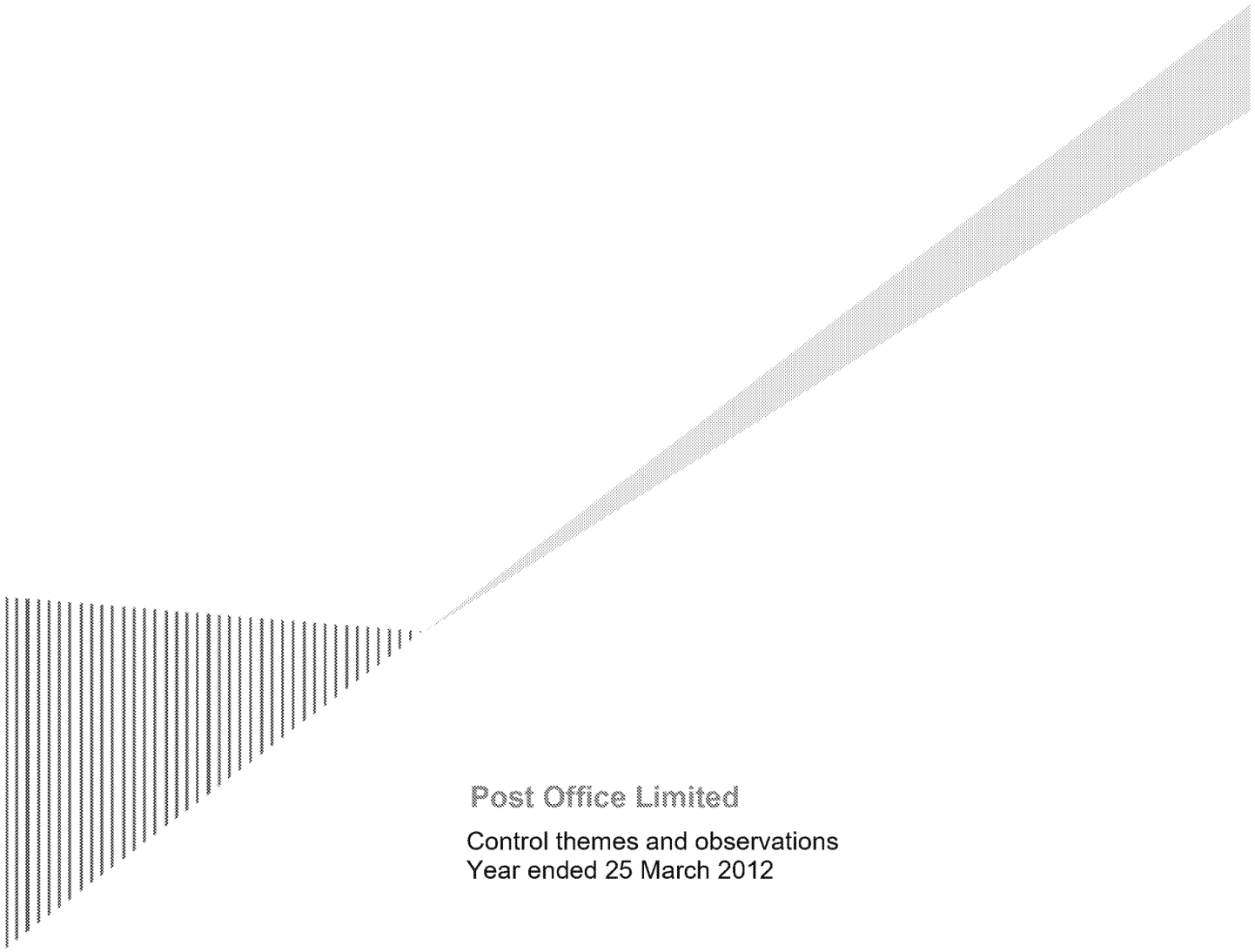
POL00143525



Post Office Limited

Control themes and observations
Year ended 25 March 2012

ERNST & YOUNG

POL00143525

POL00143525

Ernst & Young LLP
1 More London Place
London SE1 2AF

Tel: GRO
Fax: GRO
www.ey.com/uk

Private and confidential

Chris Day

Finance Director

Post Office Limited ("POL")

148 Old Street

London

EC1V 9NN

13 August 2012

Dear Chris

Control themes and observations from our 2012 audit

I am pleased to enclose the control themes and observations from our audit for the year ended 25 March 2012.

Our review of the company's systems of internal control is carried out to help us express an opinion on the financial statements of the company as a whole. This work is not primarily directed towards the discovery of weaknesses, the detection of fraud or other irregularities (other than those which would influence us in forming that opinion) and should not, therefore, be relied upon to show that no other weaknesses exist or areas require attention.

Accordingly, the matters reported below are limited to those matters that we identified during the audit and that we concluded are of sufficient importance to merit being reported to you. We would be happy to discuss any of the points contained within this letter in more detail with you.

We would also like to take this opportunity to thank management for their input into this process, and to thank you and your staff for assistance during the course of our audit.

Yours sincerely

Angus Grant
Partner, on behalf of Ernst & Young LLP
Enc

POL00143525

Contents

POL00143525

1. Executive Summary

Introduction

Consistent with the prior year, this report has been produced to draw out commentary and observations on a number of issues arising from our audit work which we consider to be of relevance to the business. Whilst our audit work is designed to support our formal audit opinions, this work produces other findings as well.

The finance leadership team at Post Office Limited ("POL") has continued its success in implementing process improvements across their finance and IT functions, despite having to deal with the challenges of separation-related activity at the same time. Focused management action has addressed many of the issues raised in our prior year management letter, with finance functions including payroll continuing to see improvements. Whilst there continue to be challenges in areas including POL's IT environment, management have taken steps to ensure these challenges are, and continue to be, addressed.

This report details these findings under the following sections:

- Current year observations for FY 2011-12; and
- An update on non-IT matters we raised in 2010-11

We have not separately provided an update to the prior year IT related matters given the similarity of findings and to avoid redundancy within this report.

We have shared these observations with the Company and management is reflecting on them in conjunction with other priorities in the business.

