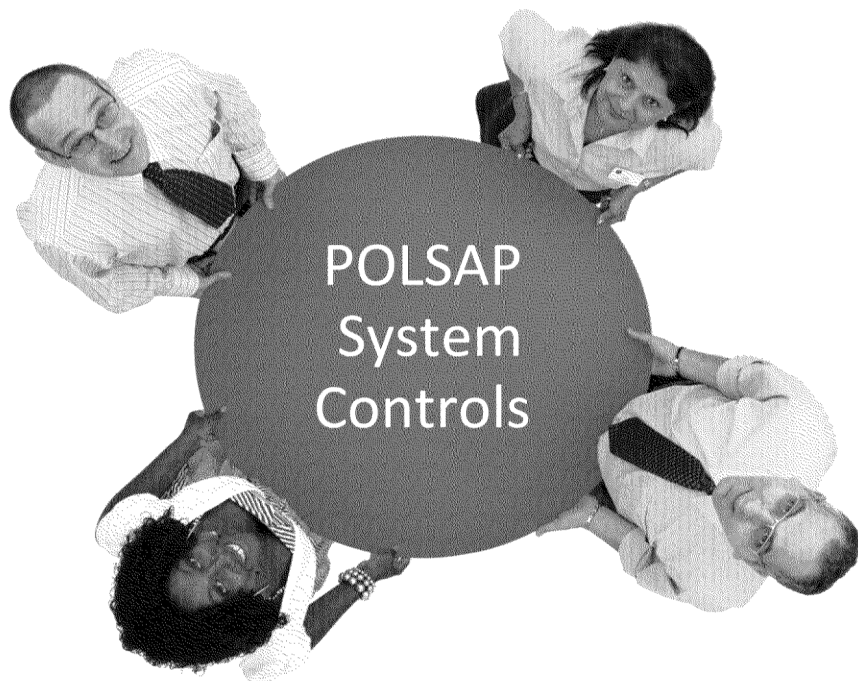


This DRAFT document contains information relating to Post Office Limited. It is intended for discussion purposes only for the named recipients only and should not be disseminated further.



## Follow Up Review of Key System Controls in POLSAP Post Office Limited

Draft Report: AR 12/037b

Assurance Review

May 2013

## Context and Objectives

Post Office Limited (POL) customer transactions are captured through the Horizon Electronic Point of Sale equipment in branches, with daily summaries transmitted to the central accounting system, POLSAP. The translation process between the two systems is enabled by SAP Middleware. The POLSAP system was implemented in 2005/06 and contains functionality to calculate branch balances (cash, stocks, suspense, debtors and creditors) and to settle client balances.

The objective of our review was to assess the degree to which the eleven recommended actions raised in our September 2012 'Review of Key System Controls in POLSAP' (report reference AR12/037) have been implemented.

## Key Findings and Conclusion

Eight of the eleven recommended actions have been implemented. Three areas remain that require further input from management to ensure that the recommended actions have been fully implemented, or the current risk accepted, specifically:

**Transaction Data** – As Wincor are being replaced with NCR for the Post & Go contract, consider whether the original action to draft and agree Service Level Agreements ('SLAs') between POL and Wincor should be completed for the remaining duration of the current Wincor contract.. Furthermore management should ensure the new NCR service contract includes appropriate SLAs for the Post & Go replacement service .

**Access to software** - Complete the review of POLSAP user access in POL FSC. Remove any user accounts and access assignments that are no longer required in the application with immediate effect.

**Change Management** – POL management should consider whether, under the current structure of POLSAP and the current change process, an end-to-end 'overseer' of all or some critical types of changes is required to mitigate the risk of changes not following the established processes .

**Control Environment Rating:** Recommended Actions Partially Implemented

## Management Response

*We agree with this report and its findings, and we have already begun to progress the agreed action plan within the agreed timescales. - Lesley J Sewell*



## Summary Findings

The summary findings from our review are noted below, showing the status of implementation of recommended actions as at 1 May 2013.

