Post Office Limited

Management letter for the year ended 27 March 2011

ERNST & YOUNG
Quality In Everything We Do

Private and confidential

Sarah Hall
Post Office Ltd
148 Old Street
LONDON
EC1V 9HQ

XX August 2011

Dear Sarah

Internal control matters arising from the 2011 audit

I am pleased to present our management letter for the year ended 27 March 2011.

Our review of the company's systems of internal control is carried out to help us express an opinion on the accounts 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 comments in this letter refer only to those matters that have come to our attention during the course of our normal audit work and do not attempt to indicate all possible improvements that a special review might develop. We would be happy to discuss any of the points contained within this letter in more detail with you.

We would like to take this opportunity to thank management for their input into the management letter 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

The contents of this report are subject to the terms and conditions of our appointment as set out in our engagement letter.

This report is made solely to the Board of Directors and management of Post Office Limited in accordance with the terms of our engagement letter. Our work has been undertaken so that we might report to the Board of Directors and management of Post Office Limited those matters that we are required to and for no other purpose. To the fullest extent permitted by law we do not accept or assume responsibility to anyone other than the Board of Directors and management of Post Office Limited for this report or for the opinions we have formed. It should not be provided to any third party without our prior written consent.

1. Executive summary

The finance leadership team at Post Office Limited (POL) has implemented and process improvements throughout the organisation during the past financial year.

In particular, focussed management action has addressed many of the issues raised in our prior year management letter and led to significant improvement in the overall payroll control environment. The recommendations we have made in this report should be seen as refinements rather than fundamental control deficiencies in comparison.

The main area we would encourage management focus on in the current year is improving the IT governance and control environment.

Within the IT environment our audit work has again identified weaknesses mainly relating to the control environment operated by POL's third party IT suppliers. Our key recommendations can be summarised into the following four areas:

- Improve governance of outsourcing application management
- Improve segregation of duties within the manage change process
- Strengthen the change management process
- Strengthen the review of privileged access

We also encourage management to continue to enhance the Legal & Compliance review framework to manage risks in relation to regulatory compliance associated with financial services activities.

2. Prior Year Comments – Update

	Issue	Location	Background	Recommendation	Management Comment	Current Year Update
1	**Post Office Saving Stamps Liability (POSS)**	POL - Chesterfield	The liability for Post Office Savings Stamps is £25.6m. A further £11.6m (£9.5m 2009) liability for losses has been recognised due to stamp redemption losses (predominantly fraud). The liability for redemption losses is highly judgmental and has been calculated by updating the prior year liability for an estimate of losses incurred in the current year from the results of sample checks of pouches received. Approximately 50% of returned pouches are checked. The product is due to be curtailed during 2010/11 and as a result it is expected that the majority of the liability will be run down by year end 2011.	► Based on the level of losses estimated in the year (£2.1m), we recommend that a higher proportion of returned pouches are checked while the product is run off. ► At year end 2011 the remaining liability should be calculated on a whole portfolio basis rather than as an adjustment to the brought forward liability as this will improve the accuracy of the remaining unknown liability	We accept the recommendation and had already explained during the course of the audit that we would increase our coverage during the period of the withdrawal of savings stamps. The % of pouches checked has increased from 25% at the beginning of 2009/10 to 50% now, with focus continuing to be on those pouches which we expect to be most at risk of errors. The Savings Stamps product has been withdrawn on 25th May but will continue to be accepted as a method of payment in Post Office branches until 28th August, 2010. The current value and volume of redemptions has increased by 10% and 14% respectively, but we are anticipating that by August the redemptions will drop off significantly. We anticipate that we will start to reduce the work in this area during August and the value and volume of redemptions will drop off further after this date. We will closely monitor the redemption profiles and arrange the checking work in line with these.	The support for the calculation provided in the current year addressed the recommendation from prior year. The calculation factored in the basis of estimation and showed both the higher and lower end of the range of potential outcomes. As anticipated, the withdrawal of this product has made the tracking of the liability and forecasting of redemptions easier to manage and review.

					We will also review the aggregate liability on saving stamps and bring to bear the facts of customer migration as the budget card replacement is rolled out.	
2	**Variance Report for Agents**	Payroll – Bolton	A 300 page report is produced every month showing a detailed weekly variance analysis for agents. Payroll management inform us that a review of significant variances identified within this report is intended to be a key control. The front summary sheet for each report is now signed off. However, the level of detail of the review performed varies month on month and the parameters used for selecting variances are not clear. It is also not clear why some selected variances for review are adjusted for and others not. The report is intended to be a significant control to detect any issues within the agent or employee payroll. Failure to complete the review increases the risk of an issue in the agent pay not being detected on a timely basis or at all. This could cause cash loss for the business	We repeat our recommendation from prior year that the reports are shortened to focus on the key variance analyses for the main risks. We further recommend that there is a second signatory of the report at manager level to ensure the review is happening, with a short bullet point summary of any significant variances and action taken to follow up and resolve them.	The report was kept in place in the same level of detail following the internal audit visit at half year where, although time consuming, it was felt to be of value. The report has been reviewed and subsequently revised and is now run for key variances, the output of which is a 70 page report rather than 300 pages. This has been in place since Period 11. In addition we have revised the front facing sheet to include one off payments and identification of weeks in each period both of which will highlight known variances. The facing sheet is signed and dated by both the person preparing the report and the manager reviewing the work performed.	We noted that the length of the report has decreased significantly, with more meaningful explanations for variances being noted on actual variance reports from SAP, and a higher level of detail noted on the front summary sheet summarising actions taken. This is also now being signed off at a manager level. We did however note that a number of variances that were noted on variance reports were not brought forward to the summary sheet, and have suggested that appropriate parameters be put in place for those variances which require management review.