Summary of non-IT control observations

As mentioned in our Audit Committee Report presented to you in May 2012, we utilised a controls based approach in respect of the identified significant processes of revenue, purchasing, cash settlements and payroll. Our controls testing approach focuses on the controls implemented across the entire POL business, including the London head office, Bolton (payroll), Chesterfield (shared services), branches and cash centres. Whilst we test controls in London, Bolton and Chesterfield annually, we rotate our cash centre and branch visits every year. A summary of our findings were as follows:

- **Financial Statement Close Process:** Management continues to employ a robust system of internal controls around its financial reporting and financial statement close process. Despite the increase in separation-related activity by the finance team, we noticed no adverse impact on the quality of information produced. At all times through the audit process, there was early and timely resolution of accounting and technical issues as a result of regular interaction throughout the year between POL's finance team and ourselves, and this led to a smooth 'no surprises' financial statement close process.
- **Payroll Process:** We continued to see improvement in the payroll process during the current year, as management was able to successfully respond to our prior year management letter comments. The last two years have seen significant improvement as comments raised by us in previous years have now been addressed effectively by management.
- **Transactional, branch and cash centre process and controls:** For the revenue, purchasing and cash settlements processes, we note that the controls framework remains consistent with prior year with no significant findings from our testing.
- **Whilst we have raised observations and recommendations based** on the above processes in this report, these should be seen as refinements to the current process as opposed to significant control deficiencies.

POL00143525

Summary of IT Control Observations

As discussed in earlier communications, we continued to identify significant control weaknesses in POL's IT environment, which in our view, reflected a need for improvement on the part of the service provider Fujitsu and also a change in approach on the part of POL in terms of the governance, risk and control framework over its business critical systems. These weaknesses in the IT control environment, coupled with the lack of an ISAE3402 (formerly SAS70) report on Fujitsu's control environment contributed to a lengthy and inefficient audit process.

Improvements noted during the current year audit included the following areas:

- **High risk areas:** POL took action in the year to address the two highest risk areas we raised in our prior year letter being improvement of governance over outsourcing application management and improving segregation of duties within the manage change process.
- **Planning:** At an early stage in this audit cycle, Fujitsu, POL and EY took part in a workshop to consider the control framework for POL and agreed planning milestones and protocols.
- **People & commitment:** Lesley Sewell and her team's continued support and sponsorship, coupled with the commitment of Fujitsu set the tone for improvements in the current year, and this was reflected in the significant improvement to the audit process during the current year.
- **Actions taken to drive efficiency in the future:** We understand Fujitsu have initiated discussions to commission an ISAE 3402 report for FY2012-13. If commissioned, we plan to place reliance on the findings of such a report, subject to the opinion expressed in it.

However, whilst we noted that the IT general control environment for POLSAP and HNGX has improved year on year, there is still scope for significant improvement, as detailed later in this report. A summary of key findings is highlighted below:

- **Fully implementing and embedding improvements:** There were a number of issues raised in the prior year which were partially addressed or implemented part way through the year; therefore, these require further work to close.
- **Review of privileged access:** There remain 7 users with superuser access rights in POLSAP, which in our opinion is high for a business of POL's size and nature. POL need to verify whether the existing process for determining the appropriateness of privileged access is sufficiently robust.
- **Continue to strengthen the change management process:** Change management processes need to be further enhanced, as documentation to evidence authorisation needs to be improved. POL should work with Fujitsu to verify the classification of maintenance and fix changes is adequately documented between POL and Fujitsu.

Overall, many of our recommendations are made with the expectation of implementing automatic prevent controls to mitigate our findings. However, in many cases POL has assessed that this is not possible and instead have implemented detect monitoring controls to cover the identified risk. Whilst this approach is acceptable, POL will need to be diligent in ensuring that these manual controls are continuously carried out effectively or risk a deterioration or breakdown in the IT control environment.

Finally, for certain of our recommendations, we note that Management's response represents a conscious decision to accept the risk associated with our finding. In these cases, POL should put a formal governance structure in place whereby formal acceptance of risk is documented and concluded and for those higher risk areas, concurrence from the Audit Committee is also received.

We recognise this is a journey which will require continued focus and attention. We will continue to support management in its continuous improvement initiatives throughout 2013.

Our findings are set out in greater detail in the following pages.

POL00143525

2. Current Year Recommendations – non IT related

	Issue	Location	Background	Recommendation	Management Comment
1	**Account Mapping (Current Year)**	POL - Chesterfield	We have noticed whilst reconciling the BCS trial balance to the stats some classifications are not as expected e.g. Provisions within creditors. In addition some POLSAP mappings have changed in the year as team members have changed departments, the impact of which has been that the stats classification changes when these figures flow into ESFS/BCS. Through the reconciliation between POLSAP and ESFS the mapping does not seem to be checked.	Ensure that stats classification maps in straightforward manner to BCS trial balance to ensure easy reconciliation and that no items are missed/misclassified to ease stats reporting at year end.	The provision codes used in POLSAP are owned by specified P&BA senior managers and these in turn map to specific ESFS codes. At the beginning of 2011/12 accountabilities changed, so the items mapping to the specific POLSAP codes was changed to be in line with this new accountability. At audit, a full reconciliation was provided to explain these changes. We will review the existing ESFS/BCS mapping to make sure provisions are not misclassified.
2	**GRNI**	POL - London	We recommended in previous years that management continue to look for ways to improve the purchasing process to reduce the required levels of manual input into the GRNI accrual. The balance has continued to reduce during the period as management's review of the balance has been more detailed.	During the current year, we noted that management had regularly reviewed the GRNI balance to ensure that all the GRNI items on the list were being monitored and regularly challenged. We saw an improvement in the aging of GRNI balance compared to prior year. However, it is difficult to monitor the GRNI balance when there are a	As discussed, GRNIs are reviewed regularly on a monthly basis. There are very few manual accruals and these are: (a) that were missed out by Purchasing Services at the month end and; (b) the reversal of system accrual made after the 'Delivery date' in system, where the goods/services have not been delivered. We agreed both these should be made to ensure the accounts are right. The three way matching is not currently available and we are aiming

