



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

Report: AR 12/037a

Assurance Review
March 2013

Internal Audit & Risk Management

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 overall objective of the review was to assess the degree to which the issues raised in the 2011/12 Ernst & Young (E&Y) Management Letter regarding the POLSAP control environment have been addressed. Where actions have not been completed, or were completed part way through the financial year 2012/13, any existing compensating controls were also assessed.

Key Findings and Conclusion

The majority of the areas identified by E&Y as requiring improvement have been addressed by POL and third party suppliers. Three areas remain that require further input from management to ensure that the recommended controls have been designed and fully implemented, specifically:

1. Change management: The policy is under development, but has not been formally agreed and communicated as at February 2013.

Implication: Inconsistent changes may be undertaken within the system.

2. User administration: A regular review of POLSAP users in the Cash Centres with privileged system access (including access to create and change user permissions) was initiated in December 2012 but was not performed throughout the whole financial year.

Implication: Inappropriate access may have been obtained, leading to inappropriate activities being undertaken within the system.

2. Password parameters: Whilst a number of password parameters have been changed in line with the E&Y recommendations, the password parameter for account lockout has not been strengthened.



Implication: Inappropriate access may be obtained, leading to inappropriate activities being undertaken within the system.

Conclusion: The majority of areas for improvement identified by E&Y have been completed, or where areas for improvement had not been implemented, it was either demonstrated that compensating controls have been in operation for the whole of the financial year 2012/13 or the risk related to not implementing the proposed changes was accepted by the POL Risk and Compliance Committee. Three areas have been partially implemented and require some further work to complete the recommendations. The findings, summarised on pages 3 – 7 have been shared with E&Y and reflect the IA&RM assessment as at February 2013.

Rating: Substantially Implemented.

Summary Findings

The summary findings from the review are noted below and represent the status of controls as at February 2013. Testing was performed from the control remediation date. Where actions have not been completed, or were completed part way through the financial year 2012/13 any existing compensating controls have been assessed from April 2012.

E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
1 Privileged Access: Consider the implementation of monitoring controls to help ensure controls operated by third party suppliers are in place and in operation.	Nov 2012	Inspected the review of user access performed by management for both POL and third party users on POLSAP. Due to the completion of this recommendation during the year, IA&RM inspected the review of privileged POLSAP activity at the Information Security Management Forum (ISMF) from April 2012 to February 2013.	A review of generic and privileged accounts, including those operated by third parties, commenced in November 2012 at the ISMF. This control has operated on a monthly basis since that date. Additionally, user and system accounts with privileged access in POLSAP have been reviewed at the ISMF since April 2012. Consequently mitigating controls have been operating effectively during the year.	
2 Privileged Access: Where the privileged POLSAP accounts are used to run scheduled jobs, POL should consider creating system accounts with manual login to promote accountability.	N/A	Reviewed the minutes from the Risk & Compliance Committee in November 2012 and correspondence with E&Y in December 2012.	The risks associated with the decision to continue with existing controls, and not to implement the E&Y recommendation, were accepted by the Risk & Compliance Committee (R&CC) in November 2012.	

Key



Control implemented as recommended for the whole financial year / Control implemented part way through the year but with compensating controls in place prior to implementation / Risks of not implementing recommendation accepted by the POL R&CC.







Control implementation in progress but not fully completed / Control implemented part way through the year.

Confidential

Internal Audit & Risk Management

Page 3 of 9

Summary Findings (continued)





E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
3 Privileged Access: Review the need to grant the existing level of access for POLSAP accounts specifically associated with SAP_ALL, SAP_NEW in production.	Nov 2012	Assessed the review of user access performed by management for both POL and third party users on Horizon. Due to the completion of this recommendation during the year, IA&RM inspected the review of privileged Horizon activity at the ISMF from April 2012 to February 2013.	A review of generic and privileged accounts, including those operated by third parties, commenced in November 2012 at the ISMF. This control has operated on a monthly basis since this date. Additionally, system and user accounts with privileged access in POLSAP have been reviewed at the ISMF since April 2012. Consequently mitigating controls have been operating effectively during the year.	
4 Privileged Access: Conduct a review of privileged access to determine the level granted is appropriate and revoke where not.	Nov 2012			
5 User Administration: Strengthen the existing user administration process for cash centres to ensure that 1) documentation is retained, 2) cash centre managers are made aware of the process to follow, and 3) consider the implementation of monitoring controls.	June 2012	Reviewed the documented POLSAP user administration process and the communication of this process to Cash Centre Managers. Point 3) of the E&Y recommendation was tested as noted in area 6 of this report below.	The user admin process in Cash Centres has been designed and implemented since 1 April 2012. However, due to the observation made in the earlier IA&RM POLSAP audit report, management were required to re-communicate this process to ensure cash centre managers are aware of the process. The process was re-communicated to Cash Centre Managers in June 2012.	
6 User Administration: Implement a monitoring process around privileged users (cash centre SU01) where the admin process is controlled by third party suppliers.	Dec 2012	Assessed the review of user access performed by management for both POL and third party users on POLSAP.	A control to monitor the activities of privileged users in POLSAP, including Cash Centre users with access to create and amend user permissions (by means of POLSAP transaction SU01) was introduced in December 2012. This control was not in place prior to this date.	

