POL00380823

Follow Up Review of Key System Controls in Horizon

Post Office Limited

Assurance Review

Report: AR12/050a

May 2013

Internal Audit & Risk Management

Context and Objectives

The Post Office Limited (POL) network consists of approximately 11,000 branches which process 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.

This assignment is part of a comprehensive review of all agreed recommendations raised by Internal Audit & Risk Management throughout 2012/13 and has been agreed with the POL Audit & Risk Committee as part of the 2013/14 audit plan. This is to ascertain which items are still outstanding as the POL Internal Audit Team takes over with effect from 1 July 2013. The specific objective of our review was to assess the degree to which the five recommended actions raised in our December 2012 'Review of Key System Controls in Horizon' (report reference AR12/050) have been implemented.

Key Findings and Conclusion

Two of the five recommended actions have been implemented, or the risk of not implementing the recommendation has been accepted by the POL Risk & Compliance Committee. Management have commenced discussions with Fujitsu to address the remaining three recommendations which had a January 2013 target completion date. At the time of our review these discussions are ongoing and as such the recommendations have not yet been fully implemented. Management expect to have implemented these actions by 31 July 2013, the reason for the delayed implementation is that management are reliant on Fujitsu actioning the actual recommendations. These three actions relate to password parameters, specifically:

Password parameters:

1. To fully align the Horizon Security Policy (the 'Community Information Security Policy' (CISP) with Fujitsu) with the Windows AD password parameters in place;

2. To work with Fujitsu to ensure that the process for manually changing privileged account passwords on the Oracle databases and Linux operating systems is documented within the CISP; and

3. To continue discussion with Fujitsu to define key password parameters which should then be reviewed on a periodic basis.

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

POL00380823

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		Planned Remediation date	Work Performed	Findings	Rating
1	Management should set out the reasons for having generic privileged accounts on Horizon and present this to the Risk & Compliance Committee ('R&CC') for review. Priority 2 **Andy Jones**	Nov 2012	We reviewed the R&CC meeting minutes from 26 November 2012 to confirm the status of the action to review generic privileged accounts by the R&CC. We also reviewed Paper Fourteen - EY Management Letter Update RCC Nov 12 v2 Appendix B and observed specific reference to the acceptance of the risk of generic privileged accounts on Horizon.	The evidence reviewed confirmed that the risk associated with the use of generic privileged accounts was considered, and accepted, by the R&CC during the meeting which took place on 26 November 2012. **Complete**	■
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**	Nov 2012	We reviewed the R&CC meeting minutes from 26 November 2012 to confirm the status of the action to review the use of two Information Security Policies by the R&CC. We also reviewed Paper Fourteen - EY Management Letter Update RCC Nov 12 v2 Appendix B.	The evidence reviewed confirmed that the R&CC were satisfied that the current use of two Information Security Policies, one for Horizon and one for POLSAP, was acceptable, and hence no further action was required. **Complete**	■
3	Ensure that the CISP is reviewed and changed to reflect the configuration of the password parameters detailed within Appendix A of report AR12/050. Priority 2 **Mark Pearce**	Jan 2013	We reviewed the CISP with Fujitsu on screen with Mark Pearce to confirm whether it had been updated as per the recommended action.	The CISP with Fujitsu remains inconsistent with the implemented Windows AD policy which controls Horizon logical access parameters. The Windows AD parameters currently utilised result in access lockout after 6 failed attempts, whereas the CISP refers to a lockout after 3 failed attempts. **Ongoing - Target date July 2013**	▨

Summary Findings (continued)

	Recommended Action	Planned Remediation date	Work Performed	Findings	Rating
4	Ensure that the process for manually changing privileged account passwords on the Oracle databases and Linux operating systems is documented within the CISP. Priority 2 **Mark Pearce**	Jan 2013	Update obtained through discussion with Mark Pearce.	The process for manually changing privileged account password on Oracle and Linux is not yet documented within the CISP, although the process of engaging with Fujitsu to implement this amendment is underway. **Ongoing - Target date July 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 CISP. Priority 2 **Mark Pearce**	Jan 2013	Update obtained through discussion with Mark Pearce.	A definition of password parameters to be reviewed on a periodic basis is currently under discussion with Fujitsu. Once identified, a process will be implemented to review these parameters on a periodic basis. **Ongoing - Target date July 2013**	▨

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

POL00380823

Agreed Actions

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

Password parameters

1. Continue discussion with Fujitsu and other stakeholders regarding aligning the relevant CISP "number of failed attempts before account lockout" parameter (3 attempts) with the actual Windows AD policy implemented (6 attempts). **(July 2013 – Mark Pearce) – Priority 2**

2. Continue discussion with Fujitsu to ensure that the process for manually changing privileged account passwords on the Oracle databases and Linux operating systems is documented within the CISP. **(July 2013 – Mark Pearce) – Priority 2**

3. Continue discussion with Fujitsu to 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 CISP. **(July 2013 – Mark Pearce) – Priority 2**

Circulation List

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
Julie George, Head of Information Security

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