POL00143525

	Issue	Location	Background	Recommendation	Management Comment
			The main issues continue to be the volume of line items within the listing, the difficulty in tracking delivery dates, in particular for services, and the clearing of residual values.	large number of accruals, such as in a month such as P12 when purchases are ramped up. Similarly, whilst a review will identify and ensure that high value items are being monitored, we noticed a lot of "residual" amounts < 10,000 GBP in the aged GRNI balance. We encourage management to look to reduce level of manual input into GRNI accrual in the future.	to improve the current process under the new Finance Roadmap, which will deliver the new Finance System for independent POL.
3	**DVLA Balance**	POL - London	At the end of May (around stats signing time), the DVLA creditor balance at year end is trued up to reflect RPI adjustment communicated by the DVLA. This can result in an adjustment posting to DVLA creditor in the following year as the books are closed.	We recommend management to be proactive with anticipating the RPI rate, either by contacting DVLA in advance of what the RPI rate will be, or looking at rates from Office of National Statistics to do a reasonableness check. When we checked this for stats during current year, the amount wasn't material, but may be in future periods.	In the jointly-agreed outturn forecasts POL use DVLA-supplied inflation assumptions, which as you say are "trued up" the following year. This later adjustment is only the difference between the actual RPI and the assumed one and ought not to be material.
4	**IPS Balance**	POL - Chesterfield	POL supply passport services on behalf of IPS, and have an IPS Vendor Creditor at year end. During the year, IPS experienced difficulties and significant problems in recording the complete amount of money owing from POL to IPS, resulting in IPS billing POL less than it	Whilst we were happy with the IPS Creditor from an audit point of view, noting that the balance on system was reasonable, and that the problem lies on IPS' side, we encourage POL to push IPS to solve their billing problems as soon as possible, as this can be more complicated to resolve as the balance	P&BA highlighted this to IPS last November and continue to challenge IPS regarding correcting the current issue on a weekly basis. Our contact within IPS is testing the use of an improved reporting programme that should reduce the number of barcodes that are being incorrectly removed from IPS invoice. They have tested this on 2 invoices which we are yet to receive, however early indications by IPS are that this has been successful. On receipt of these invoices and the completion of the settlement adjustments,

POL00143525

	Issue	Location	Background	Recommendation	Management Comment
			should have been owing them. However, POL have been able to track the correct amount of the balance, and have been been reimbursing IPS by way of "settlement differences". POL made £20.7m of payments by way of "settlement differences" in the current year. We note that POL is able to justify the correct IPS Vendor Creditor balance of £14m at year end, and we were able to be comfortable from an audit point of view.	increases and as time goes on. A solution has to be found, which may include; third party reporting to gain a position balance as at March 2012 end, followed by a new approach to billing or a new agreement (such as settling on POL data).	POL will be in a position to confirm whether this improvement has been successful. P&BA continually challenged the late receipt of invoices which has led to a change in the IPS billing process, resulting in a faster turnaround of invoices. IPS have been approached in the past regarding settling on POL data but were reluctant to progress.
5	**Bonus Accrual**	Payroll – Bolton	Every quarter, the Bolton payroll team sends the London finance team (ie. Finance Analyst Ravi Dudala) a calculation of quarterly bonuses for approval, which the London team confirm by email. All bonus payments are authorized by both the operational manager and a financial manager, and a log maintained of those which are reviewed and authorised.	We recommend that there are clear methods of communication from Finance team to Bolton payroll centre to approve the Bonus calculation, and management should ensure they keep a record of this. The payroll service head must also be copied into the email confirming the final bonus to be applied, since this is an important issue that occurs on a quarterly basis.	Agreed that in this area the control check failed which was not due to the actual control not being adequate but more so that it has just not been delivered in full for 2 x quarters ie. sign off not received. It was also noted that Q3 check had been delivered and since the audit check subsequent bonus payments have all been subject to full control check.

POL00143525

	Issue	Location	Background	Recommendation	Management Comment
			For Q3 & the Annual Bonus Payment, we observed that both the approval from London Finance team & payroll manager reconciling SAP output to the bonus spreadsheet were in place, and the control was effective. However, for both Q1 and Q2, we noted that whilst there was clear evidence that the payroll manager reconciled SAP output to the bonus spreadsheet, there was no email record as at Q1 &Q2 on the London finance team approving the bonus calculation.		

POL00143525

3. IT related Recommendations

Ref	Observation	Location	Background	Recommendation	Management Comment
1	**Privileged access**	IT	We reviewed privileged access to IT functions including access to user administration functionality across the in-scope applications and their supporting infrastructure. Whilst we noted some reduction on the number of accounts assigned with privileged access to POLSAP, the following observations identified last year remained open at the time of our review: POLSAP • The following seven dialog and service generic accounts were found to be assigned to the SAP_ALL and SAP_NEW profiles within the POLSAP production environment (PLP-400): ○ ADMINBATCH ○ BASISADMIN ○ DDIC (assigned to the SAP_ALL profile only) ○ OTUSER ○ SAP* ○ SOLMANPLM500 ○ WF-ADMIN. Users with SAP_ALL access have unrestricted access to POLSAP, including the capability to process and approve financial transactions. The SAP_NEW profile provides general access to new profiles and authorisations which are included in a new SAP	We recommend that management conducts a review of privileged access to IT functions across the in-scope applications and their supporting infrastructure to determine whether the level of privileged access granted is appropriate. Where access is deemed to be inappropriate, this access should be revoked immediately. For POLSAP accounts associated to the SAP_ALL and SAP_NEW profiles, management should revisit the need to grant this level of privileged access to the production environment. Access to accounts with the SAP_ALL and SAP_NEW profiles should only be used when needed. Where privileged POLSAP accounts are used to configure and run scheduled jobs, management should consider creating system accounts to run scheduled jobs so manual login is not allowed and individual dialog accounts to configure scheduled jobs in order to promote accountability. Where it is unavoidable to remove SAP_ALL	This observation and recommendation, repeated in previous audits, has been successively addressed by increasing levels of control. Since the last audit the use of Generic Privileged Accounts is monitored continually by Fujitsu. The granting of this privilege must be justified; is time-bound and is reported monthly to the POL Information Security Management Forum (ISMF) for approval by the head of Information Security. In addition, where users have access to this privilege, their ability to 'SUDO' (switch privileges inside user session) is additionally monitored. As for previous years there is a continuing need for certain key system activities to be executed by these admin teams with these privileges. For out of hour's support it is not possible to predict the privileges

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			release. • The SAP* and DDIC accounts were not locked. This does not meet recommended practice of removing all profiles from SAP* and locking both the SAP* and DDIC accounts. We also noted that the SAP* account had a last login date during the audit period and that the DDIC account is associated to the S_A.SYSTEM privileged profile. <u>HNGX</u> We understand that Fujitsu has undertaken actions to investigate some of the inappropriate privileged access identified from last year's audit, however the prior year observations noted below for HNGX were still valid at the time our review. • There are inappropriate system privileges assigned to the APPSUP role and SYSTEM_MANAGER role at the Oracle database level on the Branch Database server (BDB) supporting HNGX. • There is inappropriate privileged access at the Oracle database level on the Transaction Processing System server (DAT) supporting HNGX: ○ System privileges assigned to the APPSUP role and OPS$TPS account are inappropriate. ○ The following accounts associated to the DBA	and SAP_NEW access, it is recommended that a periodic review of the activities executed by the accounts granted permanent SAP_ALL and SAP_NEW access is performed to gain assurance that no inappropriate or unauthorised activity has been performed which may adversely impact the financial statements. Management should implement monitoring controls to help ensure that controls operated by the third party service providers are in place and are in operation, for example, monitoring of appropriateness of access to privileged users/profiles.	required for support, therefore the use of elevated privileges is justified. Devolving SAP_ALL privileges to specific roles could not adequately cover all out of hours support scenarios. Further additional controls do not appear to be justified. However the rigour of the monthly check at the ISMF will be tested to ensure it is adequate, if not steps will be taken to optimise the checking of these accounts. The issues around privileged access are focused on the possibility that a privileged user may abuse their access. Post Office believes that the existing process provide sufficient transparency and accountability to deter such activity. Post Office accepts that deterrence is not as strong as prevention but in this case the operational impact of devolving SAP_ALL privileges is