	Recommended Action	Remediation date	Work Performed	Findings	Rating
1	<p>Perform a review of master data profiles that provide access to create, modify and remove master data in the Supply Chain and FSC teams and include this within the annual review of user access scheduled for Q3 2012/13.</p> <p>Priority 2</p> <p><b>Mark Wardle</b></p>	Jan 13	<p>We obtained evidence of the FSC user access review and confirmed that user access had been approved.</p> <p>We obtained evidence of the Supply Chain user access review and confirmed that user access had been approved.</p>	<p>Evidence was obtained showing that master data user reviews were performed in Dec 2012 for Supply Chain and in April 2013 for FSC.</p> <p><b>Complete</b></p>	
2	<p>Assign responsibility for monitoring the accuracy and completeness of the interfaces between Paystation, Post&amp;Go and POLSAP to appropriate members of staff.</p> <p>Priority 2</p> <p><b>Steve Beddoe</b></p>	Sept 12	<p>We obtained an update through discussion with the Service Support team.</p> <p>We reviewed personnel roles for Paystation, Post&amp;Go and POLSAP interface monitoring.</p>	<p>Since September 2012 these duties have been split between three staff members who are now responsible for monitoring interfaces and exceptions on each system.</p> <p>These staff are based in Cortonwood, Dearne in the Service Management team and were all identified while on site to be performing the roles required.</p> <p><b>Complete</b></p>	

Rating:	Control implemented / Risk of not implementing recommendation accepted by the POL R&CC	Control implementation in progress but not fully completed	Not Implemented
---------	--	--	-----------------

## Summary Findings (continued)

	Recommended Action	Remediation date	Work Performed	Findings	Rating
3	<p>Draft and agree service level agreements between POL and Wincor for the timely resolution of transaction data errors during the interfaces between Paystation, Post&amp;Go and POLSAP.</p> <p>Priority 2</p> <p><b>Steve Beddoe</b></p>	Jan 13	<p>We discussed with Helen Love and Sharon Brearley the current status of Wincor SLA development.</p> <p>We reviewed the Paystation and Post&amp;Go Application Interface Specifications.</p>	<p>Note: Wincor are the application vendor for Post&amp;Go only. Ingenico are the vendor for Paystation.</p> <p><b>Change Implemented:</b> A fix had been implemented that resolved legacy transactional data transfer failures for around 780 of the approximately 800 data issues, thereby clearing the backlog.</p> <p><b>SLA</b> No contractual SLA is in place between POL and Wincor. The Wincor contract is being terminated in December 2013 to be replaced by NCR. SLAs have therefore not been implemented within the Wincor contract, but will be introduced for the new NCR service.</p> <p><b>On-going – Actions #1 and #2 Raised.</b></p>	
4	<p>Review, define and prioritise which POLSAP batch jobs should be reported to POL by Fujitsu on a regular basis.</p> <p>Priority 2</p> <p><b>Steve Beddoe</b></p>	Feb 13	<p>We reviewed confirmations that batch job listings have been reviewed and obtained listings of batch jobs required to be reported out of hours.</p>	<p>The review has been performed by Service Management. Service Management confirmed with Supply Chain and FSC that the batch jobs reported on are effective.</p> <p><b>Complete</b></p>	
5	<p>Ensure that the process to manage access to software is re-circulated to key personnel who are responsible for managing this process.</p> <p>Priority 2</p> <p><b>Mark Wardle</b></p>	Dec-12	<p>We reviewed evidence of the recirculation of access management process to the relevant team members.</p> <p>We reviewed the distribution list containing those responsible for managing the process.</p>	<p>The process has been recirculated and reinforced to all those stakeholders required.</p> <p><b>Complete</b></p>	

## Summary Findings (continued)

	Recommended Action	Remediation date	Work Performed	Findings	Rating
6	<p>Include a review of POLSAP user access in POL FSC, Supply Chain, Steria and Fujitsu within the review scheduled for Q3 2012/13. Remove any user accounts and access assignments that are no longer required in the application immediately.</p> <p>Priority 2</p> <p><b>Mark Pearce</b></p>	Jan-13	<p>We obtained evidence of the Supply Chain user access review.</p> <p>We requested the FSC user access review.</p> <p>We obtained the Steria and Fujitsu monthly privileged and semi-annual full user access review documentation.</p>	<p>The Supply Chain , Steria and Fujitsu user access reviews have all been completed. In addition, a Supply Chain review is now scheduled every quarter and ISMF meetings record Steria and Fujitsu user changes each month.</p> <p>However, the FSC review has not yet been completed due to issues with user licensing costs taking priority.</p> <p><b>Partially complete – Action #3 Raised.</b></p>	
7	<p>Review the process for identifying and taking action on POLSAP user accounts where the user has left the business. Consider disabling accounts automatically for user accounts that have not logged in for a defined number of days.</p> <p>Priority 2</p> <p><b>Mark Pearce</b></p>	Mar-13	<p>We reviewed Risk &amp; Compliance Committee ('R&amp;CC') meeting minutes from 26 November 2012 to confirm the status of the action to review risks to be accepted and endorsed by the R&amp;CC.</p> <p>We reviewed Paper Fourteen - EY Management Letter Update RCC Nov 12 v2 Appendix B and observed reference to acceptance of the risk of leavers accounts remaining open.</p>	<p>The evidence reviewed confirmed that the risk associated with this action has been formally accepted within the R&amp;CC meeting on 26 November 2012.</p> <p><b>Complete</b></p>	
8	<p>Assign an owner to be responsible for the end-to-end POLSAP change management process for all functional and role changes within the system.</p> <p>Priority 2</p> <p><b>Andy Jones</b></p>	Jan 13	<p>We obtained an update through discussion with Mark Pearce and Andy Jones.</p> <p>We reviewed the POL Change management policy.</p>	<p>The role of end-to-end change management has not yet been implemented as per the action. There has been work to introduce a formalised Change Management Policy encompassing all processes for change within POLSAP, however, no single owner has been identified for the entire process.</p> <p><b>On-going – Action # 4 Raised.</b></p>	

