POL00143065

Post Office Ltd – Strictly Confidential

POL()

POST OFFICE LTD
Briefing for Paula Vennells (Chief Executive) and Chris Day (Chief Financial Officer)

Post Office IT General Controls
Ernst & Young Audit 2011/12

1. Purpose

The purpose of this paper is to provide an update on the:

1.1 Progress made in addressing the observations from the 2010/11 IT General Controls Audit.
1.2 Implementation of a SAS70 (ISAE3402) style report.
1.2 Observations arising from the 2011/12 audit and the proposed Management Response.

2. Background

2.1 As part of the annual independent Financial Audit, Ernst & Young undertake an audit of the core Post Office systems that support financial transactions, namely:

- Within the Post Office domain hosted by Fujitsu
  - HNGX (product sales platform)
  - POLSAP (product and branch accounting and supply chain / stock management)
- Within the Royal Mail domain hosted by CSC
  - SAP HR (human resources)
  - SAP ESFS (general ledger)

2.2 The focus of the IT General Controls audit for each of these systems covers:

- Change Management
  - Only appropriately authorised, tested, and approved changes are made to applications, interfaces, databases, and operating systems.
- Logical Access
  - Only authorised persons have access to data and applications (including programs, tables, and related resources) and that they can perform only specifically authorised functions (e.g., inquire, execute, update).
- Operations
  - Data supporting financial information is properly backed up so such data can be accurately and completely recovered if there is a system outage or data integrity issue.
  - Programs are executed as planned and deviations from scheduled processing are identified and resolved in a timely manner.
  - IT Operations problems or incidents are identified, resolved, reviewed, and analysed in a timely manner.

2.3 The 2010/11 audit resulted in a number of actions for Post Office and Fujitsu to address which were concluded by October 2011. The implementation of

POL00143065

these actions has resulted in significant changes to our processes and to deliver improvements to our IT General Controls.

2.4 Given the timing of this year's audit (January and February 2012), there was some time for these changes to have embedded. The improvements are evidenced in the findings of the 2011/12 audit where there are no high risk observations within the 7 identified (versus 10 last year) and only 25 specific recommendations (versus over 70 last year).

3. Summary of the 2010/11 audit position

3.1 The 2010/11 audit identified 10 observations (classified as 4 high risk, 3 medium and 3 low) with over 70 specific recommendations.

3.2 In response to these observations, Post Office and Fujitsu agreed a series of actions (as identified in the Management Comments to the audit report for 2010/11) to address the areas of risk identified.

3.3 A Post Office led Audit Steering Group was established to track and manage the agreed actions, with all being completed by the end of October 2011, as planned.

3.4 Through an independent Royal Mail Group audit conducted on the Post Office systems (November 2011), it was agreed that all actions had been completed as planned. Two actions had minor activities still to be completed, which were addressed by December 2011. (See Appendix A for a summary statement for each of the 2010/11 observations as agreed with the RMG audit.)

4. Update on the SAS70 (ISAE3402) style report implementation

4.1 One specific recommendation from the 2010/11 audit was to investigate the feasibility of having a SAS70 style report produced annually (now known as ISAE3402), with a view to establishing greater standardised controls and continuously evidenced compliance. Post Office have worked with Fujitsu and Ernst & Young to agree an initial way forward where Fujitsu will, at their own cost, engage Ernst & Young to produce such a report for the Fujitsu hosted Post Office systems within the scope of our annual IT General Controls audit.

4.2 The Fujitsu ISAE3402 report will be introduced for FY2012/13. It will bring benefits to both Fujitsu and Post Office. Whilst initially Fujitsu will still require the same level of effort to support the ISAE3402 audit, over time the scope of that audit will be expanded to cover other standards (e.g. ISO27001, PCI, LiNK). This results in economies for Fujitsu as only one audit is required for all those controls that are common across all standards. As the adoption of the annual ISAE3402 report embeds, the good practice of continuous evidencing of compliance will also deliver efficiencies, with each subsequent annual audit having more immediate access to evidence of control.

4.3 Post Office will also benefit with the introduction of Fujitsu's ISAE3402 report. With the initial scope covering the controls within the annual IT General Controls audit, our auditors will be able to draw on the ISAE3402 report as a trusted source of evidence. Where control is evidenced in that report, reduced investigation will be required by our auditors, with resulting efficiencies.