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			role are no longer required: ▪ CFM_DBA ▪ SPLEX_ROLE_BOTH. ○ The following accounts have inappropriate access to user administration functionality through the Admin access parameter 'ADM is set to yes': ▪ OPS$TPS ▪ SPLEX_ROLE_BOTH. Unrestricted access to privileged IT functions increases the risk of unauthorised/inappropriate activities which may lead to the processing of unauthorised or erroneous transactions.		believed to carry more risk of operational instability. Consequently, Post Office's attention will address enhancing the process to ensure that lapses in record keeping can not easily occur in the future; and that attention will be given to enhancing this accountability and transparency where possible. **HNG** Post Office has significantly improved the processes around 'Privileged Access' since the last audit. There are a number of controls in place to monitor system privileges. The levels of privileges required to maintain the infrastructure and service are deemed appropriate. A standardised approach to access control now exists including reporting for Privileged Access Utilisation. Further mitigating controls are in place

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					through the use of iKeys and issuing procedures. The Post Office Information Security Management Forum reviews the adequacy and controls in place regularly as part of its BAU function and reviews appropriateness of access against best practice for centre of excellence models. **POLSAP** Post Office will follow up on the privileged access improvements identified and liaise with the third party supplier to ensure such as access is appropriately controlled. Post Office will aim to ensure such privileged access is given on a strict business need basis such as incidents and change requests raised and where given effective monitoring processes are in

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					place. Currently, the review and management of privileged access through these accounts is undertaken by all requests being approved via Post Office Service Management and subsequently reviewed on a monthly basis with suppliers and Post Office Information Security. The use of privileged accounts for scheduled jobs and process for scrutiny of this use will be reviewed to assess the feasibility of further strengthening the controls over privileged users. Post Office accepts there is further work that can be done to reduce the existing risks in this area and the associated actions look to close these risks down. **Action 1.a.** Post Office to verify that the existing process for determining appropriateness of

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					privileged access is sufficiently robust and if not then to action further improvements. ***Owner Richard Barber. Target completion date 31/07/2012.*** **Action 1.b.** Verify the existing process adequately assesses the activities executed by the accounts granted permanent use of SAP_ALL, SAP_NEW privileges to ensure no inappropriate or unauthorised activity has been performed. If not then assess and where possible implement more robust process. ***Owner Richard Barber. Target completion date 31/08/2012.*** **Action 1.c.** Post Office, through their supplier Fujitsu, will investigate the use of privileged accounts with manual login for scheduled jobs and report the outcome through the Information Security Management Forum.

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					Owner Mark Arnold (TBC). Target Completion Date: 31/08/2012
2	**User administration process**	IT	Our examination of the processes for the creation, modification and removal of users' access showed the following: HNGX • There was no evidence to support the authorisation of the creation of one user account selected for our walkthrough. • The termination date for the leaver we selected for our walkthrough was 06/05/11 whilst the request to remove the access was raised only on 06/09/11, four months after the leaving date. • Based on our reconciliation of the Fujitsu terminated employee listing to the Active Directory listing which controls access to the HNGX estate, we noted one terminated employee whose Active Directory account remained active. • There was no evidence to support the authorisation of the removal of an Active Directory group membership for one user account selected for our walkthrough.	We recommend the following improvements: HNGX Strengthen the existing user administration processes within Fujitsu so that documentation supporting the request, approval and set-up of access to the HNGX estate is retained. POLSAP • Strengthen the existing user administration process for cash centre users so that (i) documentation supporting the request, approval and set-up of temporary assignment of access to cash centre users is retained (ii) cash centre managers are made aware that permanent access modifications should follow the standard user administration process for supply chain users, where an authorised SAP ADS access request form is completed. Furthermore, management should consider implementing a monitoring control to ensure that the process implemented for assigning temporary access to cash centre users is	**HNG** The process for managing the User Admin process has been improved since the last audit. However, Post Office will monitor the process regarding retention of the documentation that supports request, set-up and approval. **Action 2.a.** Post Office will work with Fujitsu to re-iterate the process regarding the document retention ***Owner Bill Membery. Target completion date 30/06/2012.*** **Action 2.b.** Post Office will work with Fujitsu to ensure the Joiner/Leaver/Transfer process is fully embedded and appropriate checks are being performed.

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			POLSAP • We found a POL employee who left on 04/06/11 but the account remained active up to 23/09/11. Further investigation showed that this delay was caused by late notification from the line manager. • As we observed in the 2010/11 audit, POL cash centre managers are granted limited access to user administration in POLSAP through transaction *SU01* allowing them to assign cash centre profiles to users within their depot. As such there is a lack of segregation of duties between the authorisation and granting of access to cash centre users. In response to our comments last year, POL has implemented a process whereby a form is required to authorise the temporary assignment of roles to cash centre users and a monthly review is performed to check that roles assigned to cash centre staff do not create a segregation of duties conflict. However, based on our walkthrough and testing samples of 27 new and modified user access to POLSAP, we noted 17 users (16 POL users, one Steria user) where the line manager or cash centre manager authorising/confirming appropriateness of access also had access to user administration on POLSAP.	being adhered to. • Implement a monitoring process around the activities of privileged users (i.e. cash centre managers with access to *SU01*). Where part of the user administration process is controlled by third party service providers, management should ensure adequate monitoring controls are in place to help ensure the controls operate as intended. HNGX and POLSAP • Strengthen the revocation of access process such that IT is notified in a timely manner when a terminated employee no longer requires access to POLSAP and the HNGX estates. 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.	***Owner Mark Arnold. Target completion date 31/08/2012.*** **POLSAP** The administration process within Cash Centres has been improved following the last audit. However Post Office will re-iterate the process for retention of documentation supporting the request, approval and set-up of temporary assignments to cash centre users. Additionally Post Office will re-communicate to cash centre managers that the standardised process for user administration should be strictly followed. Post Office will also consider a monitoring process as part of this review both within Post Office and with 3rd party suppliers. Post Office accepts there is further work that can be done to reduce the existing risk and the associated actions look to

