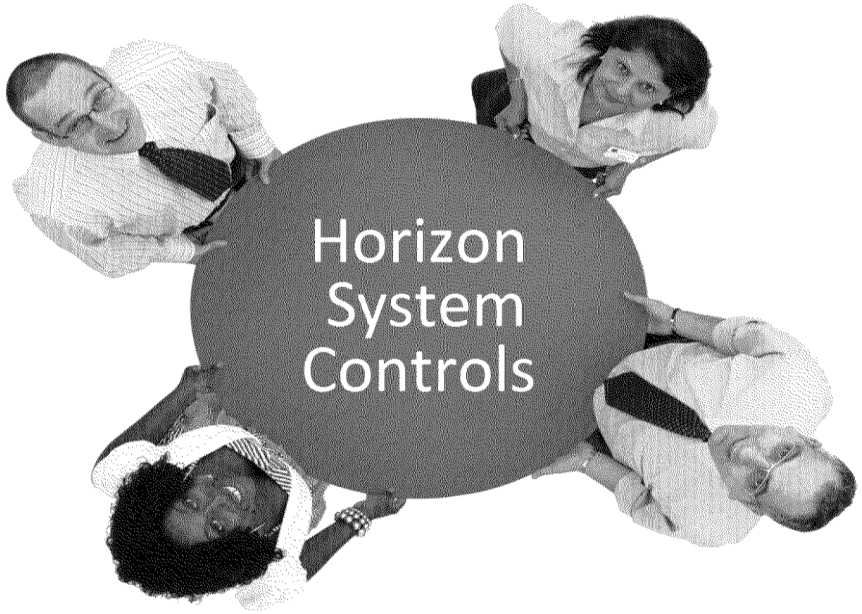
POL00029713



Follow Up Review of Key System Controls in Horizon

Post Office Limited

Assurance Review

December 2012

Report: AR12/050

POL00029713

Context and Objectives

The Post Office Limited (POL) network of some 11,000 branches processes client and business transactions in excess of £100 billion annually. The majority of transactions are conducted on behalf of other parties, for example, receiving payment for domestic utility bills and paying out National Savings. Customer transactions are captured through the Horizon electronic point of sale system in branches and transmitted to central systems (utility payment, external banking and POL finance systems) throughout the day.

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 Horizon control environment have been addressed by management. 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

The 2011/12 E&Y Management Letter identified a number of areas for improving Horizon system controls. This Internal Audit & Risk Management (IA&RM) review assessed the degree to which management action plans have progressed to address the issues which related to Horizon only. Overall, the majority of the areas for improvement identified by E&Y have been completed by POL and third party supplier management. There remain a few items that require further input from management to ensure that all controls have either been designed and implemented or that the risks have been accepted by POL, specifically:

1. **Generic privileged accounts:** Generic privileged accounts remain in use on Horizon by Fujitsu. A paper was presented to the November POL Risk and Compliance Committee where any residual business risks associated with this control were accepted by IT and Change on behalf of the business.

Implication: Accountability in the application may not be fully controlled, leading to a risk of inappropriate activities being undertaken within the system.

2. **Password parameters:** E&Y recommended that POL operate a single Information Security Policy, however POL management use two separate policies, one for Horizon and one for POLSAP respectively. Any residual business risks associated with this control were accepted by IT and Change on behalf of the business at the November POL Risk and Compliance Committee meeting.

In addition, POL management have not completed the E&Y recommendation to review key password parameters, as these have not been defined. Testing also identified two password parameters configured in the Horizon application that did not comply with the Horizon Security Policy.

Implication: Unauthorised access may occur, leading to a risk of inappropriate activities being undertaken within the system.

POL00029713

Conclusion

Conclusion: POL management have made progress against the areas for improvement identified by E&Y. Where areas that have been improved had not been addressed from the beginning of the year testing has demonstrated that compensating controls have been in operation for the financial year starting in April 2012. There remain, as noted above, some areas where POL management should either accept the risk of not implementing the E&Y recommendations in full, or where further work is required to strengthen the control environment. The findings, summarised on pages 4 – 8 have been shared with E&Y and reflect the IA&RM assessment as at the end of November 2012.

Control Environment Rating: Recommended Actions Partially Implemented.

Management Comment

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**

POL00029713

IT Management Disciplines and Transaction Controls Summary Findings

The summary findings from the review are noted below and represent the status of controls at 30th November 2012. Testing has been 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 1st April 2012.