Confidential

Internal Audit & Risk Management

Page 4 of 9

Summary Findings (continued)



E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
7 User Administration: Strengthen the revocation process of employees that are terminated or no longer require access to POLSAP or Horizon. Consider a tie in with Human Resources.	Nov 2012	Reviewed the minutes from the Risk & Compliance Committee in November 2012 and correspondence with E&Y in December 2012.	The risks associated with the decision to continue with existing controls, and not to implement the E&Y recommendation, were accepted by the R&CC in November 2012.	
8 Change Management: POL to increase their involvement in the change management process, specifically user testing of maintenance fixes. The change management policy should describe this and definitions and responsibilities of all parties involved should be described.	Nov 2012	Reviewed recent communications to the POL testing team for compliance.	All functional and role based changes on POLSAP from the sample tested were communicated to the POL testing team prior to implementation to ensure that appropriate testing can be performed.	
9 Change Management: Implement monitoring controls to ensure controls are operated by third party suppliers.	Q1 2013/14	Reviewed the current version of the Change Management Policy.	POL management are in the process of drafting a Change Management Policy and this is currently in version 0.3. It is the intention of management that the policy will define the overall change management process.	
10 Periodic User Access Reviews and Monitoring Controls: Consider the implementation of a periodic review of appropriateness and segregation of duty issues.	Nov 2012	Assessed the review of user access performed by management for both POL and third party users on POLSAP. Due to the completion of this recommendation during the year, IA&RM inspected the review of privileged POLSAP activity at the ISMF from April 2012 to February 2013.	A review of privileged and generic user accounts on POLSAP was carried out in October 2012 and signed off in November at the ISMF.	

Confidential


Internal Audit & Risk Management

Page 5 of 9

Summary Findings (continued)

E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
11 Generic Privileged Accounts: Consider a review of generic privileged accounts to determine if these accounts can be replaced by individual user accounts.	N/A	<p>Assessed the review of generic privileged accounts performed by POL management for both POL and third party users.</p> <p>Due to the completion of this recommendation part way through the year, IA&RM assessed the review of privileged POLSAP activity at the ISMF from April 2012 to February 2013.</p> <p>Reviewed the minutes from the November POL Risk & Compliance Committee.</p>	<p>POL management have confirmed that privileged generic accounts are controlled and will not be replaced with individual accounts.</p> <p>The risks associated with this decision were accepted by the POL Risk & Compliance Committee in November 2012.</p>	
12 Password Parameters: Review the Royal Mail Group (RMG) security policy to ensure it meets recommended password settings and consider having one single policy document for password guidelines for both POLSAP and Horizon.	N/A	<p>Reviewed the password policy covering POL and third party users and reviewed the recommendation status.</p> <p>Reviewed the minutes from the November POL Risk & Compliance Committee.</p>	<p>Separate security policies were maintained for POLSAP and Horizon, which were assessed and updated during periodic management reviews.</p> <p>The risks of having two separate policies rather than one joint policy as recommended by E&Y were accepted by the POL R&CC in November 2012.</p>	

Summary Findings (continued)

E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
13 Password parameters - Configure all network, application and supporting infrastructure components in line with the policy.	Q1 2013/14	Reviewed the RSPARAM report from POLSAP to inspect password parameters that had been configured on the system.	The password parameter for account lockout (rdisp/gui_auto_logout) is configured to 3,600 seconds (60 minutes). The recommended setting from E&Y was 1,800 seconds (30 minutes).	

Agreed Actions

User Administration

1. Implement a control to monitor Cash Centre users with privileged access to the system, to include access to POLSAP transaction code SU01. **Priority 2 (March 2013 – Completed)**

Change Management

2. Complete the POLSAP change management policy, ensure that it reflects the existing process, and obtain senior management approval before communicating this to key system users. **Priority 2 (March 2013 – Andy J Jones)**
3. Assign an appropriate manager to be responsible for the end-to-end POLSAP change management process for all functional and role changes within the system. **Priority 2 (Completed)**

Change Management

4. Review the requirement to strengthen the automatic password lockout controls and initiate changes as necessary. **Priority 2 (March 2013 – Mark R Pearce)**

Importance	No. of		Implementation by Mar 13
	actions	Completed	
Priority 1	-	-	-
Priority 2	4	2	2

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