POL00397899

Confidential

POST OFFICE LTD – Risk & Compliance Committee

2011/12 IT annual audit update

1. Purpose

The purpose of this paper is to:

1.1 Update the committee on the IT audit rectification plan from the 2011/12 Ernst & Young audit.

1.2 Request endorsement from the committee of a number of observations that Post Office have mitigated against or where Post Office IT suggest Post Office accept the risk

2. Background

2.1 The 2011/12 IT audit identified seven areas that required either: actions to rectify them, to mitigate against them, or for Post Office to accept the risk against them. These seven areas were further broken into 22 specific actions based on the observations and allocated across Post Office and our suppliers to rectify.

2.2 The scope of the IT audit was based on the controls adopted for HNG and POLSAP

2.3 As a further step to determine the success of the remedial actions an independent review by Deloitte was commissioned by IA&RM of the actions related to POLSAP which has provided assurance that the controls implemented are effective. A similar audit of the HNG actions is currently underway and due to complete at the end of November 2012.

2.4 A further audit of actions still underway at the time of this paper has been requested of IA&RM currently planned for January 2013.

3. Actions Update

3.1 Of the 22 actions issued in last year's audit, 12 are complete in full (see annex A).

3.2 The outstanding actions require the R&CC to sign-off the mitigating actions or to accept the risk. These are detailed in annex B and summarised below:

3.2.1 Privileged access: Post Office was asked to consider various improvements to the management of privileged access accounts. This

POL00397899

access is required by the IT suppliers to operate the systems. Post Office believes the controls in place are adequate to mitigate the risk of unauthorized changes, they are:
1. Post Office reviews all privilege access requests.
2. Usage is monitored and reviewed.
3. Changes to IDs are reported immediately to the Post Office.
4. Periodic reviews take place to re-approve all such IDs.

3.2.2 Employment Termination: Post Office was asked to consider strengthening the revocation of system access after employment termination. The Post Office has reviewed the process and believes it is appropriate.

3.2.3 Administrator Password: Post Office was asked to consider changing the Administrator account to one with a stronger password. Post Office does not believe this necessary as the current password is set to the supplier's corporate standard which meets the Post Office standard.

3.2.4 Review Password Policy: Post Office was asked to review password policy and consider unifying HNG and POLSAP password standards. Post Office confirms that HNG and POLSAP security policies have been reviewed and are appropriate for the respective systems. Policy standards will be kept up-to-date through periodic reviews.

3.2.5 Network and Infrastructure Passwords: Post Office was asked to consider configuring network and infrastructure passwords in line with the Post Office security policy – as some are configured to the policies of third party system suppliers and reflect system restrictions. Post Office has considered this and will implement this going forward as new infrastructure is implemented. Post Office believes that it is acceptable for existing infrastructure passwords to continue to comply with the policies of the third party system suppliers.

The committee is asked to 'endorse' IT's acceptance of the risks and remaining actions.

4. Conclusion

The observations identified through the E&Y audit have either been completed, mitigated or we accept the risk. On acceptance of the mitigated and accepted risks and confirmation that those complete are acceptably closed and independently assessed, we look to sign off that all the actions raised against the IT audit 2011/12 are concluded.

5. Recommendations

The Board is asked to:

5.1 Endorse IT's acceptance of the mitigated and accepted risks

5.2 Confirm conclusion of the completed action's

Andy Jones
20 November 2012

POL00397899

Confidential

Appendix A

Completed actions from the E&Y report
(Note: numbers in brackets are the Post Office reference number)

Area	Observation	IA&RM comment from the POLSAP audit @ end September 2012	Current Status
Privileged Access	Conduct a review of privileged access to determine if the level of privilege is appropriate (1)	An annual review of user access will be performed in Q3 FY13. As this has not yet been performed the issue remains outstanding.	Complete. This review has now been completed and fully documented
Privileged Access	Implement monitoring controls to ensure 3rd party controls are in place and in operation. (POLSAP, Cash centres) (5)	Monitoring controls have been implemented over third parties. Further work is required to ensure that the scope of such reviews is approved by POL management and that these reviews are formally documented.	Complete. The scope of these reviews is agreed and approved by Post Office and formally documented
Privileged Access	Conduct a periodic review of activities executed by accounts granted permanent SAP_ALL and SAP_NEW access. (4)	Monitoring controls have been implemented for SAP_ALL and SAP_NEW privileges and follow up activity is undertaken with the third parties.	Complete at time of the IA&RM audit
Generic privileged access	Consider implementing monitoring controls to ensure that robust security practices are in place (15)	N/A for the POLSAP audit as related to HNG	Complete and forms part of the Information Management Security Forum
Periodic User Access reviews and monitoring controls	Implement a Post Office owned periodic review of appropriateness to determine if there is any inappropriate access (13)	An annual review of user access will be performed in Q3 FY13. As this has not yet been performed the issue remains outstanding.	Complete. This review has now been completed and fully documented
User Admin Process	Strengthen the process so that documentation supporting the request is retained. (HNG, Fujitsu) (6)	Although work has been undertaken to strengthen these controls, sample testing identified that documentation for one request sampled was completed incorrectly.	Complete. The controls were strengthened but one sample was discovered in the audit as not correctly documented as approved.
User Admin Process	Strengthen the process so that documentation supporting the request is retained. (7a)	Although work has been undertaken to strengthen these controls, sample testing identified that documentation for one request sampled was completed incorrectly.	Complete. Documentation is retained.