POL00143065

4.4 In addition, Post Office IT & Change and Information Security functions are jointly aiming to adopt ISAE3402 good practices to establish a single audit framework to manage how Post Office maintains compliance with the controls across all required standards. This single audit framework will not only drive efficiencies for Post Office, similar to the benefits identified above, it will also drive improvements in the adoption of our policies and processes through the requirement for continuous evidencing of compliance.

5. Update on the 2011/12 audit

5.1 Building on lessons learned from the 2010/11 audit, a more rigorous management control approach was adopted for the 2011/12 audit. This involved clear planning and communication to all parties well in advance of required involvement. As a result the 2011/12 audit operated with a high degree of cooperation across all parties and delivered on time. This is in contrast to 2010/11 that required substantial senior management intervention and delivered 3 months later than planned.

5.2 The 2011/12 audit found a demonstrable improvement from the 2010/11 audit across all previous observations and no high risk observations were identified.

5.3 A total of 7 observations have been identified this year with only 25 specific recommendations. Each of these observations built on the findings of the 2010/11 audit with Ernst & Young recommending further areas for improvement or repeated recommendations where similar weaknesses persist.

5.4 The proposed 2011/12 Management Response identifies how the agreed actions from last year's audit sought to address any repeated weaknesses. In addition, the responses identify where repeated weaknesses persist due to legacy constraints, with policy and process being used to mitigate any potential risks.

5.5 This year's responses also identify what further immediate actions will be taken, e.g. re-iteration and communication of policy. In addition, new reviews of policy and process are to take place to identify appropriate further improvements.

5.6 A summary of this year's Ernst & Young recommendations and related responses can be found in Appendix B.

5.7 Post Office Audit Steering Group will track and manage the progress of these actions and report to the Post Office Audit Committee to agree each course of action proposed, timeframes required and evidence completion of agreed actions.

6. Recommendations

6.1 This paper is provided as a briefing paper only.

Lesley Sewell
Chief Information Officer
May 2012

POL00143065

Appendix A Summary status of the 2010/11 audit observations – as agreed with the RMG independent audit in November 2011.

Finding	E&Y Rating	Summary	Status
1	High	**Governance of outsourcing arrangement with Fujitsu:** POL is responsible for the governance and risk and control frameworks and should have visibility and assurance over their design and operating effectiveness.	
2	High	**Segregation of change management duties:** Inappropriate access should be revoked and roles for development and migration to live environment should be segregated.	
3	High	**Change management process:** All changes should be appropriately authorised, tested and approved prior to deployment to live environment.	
4	High	**Privileged access:** Privileged access to IT functions should be reviewed to determine whether it is appropriate.	
5	Med	**Periodic POL-owned review of user accounts:** To assist in the identification of inappropriate access and potential segregation of duties conflicts.	
6	Med	**User administration:** Review the current user access policy and strengthen the existing user administration process within POL and third party service providers.	
7	Low	**Infrastructure logical security settings:** Undertake architectural review and periodic scan of passwords as part of a penetration testing schedule.	
8	Low	**Password parameters:** Review and update Information security policy and configure all applications in line with policy requirements.	
9	Med	**Access to generic privileged accounts:** Review across all applications. Consider replacing with individual accounts and implement monitoring controls.	
10	Low	**Incident identification and resolution:** Regular review of the problem and incident management process to ensure incidents are identified, classified and resolved on a timely basis.	

POL00143065

Appendix B Summary of 2011/12 Ernst & Young audit recommendations and proposed Management Responses.