	E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
1	**Change management -** Retain documentation to show the evidence that POL has been involved in authorisation, testing and approval of changes. In particular document evidence from 3rd party suppliers.	1st April 2012	Inspected the testing and release management processes and performed walkthroughs and sample testing of completed changes on Horizon.	Documentation for the change management procedure was in place for a sample of changes tested from 1st April to 30th November 2012. Controls were found to be operating effectively.	
2	**Generic privileged accounts** - Consider a review of generic privileged accounts to determine if these accounts can be replaced by individual user accounts.	Nov 2012	Inspected the review of generic privileged accounts performed by POL management for both POL and third party users. Due to the completion of this recommendation part way through the year, inspected the review of privileged Horizon activity at the Information Security Management Forum (ISMF) from 1st April to 2nd November 2012.	Through consultation with Fujitsu, POL management have confirmed that privileged generic accounts are controlled and will not be replaced with individual accounts. The residual business risk associated with this control was accepted by IT and Change at the November POL Risk & Compliance Committee on behalf of the business.	
3	**Generic privileged accounts** - Consider monitoring controls to help ensure robust security practices are in place, particularly those operated by third party service providers.	Nov 2012		A review of generic privileged accounts on a monthly basis, including those operated by third parties, commenced in November 2012 at the ISMF. Accounts with privileged access in the application have been reviewed at the ISMF since April 2012 and consequently mitigating controls were found to have been operating effectively since the start of the financial year.	

POL00029713

IT Management Disciplines and Transaction Controls Summary Findings (cont)

	E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
4	**Logical security settings** – Set an encrypted password for the LISTENER.ORA file on all Oracle databases supporting Horizon.	1st April 2012	Inspected the password policy for the LISTENER.ORA file and reviewed the recommendation status.	All Oracle databases supporting Horizon were upgraded to Oracle version 10gR2 prior to April 2012. This upgrade enabled the encryption of passwords on this file.	
5	**Logical Security Settings -** Consider monitoring controls to help ensure robust security settings are in place, particularly those operated by third party service providers.	N/A	Inspected the review of privileged Horizon activity at the ISMF from 1st April to 2nd November 2012. Tested the recommendation status with POL and Fujitsu management.	POL management confirmed that key password parameters will be reviewed on an annual basis. Presently, a review of key password parameters on the Horizon application has not been performed. Password parameters on Windows Active Directory were mainly found to meet those defined in the Horizon Security Policy. However two exceptions were noted and are listed in Appendix A.	
6	**Password Parameters -** Review and update the 'RMG Information Security Policy' to meet the recommended generally-accepted practice password settings outlined below. Management should also consider having only one policy document outlining the password guidelines that apply to both Horizon and POLSAP.	N/A	Inspected the password policy covering Horizon used by POL users and third party users and reviewed the recommendation status.	POL management have presented a requirement to have one security policy covering Horizon and another covering another application, POLSAP. Security policies are maintained and reviewed through periodic reviews and POL management confirmed the appropriateness of the security policies during this review. The residual business risk associated with this control was accepted by IT and Change at the November POL Risk & Compliance Committee.	

POL00029713

IT Management Disciplines and Transaction Controls Summary Findings (cont)

	E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
7	**Password Parameters -** Configure all network, application and supporting infrastructure components in line with the policy requirements. For infrastructure supporting the applications in scope, where the critical authentication level is at the POLSAP application layer or Active Directory, management should consider the risk of unauthorised access to the financial data by privileged accounts on the Oracle database and Linux operating system.	N/A	Inspected password parameters for the Oracle, Linux and Windows environments supporting the Horizon application used by POL and third party users and reviewed the E&Y recommendation status.	Password parameters are set in the Windows Active Directory Group Policy. The Group Policy overrides password configurations on the local Oracle and Linux systems that make up the Horizon environment. Password parameters on Windows Active Directory were mainly found to meet those defined in the Horizon Security Policy. However two exceptions were noted and are listed in Appendix A. Passwords for privileged accounts on the Oracle database and Linux operating systems conform with the Horizon Security Policy and are restricted to a small number of system administrators in Belfast. Passwords are enforced manually in line with the Horizon Security Policy. However the process for manually changing privileged passwords on the Oracle and Linux operating systems needs to be documented within the policy.	