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			• Based on our sample of 25 instances of new and modified user access to POLSAP, we noted that: ○ The new process noted above was implemented on 01/10/11. For one out of two cash centre modifications which took place after this date, we noted that this form had not been retained. ○ For one cash centre user modification the line manager stated that the role had been assigned permanently, in which case the modification of access should have followed the supply chain user administration process rather than the process for assigning temporary roles to cash centre users. • Based on our reconciliation of the Fujitsu and Post Office terminated employee listings to the POLSAP user listing we noted four terminated employees whose user accounts remained active. Failure to maintain appropriate documentation for the user administration process increases the risk that accounts with excessive or inappropriate privileges may exist, therefore increasing the risk of unauthorised/unnecessary access to systems. Furthermore, this risk is increased by inadequate segregation of duties between the approval and setup of access as well as failure to remove terminated employees' access promptly.		resolve them. **Action 2.c.** Post Office will re-iterate the process for documentation retention of temporary assignments to cash centre users. Ensure that the existing monitoring process for cash centre approvals and 3rd party suppliers is robust. ***Owner Sid Hadadi. Target Completion date 30/06/2012.*** **Action 2.d.** Post Office will re-iterate to cash centre managers the requirement to follow the standardised process for user administration. ***Owner Sid Hadadi. Target Completion date 30/06/2012***. **Action 2.e.** Post Office will review the monitoring controls for 3rd party suppliers for POLSAP to ensure that the controls are in

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					place and in operation. ***Owner Andy Jones (TBC). Target Completion date 31/08/2012***
3	**Change management process**	IT	We reviewed the processes implemented to determine that all program changes are appropriately authorised, tested and approved prior to implementation into the production environment for the applications in scope. Whilst we noted some improvements on the process compared to last year, some of the points raised last year have not been fully remediated. Specifically, we noted the following : <u>POLSAP</u> Based on a sample of 17 changes made to the POLSAP production environment during the audit period we noted: • For six changes, whilst we were able to obtain evidence that the changes had been tested by Fujitsu, the name of the person who performed the testing was not recorded • For four changes, whilst we were able to obtain evidence of approval from the POL Change Control team, the name of the person who approved the change to go live from POL was not recorded • For two changes, we noted that POL initiated the change but the name of the Product and Branch	Management should seek to enhance the current change management process/policy further to include: • The level of documentation to be retained to evidence that POL is involved in authorisation, testing and approving changes made to the applications. In particular, evidence to support the individual from POL or third party service provider authorisation, testing and approval of the change prior to deployment should be retained to promote accountability. This will provide management reasonable assurance that program changes being implemented into the production environment have been authorised, tested and approved prior to deployment. Please note that all documentation should be retained. • Definitions of the responsibilities of all parties involved in the authorisation, testing and approval of changes deployed into the production environment, based on the nature of the change. There is a need for POL to increase their	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. 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. 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

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			Accounting (P&BA) team member who logged the call was not recorded • For one change, we were unable to obtain evidence that the change had been authorised by POL or Fujitsu prior to development • For one change, we were unable to obtain evidence that it had been approved by POL prior to deployment into the production environment. Whilst we have been advised that POL is not usually involved in testing fixes or maintenance changes, we have noted from the samples of changes made to POLSAP that POL has tested one out of ten changes of this nature. <u>HNGX</u> Based on our walkthrough and testing samples of 11 back end changes, 11 counter changes and six manual changes made to the live HNGX estate during the audit period, we noted the following: • For two manual changes and three back end changes, although POL approval was recorded in the Manage Service Change (MSC) system prior to implementation, the name of the member of the POL Change Control team who provided the approval was not recorded. • For 28 changes we were unable to obtain evidence of	involvement in the change management process, specifically business user testing of fixes and maintenance changes to the in scope applications. The change management policy documentation should also describe the overall manage change process Management should implement monitoring controls to help ensure that controls operated by the third party service providers are in place and are in operation.	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. However, Post Office accepts there is further work that can be done to reduce the existing risk. **Action 3a.** Post Office will amend its change processes so that names are recorded in the authorisation, testing and approval process of changes. ***Owner Andy Jones. Target Completion date 31/08/2012.*** **Action 3b.** Post Office will work with Fujitsu to verify that the

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			testing performed by POL where 19 changes relate to maintenance changes made by Fujitsu (e.g. anti-virus updates, standard platform build, branch/router configurations, security upgrades, infrastructure changes) • For one change we were unable to obtain evidence of testing performed by Fujitsu. • For one change we were unable to obtain evidence of POL approval prior to implementation in the live environment. There is an increased risk that unauthorised and inappropriate changes are deployed if they are not adequately authorised, tested and approved prior to migration to the production environment and documentation supporting these controls is not retained.		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. ***Owner Andy Jones (Post Office) and Mark Arnold (Fujitsu). Target Completion date 31/07/2012.***
4	**Periodic user access reviews and monitoring controls**	IT	In the 2010/11 audit we recommended improvements to the periodic user access review process and monitoring controls. Whilst we have noted the efforts by management to strengthen the control environment this year, we noted opportunities to improve the process further. HNGX Whilst we have been advised that there is a new process	Management should consider the implementation of 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	The existing process verifies that all joiners, leavers and movers have appropriate access for their role. The annual review of all accounts verifies this. The monthly review of all movers captures interim changes and in addition the inactive users are also identified after a pre-defined period of inactivity and

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment

			in place this year for the periodical review of the appropriateness of access assigned to the HNGX estate, we understand that this is based on a database that records access granted and terminated, rather than on user access listings generated directly from Active Directory, which diminishes the effectiveness of the control.
			
			Our user appropriateness review identified one user account that no longer required access to HNGX.
			
			<u>POLSAP</u>
			
			Whilst we note that there is a process in place to review the appropriateness of P&BA and Supply Chain users' access to POLSAP on a periodic basis, sufficient evidence of the review has not been retained.
			
			Conflicts in segregation of duties and excessive or inappropriate access to financial systems may arise if a regular re-validation of user access is not performed.
				applications.
				
				The following outlines how this process may be implemented:
				
				• User listings containing all active users and their access levels to be generated by IT and emailed to relevant department managers whereby they provide responses detailing:
				  ○ Whether the current access of their employees is in line with their job role
				  ○ Whether any users require their access be modified or removed. Where additional access is required requests should be made through the existing user modification process. Where access is required to be removed, flagging these users and providing comments is sufficient. These responses should be actioned by IT on a timely basis.
				• All documentation to support the operation of these controls should be retained, including:
				  ○ Emails to managers requesting responses
				  ○ Responses from managers detailing
					then reviewed. These processes are considered sufficiently robust. However, Post Office accepts there is further work that can be done to reduce the existing risk. Therefore, Post Office in conjunction with Fujitsu will verify that adequate authorisation is identified and recorded and where not will take appropriate steps to remediate.
					