POL00397899

Confidential

User Admin Process	Strengthen the process so that the standardised process is followed. (7b)	Although work has been undertaken to strengthen these controls, sample testing identified that documentation for one request sampled was completed incorrectly.	Complete. The controls were strengthened but one sample was discovered in the audit as not correctly documented as approved.
User Admin Process	Implement monitoring controls around the activities of privileged users where the process is controlled by 3rd party suppliers. (8)	Monitoring processes do not include a review of SU01 access.	Complete for all privileged users. The SU01 is a 'role' and not a user. However, IT will review the usage of this role going forward.
Change Management Process	Define the responsibilities of all parties involved in the authorisation, testing and approval of changes deployed into production. (11)	Although controls have been strengthened in this area, an issue was identified with one out of six changes sampled.	Complete. The controls were strengthened but one sample was discovered in the audit as not correctly documented as approved.
Change Management Process	Documentation to be retained to evidence the authorisation, testing and approval of changes made to the applications. (10)	Documentation for the change management procedure was in place.	Complete.
Change Management Process	Implement monitoring controls to ensure controls operated by 3rd party suppliers are in place and in operation. (Operational Change Process) (12)	POL need to define responsibility for the end-to-end change management process.	Complete. The change management policy has been written and is going through approval.

POL00397899

Confidential

Appendix B
Actions from the E&Y report that require R&CC endorsement
(Note: numbers in brackets are the Post Office reference number)

Risk	E&Y Action	Mitigation	Why acceptable
There is a risk that people make unauthorised changes to the systems and affect our data integrity.	Revisit the need to grant the level of privileged access through SAP_ALL and SAP_NEW profiles (2) Consider creating system accounts to run scheduled jobs so manual login is not allowed where privileged access to POLSAP accounts are used (3) Consider a review of generic privileged accounts and determine if these can be replaced with individual user accounts (14)	**Mitigated Risk** • The supplier along with the Post Office initially 'approves' the user as authorised and then on an on-going basis (monthly) reviews the users. • All usage is monitored by the supplier and the Post Office monitors this usage monthly through reports. • All user ID changes are reported to the Post Office immediately and Post Office review these monthly at the Information Security Management Forum. • Semi-annually the Post Office re-approves all ID's and this was completed this November. All of these are auditable. • To date no inappropriate activity has been noted.	• IT suppliers require this level of access to run the system and this is not unique to the Post Office solution. • Unauthorised changes will be detected through monitoring • In November Post Office reviewed all users.
There is a risk that users may remain live on the system as a 'user' after they have terminated their employment with the supplier or move away from the Post Office account.	Strengthen the revocation of access process such that IT is notified timely when a terminated employee no longer requires access. Perhaps through a periodic report from HR to IT for validation (9)	**Accepted Risk.** • There is a documented process within Fujitsu that details the process for adding, deleting, removing and modifying users within the Post Office account. • This process has been reviewed by Post Office information security forum members as part of this audit and deemed appropriate. • The supplier Operational Security team have processes in place through this document that ensure individuals are removed from the directory as they leave. • To gain assurance the leaver numbers are reported to Post Office monthly • To strengthen this Post Office will receive	• This process has been reviewed by Post Office information security forum members as part of this audit and deemed appropriate. • Through the last audit there was one incident that was identified through the sample where a leaver was not removed from the directory in a timely fashion. This user did not access the system following their leaving. • Post Office deems that the existing revocation process and the level of control is

POL00397899

Confidential

		data with ID's going forward.	appropriate based on this single deviation. We will monitor the situation and should the status change we will act on that accordingly.
There is a risk that the existing password for the default administrator account is not strong enough	Disable the default Administrator Account and replace with an Administrator Account with a stronger password (20)	**Accepted Risk.** • The current password is set in line with the Fujitsu corporate policy the standards of which are stronger than the requirements agreed with Post Office	• Considered with the supplier replacing the Admin Account and including a stronger password but not required as the current password is set to Fujitsu corporate and not the Post Office Account policy standards which is stronger.
There is a risk that access could be made to the LISTNER.ORA file, which checks for inappropriate activity and the potential for changes made to its integrity.	Assess the setting of an encrypted password for the LISTENER.ORA file on all Oracle databases (19a) Set the encrypted password for the LISTENER.ORA file on all Oracle databases (19b)	**Mitigated Risk.** • This observation was assessed and was mitigated through the upgrade of all Oracle databases to version 10gR2. This upgrade enabled the encryption of passwords on this file.	• Redundant as an action as mitigated through the upgrade of the Oracle databases
There is a risk that certain password parameters have not been defined	Review and update the 'RMG security policy' to meet generally accepted password settings and consider having one policy outlining the password guidelines for HNG and POLSAP (16)	**Accept the Risk.** • Post Office has two security policies, one for HNG and one for POLSAP as these are two functionally separate systems. • These policies are periodically reviewed and updated as appropriate. • Post Office does not own the RMG security policy and therefore cannot amend it.	• The two security policies within Post Office for HNG and POLSAP are maintained and up-to-date through periodic reviews. • Additionally the PCI audit, report completed 31st July 2012, reviewed and acknowledged that the password strengths were appropriate.
There is a risk that the network and infrastructure passwords have not been configured in	Configure all network and infrastructure in line with the security policy (17) Consider implementing monitoring controls to ensure that robust security	**Mitigated Risk.** • The network and infrastructure system passwords may not be set to the standards defined in the policies because in certain areas of the system, passwords are defined	• All new architecture design takes into account the required security policies and signs off its design. • Existing network and

POL00397899

Confidential

line with the policies	settings are in place (18)	by third party suppliers e.g. Oracle, and do not match the 'generally' accepted password parameters. These are system restrictions.	infrastructure passwords may be set to third party system standards but these are consistent with that provider needs. • This will be reviewed as part of any future HNG upgrade