E&Y Recommendations	Summary of the proposed Post Office Management Response
1. Privileged Access. • Conduct a review of privileged access for in scope applications (HNG and SAP) • Revisit the need to grant access at SAP_ALL and SAP_NEW levels • Consider creating system accounts to run scheduled jobs for POLSAP • Periodic review of the activities where SAP_ALL and SAP_NEW are retained. • Implement monitoring controls for 3rd party suppliers.	• **Definition:** Privileged access describes the level of control where the user having this access can perform all or nearly all tasks within the system e.g. SAP_ALL provides the capability to process and approve financial transactions within a SAP system. The purpose of SAP_ALL is to enable qualified administration users the capability to maintain the system. • **Observations from last year:** Observations from the last audit identified inappropriate privilege access in HNGX and POLSAP. • **Observations this year:** This year repeats the same observations but notes a reduction in accounts assigned with privileged access in POLSAP and reviewed inappropriate privileged access in HNGX. • **What have we done to address the observations:** Since the last audit the use of privileged accounts is monitored so that the granting of this privilege must be justified, time bound and reviewed monthly by POL. There is continuing need for certain key system activities to be executed by the administration teams with these privileges'. For example, for out of hour's support it is not possible to predict the privileges required to resolve any incident, therefore the use of encompassing privileges is justified. Further additional controls do not appear to be justified. However the rigour of the monthly check at the ISMF (Information Security Management Forum) will be tested to ensure it is adequate. If not steps will be taken to optimise the checking of these accounts.

POL00143065

2. User Admin Process. • Strengthen the HNG user admin process to retain approval documentation for access to the HNG estate • Strengthen the POLSAP user admin process to retain approval documentation for temporary set up for cash centres. • Consider a monitoring process for temporary set up for cash centres. • Re-communicate to cash centre managers that the standard process should be followed for permanent access modifications for SAPADS. • Implement a monitoring process for privileged users within cash centres. • Where user admin is controlled by a 3rd party ensure adequate monitoring controls. • For HNG and POLSAP strengthen the process for revocation of access when employees contracts are	• **Definition:** This is the process for the creation, modification and removal of user's access to a system. In particular HNGX and POLSAP. • **Observations from last year:** Observations from the last audit identified the need to introduce the retention of user application documentation to record the user application request. For POLSAP to identify how the segregation of duties can be maintained and for HNGX Implement a standard user administration process to include all creations, modifications and removal of access to HNGX • **Observations this year:** This year repeats much of the same with additional focus on revocation of users who have left or moved on. • **What have we done to address the observations:** There is a good strong process in place and the observations seem to be driven from some lapses in documentation e.g. some individuals did not record their name on the retained documentation. Post Office will work with Fujitsu to ensure the process is re-iterated to the user population and will work with Fujitsu to ensure the joiners / leaver's process is robust. Similarly in POLSAP we will re-iterate the process to the user population and ensure the monitoring process for third party users is robust.

POL00143065

3. Change Management Process. • To enhance the change management process by retained evidence of authorisation, testing and approval to promote accountability. • Define the responsibilities of all parties involved. • Increase involvement in the change management process specifically for fixes and maintenance changes. • Describe the overall change management process within documentation. • Implement controls to ensure that 3rd party service providers are in place and in operation.	• **Definition:** This is the process that determines that all programme changes are appropriately authorised, tested and approved prior to implementation. • **Observations from last year:** The observations from last year centred on the authorisation and testing of changes prior to go live. Of the samples taken there were a number of observations where evidence of authorisations could not be found, evidence that testing took place or evidence that approval was not received. This was based on a sample of 18 changes in POLSAP and 15 in HNGX. • **Observations this year:** Observations were much the same but referred to instances where names were not recorded on the appropriate documentation. The auditors noted that there were improvements in the process. • **What have we done to address the observations:** Post Office has further improved the process regarding change management since the last audit. However, both Post Office and Fujitsu will amend their processes to ensure that the name of the individual authorising, testing or approving changes is recorded, as identified by the audit this year. It is noteworthy that Post Office does not always engage in the authorisation, testing and approval of maintenance changes or fixes as these are often BAU maintenance of the system and 19 of the 28 samples referred to maintenance or BAU changes. However, Post Office does validate and authorise security affecting changes such as patches and anti-virus updates and ensures that testing is performed by Fujitsu and retains an audit trail. Post Office will verify that the classification of maintenance and fix changes and responsibilities is adequately documented between POL and Fujitsu, and will update the documentation if it is found deficient. Post Office has a documented change process described in the Manage Improvement & Change document. All Post Office suppliers have their own internal change processes.