					The issues around user access management seem to be focused mainly on very infrequent lapses in the existing process. Consequently, Post Office's attention will address enhancing that process to ensure such lapses can not easily occur in the future.
					
					Action 4. Post Office in conjunction with Fujitsu will verify that adequate authorisation is identified and recorded and where not will take

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
				whether changes are required (responses should be provided whether changes are required or not) o Overall signoff on the completion of the review from management. The above review should include all user accounts including those privileged user accounts owned by IT and vendors. In addition, the individual responsible for performing the review should have limited access to the application in order to prevent the review of their own access. In terms of monitoring privileged access, management should specifically consider implementing a periodic review of users with privileged access to IT functions within the HNGX estate. Evidence to support the operation of the above monitoring controls for privileged IT access should also be retained to support accountability and provide assurance to POL management.	appropriate steps to remediate. ***Owner Richard Barber. Target completion date 31/07/2012.***
5	**Generic privileged accounts**	IT	Our review of privileged access to the in-scope applications and their supporting infrastructure last year revealed individuals sharing password to multiple generic privileged accounts. The same observation remains valid this year at the time of our review:	Management should consider a review of generic privileged accounts across the in-scope applications and their supporting infrastructure to determine whether such accounts can be replaced with individual user	This observation and recommendation, repeated in previous audits, has been successively addressed by increasing levels of control. Since

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			• The password to the privileged SYSTEM account on the Oracle database on the BDB and DAT servers supporting HNGX is known to four of the 11 members of the IRE11 TST DBA team and the password to the same account on the XID and R3D servers supporting SAP XI and POLSAP applications is known to the three members of the SAP Basis team. • The password to the privileged DBA account on the Oracle database on the BDB and DAT servers supporting HNGX is known to the RMGA Unix team and four of the 11 members of the IRE11 TST DBA team respectively. The password to the DBA account on the XID and R3D Oracle database servers supporting SAP XI and POLSAP applications is known to the three members of the SAP Basis team. • The password to the privileged SYS default account on the Oracle database on the BDB and DAT servers supporting HNGX is known to four of the 11 members of the IRE11 TST DBA team respectively. The password to the SYS account on the XID and R3D Oracle database servers supporting SAP XI and POLSAP applications is known to the three members of the SAP Basis team. • The password to the default privileged Administrator	accounts to promote accountability. Management should also consider implementing monitoring controls to help ensure robust security practices are in place particularly those operated by third party service providers.	the last audit the use of Generic Privileged Accounts is monitored continually by Fujitsu. The granting of this privilege must be justified; is time-bound and is reported monthly to the POL Information Security Management Forum (ISMF) for approval by the head of Information Security. In addition, where users have access to this privilege, their ability to 'SUDO' (switch privileges inside user session) is additionally monitored. As for previous years there is a continuing need for certain key system activities to be executed by these admin teams with these privileges. For out of hour's support it is not possible to predict the privileges required for support, therefore the use of elevated privileges is justified. Devolving SAP_ALL privileges to specific roles could not adequately cover all out of hours support scenarios. Further additional controls do

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			account on the Active Directory server controlling access to the HNGX estate was known to the nine members of the IRE11 NT team. • Furthermore, the password to the following accounts with the SAP_ALL and SAP_NEW privileged profiles on POLSAP is known to the three members of the Fujitsu Basis Consultants team: ○ ADMINBATCH ○ BASISADMIN ○ OTUSER ○ SAP* ○ SOLMANPLM500 ○ DDIC (assigned to the SAP_ALL profile only) ○ WF-ADMIN. The use of generic accounts undermines accountability and can lead to unauthorised access to financial data.		not appear to be justified. However the rigour of the monthly check at the ISMF will be tested to ensure it is adequate, if not steps will be taken to optimise the checking of these accounts. The issues around generic privileged accounts seem to be focused partly on very infrequent lapses in the existing process and partly on the risk that a privileged user might misuse their access or their elevated privileges. Post Office accepts that deterrence is not as strong as prevention but in this case the operational impact of devolving SAP_ALL privileges is believed to carry more risk of operational instability. Post Office believes that the existing process provide sufficient transparency and accountability to deter such activity. Consequently, Post Office's attention will address enhancing the process to ensure that lapses

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					in record keeping can not easily occur in the future; and that attention will be given to enhancing this accountability and transparency where possible. Post Office accepts there is further work that can be done to reduce the existing risks in this area. **Action 5. T**he rigour of the monthly check at the ISMF will be tested to ensure it is adequate, if not steps will be taken to optimise the checking of these accounts. ***Owner Richard Barber. Target completion date 31/07/2012.***
6	**Password parameters**	I T	We reviewed the password configurations for the in-scope applications and the infrastructure supporting these applications. Whilst our examination revealed some improvements to the observations raised from last year's audit, the following observations remain open: • We reviewed the password configurations for the in-scope applications against Fujitsu's RMGA Security Policy and Post Office's Information Security Guide.	Whist we acknowledged that password weaknesses in the application, operating system and database level are mitigated to some extent by the network Active Directory password controls, the following is still recommended to further strengthen the control environment a) Review and update the 'RMG Information	Since the last audit the RMG Information Security policy (SVM/SEC/POL/0003) has been amended to meet recommended good practice and approved by POL. In regard to network, application and infrastructure components these have been

POL00143525

<table>
<tr><th>Ref</th><th>Observation</th><th>Location</th><th>Background</th><th>Recommendation</th><th>Management Comment</th></tr>
<tr>
<td></td><td></td><td></td>
<td>
We noted the following password parameters have not been defined:

<u>RMGA Security Policy</u>
• Reset account lockout counter
• Idle session timeout

<u>Post Office Information Security Guide</u>
• Account lockout threshold
• Reset account lockout counter
• Account lockout duration
• Idle session timeout.

We also noted that there are password setting weaknesses within the RMGA Information Security Policy:
○ Number of passwords that must be used prior to using a password again is defined as ‘Re-use of the same password must not be permitted for either a specified time or until at least 4 other passwords have been used’
○ Account lockout duration is defined as ‘the user must be locked out for at least 30 minutes or until reset by an administrator’
• There are password setting weaknesses within the POLSAP application:
</td>
<td>
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 HNGX and POLSAP

b) 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

<table>
<tr><th>Password setting</th><th>Recommended configuration</th></tr>
<tr><td>Minimum password length</td><td>6 - 8 characters</td></tr>
<tr><td>Complexity</td><td>Alphanumeric including special characters and</td></tr>
</table>
</td>
<td>
reviewed and where necessary have been amended to fall in line with new policy. The new policy has been cascaded to all users, especially admin teams. There is now regular monitoring and communication through embedded BAU process. Non compliances are reviewed at the ISMF and a Pen test has been established as part of BAU.

