Manager

Neil Lecky-Thompson, Head of Programmes and Planning

John M Scott, Head of Security

Lesley J Sewell, Head of IT and Change

Paula Vennells, Managing Director

Mike Young, Chief Operating Officer

Alice Perkins, Chairman

Derek K Foster, Internal Audit & Risk Management Director

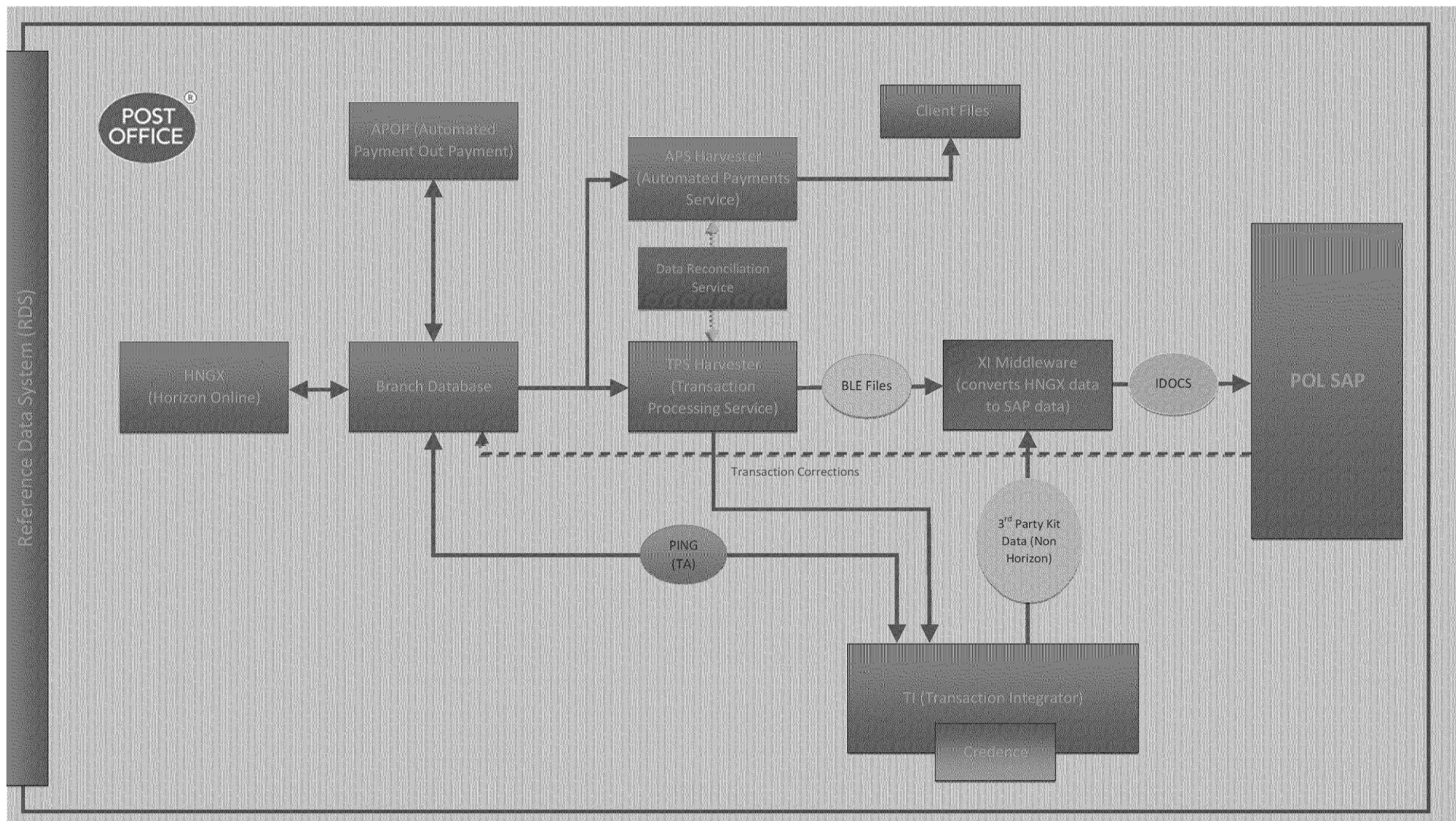Moya Greene, Chief Executive

Matthew Lester, Chief Financial Officer

Emily Pang, Chief of Staff

Peter Tansley, Head of Risk & Assurance

Ernst & Young

Appendix A - HNGX System Overview

Internal Audit & Risk Management

Appendix B - Update on Actions Arising from 2011 E&Y Audit

Finding	E&Y Rating	Summary	Status
1	High	**Governance of outsourcing arrangement with Fujitsu:** POL is responsible for the governance and risk and control frameworks and should have visibility and assurance over their design and operating effectiveness.	Substantial progress made
2	High	**Segregation of change management duties:** Inappropriate access should be revoked and roles for development and migration to live environment should be segregated.	Further work required
3	High	**Change management process:** All changes should be appropriately authorised, tested and approved prior to deployment to live environment.	Substantial progress made
4	High	**Privileged access:** Privileged access to IT functions should be reviewed to determine whether it is appropriate.	Substantial progress made
5	Med	**Periodic POL-owned review of user accounts:** To assist in the identification of inappropriate access and potential segregation of duties conflicts.	Substantial progress made
6	Med	**User administration:** Review the current user access policy and strengthen the existing user administration process within POL and third party service providers.	Substantial progress made
7	Low	**Infrastructure logical security settings:** Undertake architectural review and periodic scan of passwords as part of a penetration testing schedule.	Further work required
8	Low	**Password parameters:** Review and update the Information Security policy and configure all applications in line with policy requirements.	Further work required
9	Med	**Access to generic privileged accounts:** Review across all applications. Consider replacing with individual accounts and implement monitoring controls.	Substantial progress made
10	Low	**Incident identification and resolution:** Regular review of the problem and incident management process to ensure incidents are identified, classified and resolved on a timely basis.	Further work required

The findings above reflect our assessment as at the end of January 2012.

Internal Audit & Risk Management