POL00143065

4. Periodic user access reviews and monitoring controls. • To consider the implementation of a periodic review of appropriate access for HNG and POLSAP.	• **Definition:** This regular process reviews whether a user has appropriate privileges' for the job / role that they undertake. • **Observations from last year:** Requested that Post Office should implement a periodic review of appropriate access of users. The findings found 2 users out of 25 had left the business and 1 user had inappropriate access. • **Observations this year:** This years observation repeated that a review process be implemented based on the findings that one individual had access to the HNGX estate that was no longer required to. • **What have we done to address the observations:** The processes that manage all user privileges have been further improved from last year. The Fujitsu joiners / leavers process is greatly improved and there is now a monthly review of all movers and inactive users are identified after a pre defined period of time. Annually there is a full review of the user access and Fujitsu report on a regular basis on the user access status to the Post Office Information Security Management Forum. These processes are considered sufficiently robust. Post Office in conjunction with Fujitsu will verify that adequate authorisation is identified and recorded and where not will take appropriate steps to remediate
5. Generic Privileged Accounts. • To consider a review of generic privileged accounts and supporting infrastructure to determine if they can be replaced by individual accounts. • To consider monitoring controls to help ensure robust security practices are in place, particularly 3rd party suppliers.	• **Definition:** A Generic privileged account describes a non user specific account which can perform all or nearly all tasks within the system e.g. SAP_ALL provides the capability to process and approve financial transactions within a SAP system. The purpose of SAP_ALL is to enable qualified administration users the capability to maintain the system. • **Observations from last year:** Observations from the last audit highlighted that a number of users e.g. 10 of 11 for system accounts 4 of 11 on database accounts etc., knew the password for specific accounts and asked that we consider replacing such accounts with individual specific owned accounts to promote accountability. • **Observations this year:** This year's observations repeated very much the same. • **What have we done to address the observations:** Since last year the processes that control access to accounts, where these are privileged, generic privileged or user accounts has been further improved. The improvements mean that the use of generic privileged or privileged accounts can be tracked back through an audit record to a particular person and authorisation for the use of the accounts and the defined period for which he account is used. This is monitored and reviewed by Fujitsu at least monthly. All accounts are reviewed at least annually and Fujitsu present reports to Post Office at the monthly Information Security Governance Forum.

POL00143065

6. Password parameters. • Review and update the 'RMG Security Policy' to meet the generally accepted password settings as described in the management letter. • Consider one single policy rather than multiple policies and guidelines. • Configure network, application and infrastructure components in line with the policy.	• **Definition:** Password parameters are attributes that can be applied to the way a password is generated by a system. And which may be forced on a user when selecting a password. For example the length of the password, the mix of characters, the length of time a password exists before it must be renewed etc. Different systems and applications can and do employ widely differing sets of attributes and do not necessarily agree on the value of these attributes. These then become technical constraints on setting and enforcing policy. • **Observations from last year:** Observations last year was to review the RMG security Policy and update the password settings accordingly for the network, application and supporting infrastructure components. Additionally the auditors recognised that the risk was mitigated by the level of controls in Active Directory and that this was considered to be a low risk. • **Observations this year:** The observations were much the same and they recognised that there had been improvements to the observations raised last year. • **What have we done to address the observations:**. The ability to align all of the technical password controls is significantly limited by the flexibility and range of options of password parameters provided by the manufacturers. Given that HNGX has a significant number of legacy systems, this drives a lot of differences that cannot be reconciled at all. However, as new systems are designed and brought on line and new applications developed these differences will gradually disappear. The main reason for this is that over time manufacturers have recognised the need for comprehensive and flexible options for security settings.
7. Logical Security Settings. • To consider specific encrypted password settings for all Oracle databases and disabling the default administrator account and creating a new one with a strong password. • To consider monitoring controls to help ensure robust security practices are in place, particularly 3rd party suppliers.	• **Definition:** Logical (as opposed to physical) security settings (or system security settings) is a generic term that can apply to any security parameter of a system or its supporting infrastructure. • **Observations from last year:** This was considered to be of low risk at the last audit. It considered that there were certain logical security weaknesses identified. Five observations were highlighted and three were implemented. Of the two remaining the operational impact of HNGX was considered a marginal improvement in the logical access risk. • **Observations this year:** Observations were much the same. • **What have we done to address the observations:** Last year's observation was to encrypt the LISTENER.ORA file. Fujitsu and Post Office considered that the impact of encrypting this file was a very marginal improvement to the logical access risk and a significant increase of the risk to the long term stability of the service. However, Post Office will request Fujitsu to assess the cost and operational impact of this change.

POL00143065