Post Office believes that the controls in place are sufficient to mitigate the risk exposure. Notwithstanding that Post Office will continually monitor this to ensure continuing compliance, this risk is accepted.

Action 6a. Post Office will regularly review the scope of the BAU Pen test to ensure all relevant network, application and infrastructure component password configuration continues to meet appropriate password parameters. Where
</td>
</tr>
</table>

POL00143525

<table>
<tr><th>Ref</th><th>Observation</th><th>Location</th><th>Background</th><th>Recommendation</th><th>Management Comment</th></tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>

Minimum password length is 6 characters. This does not meet RMG Information Security Policy guideline of a minimum of 7 characters
Idle session time out is set to 3600 seconds. This does not meet the recommended setting of 1800 seconds or less
Table logging is not enabled (i.e. rec/client = OFF). This does not meet the recommended setting of ON

There are password setting weaknesses at the Linux operating system level on both the application servers supporting POLSAP (R3A) and HNGX (BAL) :

Minimum password length is 5 characters. This does not meet RMGA Information Security Policy guideline of a minimum of 7 characters
Maximum password age is set at 99999 days. This does not meet RMGA Information Security Policy guideline that passwords must expire in 30 days
Minimum password age is set to 0 days. This does not meet the recommended setting of 1 day
Account lockout after failed login attempts is not set. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts

</td>
<td>
<table>
<tr><td></td><td>upper/lower case</td></tr>
<tr><td>Frequency of forced password changes</td><td>90 days or less</td></tr>
<tr><td>Number of passwords that must be used prior to using a password again</td><td>5 (Should be higher if passwords changed more frequently)</td></tr>
<tr><td>Initial log-on uses a one-time password</td><td>Enabled</td></tr>
<tr><td>The number of unsuccessful log on attempts allowed before lockout</td><td>3 – 5 invalid attempts</td></tr>
<tr><td>Account lockout duration</td><td>Forever until manually unlocked</td></tr>
<tr><td>Idle session timeout</td><td>30 minutes</td></tr>
<tr><td>Account lockout reset counter</td><td>60 minutes</td></tr>
</table>

Management should consider implementing monitoring controls to help ensure robust security settings are in place particularly those operated by third party service providers.
</td>
<td>
this is technically feasible.
Owner Richard Barber. Review Annually.

Action 6b. Where new architecture is developed and deployed (network, application and infrastructure) these will be required to meet the appropriate password parameters and included in the BAU Pen test.
Owner Richard Barber. Review Annually.
</td>
</tr>
</table>

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			○ Password history is not set. This does not meet the recommended setting of 5 passwords ○ Idle session timeout is not set. This does not meet the recommended setting of 30 minutes. Note: This setting only applies to the POLSAP R3A platform • There are password setting weaknesses on the Windows 2003 Active Directory Controller supporting HNGX: ○ Account lockout threshold is set to 6 failed login attempts. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts ○ Account lockout reset counter is set to 30 minutes. This does not meet the recommended setting of 60 minutes ○ Account lockout duration is set to 30 minutes. This does not meet the recommended setting whereby an Administrator is required to unlock the account • There are password setting weaknesses at the Oracle database level on the database servers supporting POLSAP (R3D)and SAP XI (XID) and on the branch database server (BDB) and transaction processing system server (DAT) supporting HNGX : ○ Minimum password length is not set. This does not meet the RMGA Information Security Policy		

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			guideline of a minimum of 7 characters ○ Password composition is not set. This does not meet the RMGA Information Security Policy guideline of alphanumeric ○ Frequency of forced password changes does not meet RMGA Information Security Policy guideline of 30 days or less ○ The number of unsuccessful log on attempts allowed before lockout is set to set to 10. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts ○ Account lockout duration is not defined. This does not meet recommended practice of at least 5 days for the Oracle database ○ The number of passwords that must be used prior to using a password again is not set. This does not meet the recommended setting of 5 passwords ○ Idle session timeout is not set. The does not meeting the recommended setting of 30 minutes Weak password settings increase the risk of unauthorised access to financial processing and data.		
7	**Logical security settings**	IT	Our review last year of the logical security settings for the infrastructure supporting the applications in scope identified certain logical security weaknesses. From our review this year, we noted that these weaknesses are still	Management should consider the following: • Setting an encrypted password for the LISTENER.ORA file on all Oracle databases	Disabling the default administrator account for Active Directory for HNGX and replacing with a new administrator

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
			valid. These include: • For the Oracle database supporting SAP XI (XID) and the Branch Database server (BDB), and Transaction Processing System server (DAT) Oracle databases supporting HNGX, we noted that the password for the LISTENER.ORA file has not been enabled and the password entry does not contain an encrypted value. • The default Administrator account on the Active Directory server controlling access to the HNGX estate (ACD) has not been disabled. Inadequate system security settings increase the risk of unauthorised access to financial data.	supporting the in-scope applications • Disabling the default Administrator account and create a new Administrator account with a strong password. Management should also consider implementing monitoring controls to help ensure robust security settings are in place, particularly those operated by third party service providers.	account appears to carry no benefit as the identifying ID for the account would remain the same. The existing password follows recommendations for strong passwords. Against the marginal improvement in access risk Post Office recognise that the default admin account is embedded in key maintenance activities and replacing the default admin account carries a greater risk of causing disruption to the operational stability of the system. However, Post Office will request Fujitsu to assess the cost and operational impact of this change. There in only marginal benefit of encrypting LISTENER.ORA password when the other controls managing access to the listener service are considered. However, Post Office will request Fujitsu to assess the cost and operational impact of making this change. But it is believed that the disadvantage in terms of

POL00143525

Ref	Observation	Location	Background	Recommendation	Management Comment
					potential system disruption out way the very marginal access risk reduction. Notwithstanding the actions above (item 6) that may drive further improvements Post Office believes that the controls in place are adequate to mitigate the risk and therefore the risk is accepted. **Action 7a.** Post Office will assess the possibility of setting an encrypted password for the LISTNER.ORA file. ***Owner Richard Barber. Target Completion Date 30/09/2012.*** **Action 7b.** Post Office will request Fujitsu to assess the cost and operational impact of encrypting the LISTNER.ORA file.. ***Owner Richard Barber. Target Completion Date 31/07/2012.***