POL00029713

IT Management Disciplines and Transaction Controls Summary Findings (cont)

	E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
8	**Password Parameters** - Management should consider implementing monitoring controls to help ensure robust security settings are in place, particularly those operated by third party service providers.	N/A	Inspected the review of privileged Horizon activity at the ISMF from 1st April to 2nd November 2012 and reviewed the recommendation status with POL and Fujitsu management.	POL management confirmed that key password parameters will be reviewed on an annual basis. Presently, a review of key password parameters on the Horizon application has not been performed. Password parameters on Windows Active Directory were mainly found to meet those defined in the Horizon Security Policy. However two exceptions were noted and are listed in Appendix A.	
9	**Periodic User Access Reviews and Monitoring Controls** - Consider a POL owned periodic review of appropriateness of access to in-scope applications and their supporting infrastructure. The implementation of this review will assist in the identification of inappropriate access and potential segregation of duties conflicts. In addition, this will act as an additional control to help detect users that no longer require access to the financial applications.	Nov 2012	Inspected 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 1st April to 2nd November 2012.	A review of privileged and generic user accounts on the Horizon application was carried out in October 2012 and was signed off on 8th November at the ISMF as completed. Accounts with privileged access in the application have been reviewed at the ISMF since April 2012 and consequently mitigating controls were found to have been operating effectively since the start of the financial year.	

POL00029713

IT Management Disciplines and Transaction Controls Summary Findings (cont)

	E&Y Recommendation Summary	Remediation date	What was done	What was found	Rating
10	**User Administration** - Strengthen the existing user administration processes within Fujitsu so that documentation supporting the request, approval and set-up of access to the Horizon estate is retained.	1st April 2012	Inspected user administration arrangements for new and modified Fujitsu technical support staff.	Documentation for the user administration procedure for new and modified access on the Horizon application was in place for a sample of Fujitsu technical support staff tested from 1st April to 30th November 2012. Controls were found to be operating effectively.	
11	**User Administration Process** - Strengthen the revocation of access process such that IT is notified in a timely manner when a terminated employee no longer requires access to the Horizon estate. Consideration should be given to the HR department sending a list of terminated employees to the IT department on a periodic basis, e.g. weekly or fortnightly. This is in addition to the line manager notifying the IT department of the terminated employee. All documentation supporting this process should be retained.	1st April 2012	Inspected user administration arrangements for Fujitsu technical support staff.	Documentation for the user administration procedure for leavers on the Horizon application was in place for a sample of Fujitsu technical support staff tested from 1st April to 30th November 2012. Fujitsu administrators were notified on a timely basis and user accounts were removed on or before the leave date on the request. Controls were found to be operating effectively.	

POL00029713

What is Being Done

The following actions have been agreed with management against the observations made in this report.

Generic privileged accounts

1. Management should set out the reasons for having generic privileged accounts on Horizon and present this to the Risk & Compliance Committee for review. **Priority 2 (Andy Jones - Completed)**

Password parameters

2. Management should set out the reasons for operating two Information Security Policies, covering Horizon and POLSAP, and present this to the Risk & Compliance Committee for review. **Priority 2 (Andy Jones - Completed)**

3. Ensure that the Horizon Security Policy is reviewed and changed to reflect the configuration of the password parameters detailed within Appendix A. **Priority 2 (Mark Pearce – January 2013)**

4. Ensure that the process for manually changing privileged account passwords on the Oracle databases and Linux operating systems is documented within the Horizon Security Policy. **Priority 2 (Mark Pearce – January 2013)**

5. Define key password parameters to be reviewed on a periodic basis. Once defined, management should perform a review of key password parameters to ensure that the third party supplier is implementing the Horizon Security Policy. **Priority 2 (Mark Pearce – January 2013)**

Importance	No of actions	Implementation Completed	Implementation by Mar 13
Priority 1	-	-	-
Priority 2	5	2	3

POL00029713

Appendix A – Windows Active Directory – Password Parameters

The following password parameters in the Windows Active Directory Group Policy were observed to not meet the requirements set out in the Horizon Security Policy.

	Password parameter	Horizon Security Policy Requirement	Windows Active Directory Group Policy Setting
1	Number of failed login attempts before account lockout	After 3 to 5 failed attempts	After 6 failed attempts
2	Account lockout counter	Reset by an Administrator	30 minutes

Fujitsu have stated that they do not have the resource available to have the account lockout counter reset by an administrator, which is why it automatically resets after 30 minutes. The Horizon Security Policy should be reviewed and changed to reflect the configuration of the password parameters detailed above.

POL00029713

Circulation List

Susan Barton, Strategy Director
Susan Crichton, Legal and Compliance Director
Christopher Day, Chief Financial Officer
Kevin Gilliand, 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
Justin Thornton, Head of Risk and Assurance
Ernst & Young, External Auditors