Internal Audit &amp; Risk Management



## Summary Findings (continued)

	Recommended Action	Remediation date	Work Performed	Findings	Rating
9	<p>For POLSAP changes that require user acceptance testing ensure that these are routed to the POLSAP testing team.</p> <p>Priority 2</p> <p><b>Zoe Caddick</b></p>	Sept 12	<p>We obtained an update through discussion with Zoe Caddick and Andy Jones.</p> <p>We reviewed on screen the "CC Audience List" the distribution list for all vendor initiated POLSAP changes.</p>	<p>All changes made via supplier generated channels for POLSAP are routed via Zoe Caddick, and these are all now distributed to the POLSAP testing team through the distribution listing.</p> <p><b>Complete.</b></p>	
10	<p>Complete the review of transactions to monitor for processing capacity to ensure that the list of monitored transactions is up to date and relevant.</p> <p>Priority 2</p> <p><b>Steve Beddoe</b></p>	Jan 13	<p>We reviewed confirmations that transaction monitoring has been reviewed and confirmed with relevant stakeholders.</p>	<p>Evidence was obtained that transactions were reviewed by Service Management. Sid Hadadi (Supply Chain) and Mark Wardle (FSC) were consulted and an updated list of the top 7 transactions is now monitored by Service Management on a daily basis.</p> <p><b>Complete.</b></p>	
11	<p>Review third party user access reviews to ensure that the scope includes all areas of the application that POL determines as priority for review. Document the results of the third party user access reviews within the minutes of the Information Security Management Forum.</p> <p>Priority 2</p> <p><b>Dave King</b></p>	Jan 13	<p>We obtained the Steria and Fujitsu monthly privileged and semi-annual full user access review documentation.</p>	<p>ISMF meetings record Steria and Fujitsu user changes each month, as well as a bi-annual full user access review of these users</p> <p><b>Complete</b></p>	

## Agreed Actions

The following actions have been agreed with management to address the remaining open recommendations from the original report:

### Transaction Data

1. Consider whether the original action should be completed for the current Wincor contract, to draft and agree SLAs between POL and Wincor. (Rod Ismay? – Finance – Date and owner TBC).
2. Ensure the NCR service contract includes SLAs for the Post&Go replacement service (Rod Ismay? – Finance – Date and owner TBC).

### Access to software

3. Complete the review of POLSAP user access in POL FSC. Remove any user accounts and access assignments that are no longer required in the application with immediate effect. (July 2013 - Mark Wardle).

### Change Management

4. POL management to consider whether, under the current structure of POLSAP and the current change process, an end-to-end 'overseer' of all or some critical types of changes is required to mitigate the risk of changes not following the established processes. (Andy Jones – Date and owner TBC).

## Circulation List

Susan Barton, Strategy Director  
Susan Crichton, Legal and Compliance Director  
Christopher Day, Chief Financial Officer  
Kevin Gilliland, Network and Sales Director  
Andy J Jones, Quality and Standards Manager  
Mark R Pearce, Head of Information Security  
Lesley J Sewell, Chief Information Officer  
Paula Vennells, Chief Executive  
Malcolm Zack, Head of Internal Audit

Derek K Foster, Internal Audit & Risk Management Director, RMG  
Justin Thornton, Head of Risk and Assurance, RMG  
Ernst & Young, External Auditors