POL00143525

4. Prior Year Recommendations Update – non IT related

	Issue	Location	Background	Recommendation	Management Comment	Current Year Update
1	**GRNI**	Finance – London	We recommended in previous years that management continue to look for ways to improve the purchasing process to reduce the required levels of manual input into the GRNI accrual. The balance has continued to reduce during the period as management's review of the balance has been more detailed. The main issues continue to be the volume of line items within the listing, the difficulty in tracking delivery dates, in particular for services, and the clearing of residual values.	We have noted improvement in the review of the accrual and would encourage management to continue to strengthen the review to ensure that: - Aged balances are challenged - Significant services line items are reviewed for adequacy - Timely clearing of residual values. In addition, with upcoming changes to the business, and in particular separation activity, management should continue to explore options to improve the purchasing process.	Noted in detail in section 2 – Current Year Recommendations.	Noted in detail in section 2 – Current Year Recommendations.
2	**Human Asset Check**	Payroll – Bolton	An employee asset check was completed for the first 6 months with a response rate of 75%. The remaining 25% was not completed given the upcoming organisational	We recommend that HR reviews the results of the trial run of the employee asset check and ensure that	Agreed a) Employees – the final verification of our structure will in effect	Employees & Agents: During the current year, it was noted that whilst the POL service centre

POL00143525

			restructure. However, as all employees are expected to be put onto new online organisational chart before March 2011, Management believes this will allow for a more robust human asset check in the future. The agent asset check continues not to be in place. The design of an asset check for agents is still under discussion and the HR department have put forward a suggested process to senior management and are awaiting approval. As this control is not yet fully operational, there is a continued risk of either 'ghost' employees or agents, or that employees or agents who have left the business incorrectly remain on the payroll.	100% coverage is achieved. In addition, we await to see senior management's decision regarding implementation of the proposed agent's asset check but recommend that the proposed control is introduced at the earliest opportunity to migrate the inherent risks.	deliver the second 6 month review as per the agreed control. We also hope to deliver a trial in March 2011 of the new process which will be introduced from the new financial year. b) Agents – Currently we are performing a check of offices paid on HRSAP against office transacting basics products eg. 1st class stamps (via Credence). We intend to continue with this check and await a decision on whether we require anything further to deliver an acceptable asset check for our agent population.	carried out a human asset check in June 2011 and January 2012, and this was satisfactorily carried out so we were able to perform controls testing and place reliance. Management were also able to review the results of the process, and received a response rate of 97%, which is an improvement from 75% in prior year. We would continue to encourage management to review the results of the human asset check as it is a value-adding control to check for the existence of employees. We were able to rely on the human asset check from a controls testing effectiveness perspective and have no current year management letter comment.
3	**Change Requests (General Review)**	Payroll – Bolton	We noted a marked improvement in the maintenance and transparency of the employee changes log spreadsheet, however one month sampled identified that the 10% check had not been carried out in full, with only 8% of	We recommend that the change from a "contractual" change request to a "non-contractual" change request	Agreed – Now in place a) Additional column has now been included on our spreadsheet to	For current year audit, we have noted that management's responses to FY2010/11

POL00143525

			changes (contractual and non-contractual) being subject to review. It was also noted that the log was not amended in cases where the information would suggest a contractual change but once processed this was not the case, however it is recorded by sign off if the change lead to a contractual change. This control is important in ensuring that all changes are being reviewed and input onto SAP correctly. It was noted that this was done in the other months selected for testing apart from the exception noted above.	be clearly documented on the spreadsheet in order to ensure transparency over what contractual changes have been made. In addition, we recommend that the level of secondary check each month (eg 10% of the full population) is adhered too in all cases.	highlight where there is a change in status from the source document ie. sent as contractual and processed as non-contractual or vice versa. This is already noted on the source document however this addition adds visibility. b) 10% check as detailed in our Control Manual will be delivered. On the one month where only 8% was documented this has now been re-visited retrospectively and the team leader has checked a further sample to meet the agreed requirements.	comments have been addressed. We note that the 10% check was carried out in full for Change Requests during the current year. In addition, an additional column was included in the spreadsheet to indicate where the change was or was not contractual.
4	**Agent Leavers Review**	Payroll – Bolton	Based on our review of the secondary check-sheets used in the agent leavers processes, we identified 3 instances in one month (January) where the leaver was identified for secondary checking but the secondary review of the leaver details was not completed. We did note that the initial checks of these leavers had been completed. The secondary checks are in place to ensure that	We recommend that management ensure that the control policy to secondary check 10% of the population of leavers each month is fully implemented.	Agreed – Now in place. The 3 instances identified have now been checked retrospectively. This check is in place and documented on our	In current year, we note that EY 2010/11 recommendations have been implemented. No issues noted with 10% check, control is effective.

POL00143525

			adequate review of the process is occurring and that the leaver is correctly removed from the system to avoid overpayment.		Control Manual so should have been delivered. In addition to the standard check this area is checked periodically at Service Manager level however given the audit finding we will extend this high level check to be delivered each month, commencing P11.	
5	**Variance Report for Agents**	Payroll – Bolton	It was noted when testing the agents pay variance reports for April, August & September that there were a small number of exceptions per the generated exception reports that had not been brought forward and noted on the summary front sheet – which is in turn reviewed by the Service Team Leader (STL). There appear to be no guidelines in place which dictate which variances and follow ups require management review although those exceptions identified within the report had been investigated in the initial review but not included on the front sheet ready for STL review. A lack of clear guidelines dictating which variances should be raised for management review leaves the potential for oversight of significant variances generated by the SAP report which are not included in the STL review.	We recommend that there are clear process guidelines for the level of management checks to indicate which variances should be raised for management review, in order to ensure no significant variances and follow up actions are omitted. All items within the report meeting this threshold should then be included on the front sheet ready for management review.	Agreed – Will be fully in place for P12 processing. The check is 100% on the variances that are produced with those requiring action documented on a front facing sheet. Narrative detailing the guidelines to perform the check will accompany the front facing sheet. The sheet will also be updated to include a 'balance' of	Management had scope and materiality in place, and there were clear guidelines dictating how variances should be raised for management review.

POL00143525

					all variances identified that period which will form part of the team leader sign off.	

POL00143525

Ernst & Young LLP

Assurance

About Ernst & Young

Strong independent assurance provides a timely and constructive challenge to management, a robust and clear perspective to audit committees and critical information for investors and other stakeholders. The quality of our audit starts with our 60,000 assurance professionals, who have the experience of auditing many of the world's leading companies. We provide a consistent worldwide audit by assembling the right multidisciplinary team to address the most complex issues, using a proven global methodology and deploying the latest, high-quality auditing tools. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information, please visit www.ey.com/uk.