			or increased administrative time to correct the error.			
3	**Review of Employee Change Request (Contractual Changes)**	Payroll – Bolton	Payroll management’s process requires that all employee change requests that lead to new contracts should be reviewed. A checklist for individual change requests is completed and signed off and these are tracked on an overall log for all change requests received. Based on our review of the log we identified that; Evidence of completed reviews in respect of contractual change requests were not recorded in the log The log was updated based on inaccurate provisional information and not subsequently amended. It may not be possible for payroll management to monitor that the controls that are operating effectively and to check that the appropriate request forms are being reviewed.	We repeat our recommendation from prior year that the log is maintained and updated accurately. This will give an oversight as to the effectiveness of the control. The log should clearly identify those changes that require a new contract.	The data capture spreadsheet has been re-aligned and now encompasses all of the recommendations. In addition we have made further enhancements to the data capture spreadsheet eg. introduced new numbering system to identify when the change was processed, split out processing months by unique tab, have a clear indication of 10% checks for each tab, added a further column to identify incorrect source information and also added a short facing sheet for every change which will sit with personal papers. All of the above has been in place since Period 1.	We noted during our review that it is now possible to see where the log has been updated for changes between contractual to non-contractual changes, however this is not always clear when reviewing, and as such have raised this as a current year point. For our sample selected in the current year, we noted that where the change was contractual, the full buddy check is being carried out. We also noted that in one month, the 10% check was not fully carried out, although this can be seen as being completed in all other months in the year.

4	**Review of Employee Change Requests (General Review)**	Payroll – Bolton	Payroll management's process requires that 10% of all change request forms will be reviewed each month. This review was not being evidenced on the log until January 2010. Based on our review we noted that less than 10% had been evidenced as checked (33 out of 500 in January, 24 out of 656 in February). Payroll management is not effectively monitoring that the controls to check that the appropriate request forms are being reviewed are operating effectively.	We repeat our recommendation from prior year that the log is maintained and updated accurately. Additionally, we recommend that the review of 10% of all changes is evidenced as reviewed. This will give an oversight as to the effectiveness of the control.	This is linked to Recommendation 2 as both changes and contracts are captured on a single spreadsheet. In place from Period 1 as per Action 2 (on the same spreadsheet).	See point 3 above. We have noted that in one month, fewer than 10% of changes were subject to review and we recommend that the 10% threshold is met for all months.
5	**Human Asset Check**	Payroll – Bolton	Other divisions in Royal Mail are sent a list every 6 months from the payroll department listing all the employees who should be in their area. They review that list and highlight if anyone is on the payroll that should not be. This was only performed at the start of the period by POL. Payroll management inform us that they do not feel that the control is appropriate given the nature of the business and plan to	We repeat our recommendation from prior year that this control is implemented in line with Royal Mail Group policy on a 6 month basis or an effective alternative control be designed and implemented.	Solution for employees is via 'My Template' and this is being rolled out from Period 2. My template allows real time access for Line Managers to review their structure including their people at any given time. In simplistic terms we will get periodic sign off (all captured twice per year) from each Line Manger via e-mail. The solution proposed is for Employees only. A suite of options are being developed to close the gap for Agents. Current development areas being looked at include	We noted that this control is not operating in the current year. See current year comment noted below.

			implement an alternative procedure. If this control objective is not achieved there is an increased risk of either 'ghost' employees or that employees who have left the business incorrectly remain on the payroll.		matching SAP data to sales reports, agent check on contact with Advice Centre, check on audit visit, utilisation of area sales managers for top 2.5k offices.	
6	**Complaints Log**	Payroll – Bolton	The complaints process was transferred over from Sheffield to Bolton in January 2010, however no log is being completed in Bolton to track the complaints received and the follow up actions being performed in order to close the complaint. Without maintaining the complaints log it may not be possible for payroll management to identify what actions were taken to resolve complaints.	We recommend that a log of complaints is introduced similar to the one that is performed by the other Royal Mail Group subsidiaries.	The complaints process is in place and working from Period 2 which will capture all complaints including those via our Advice Centre. Complaints are also a standard scorecard item for monthly management performance meetings which will also capture specific actions and improvement activity. In addition we are working with HR Sheffield to identify any areas of best practice that can be incorporated in our complaints log.	We noted that a complaints log is now being maintained in Bolton with evidence of resolution and signoff as completion being made in the log.
7	**Agent Joiner and Leaver Review**	Payroll – Bolton	Based on our review of the secondary check-sheets used in the agent joiners and leavers processes, we identified a number of instances where there was no evidence of review of details being entered/removed correctly.	We recommend that the secondary check-sheets are maintained to evidence review of agent joiners and leavers amendment checks.	Revised process introduced from Period 1. All joiners and leavers source documentation will be cross checked on an individual basis to SAP reports and filed in monthly order. Document retention has also been extended to 15 months from 12 months. Facing sheet will also	We noted that for our sample selected, we were able to evidence that a 10% review was being carried out with secondary check sheets for agent joiners, but noted an issue with regards to

			Without adequate review, agents may be input twice, at the wrong pay amount and / or not removed resulting in overpayment.		accompany reports which will be checked and signed off by team leader each period.	employee leavers whereby the 10% checks were not being carried out in full when the actual check sheets were obtained. See management letter comment below.
8	**Budgetary Analysis**	Payroll & Head Office	No detailed review of payroll payments to agents and employees against the budget is documented. A high level review of staff costs against budget is performed by the finance team but this is insufficiently detailed to identify payroll anomalies. Payroll anomalies may not be detected resulting in over payment or under payment going undetected.	In order for the review process to act as an effective control we recommend that a detailed review of payments to agents and employees against the budget is performed and documented.	The high level review performed is not sufficient to identify payroll anomalies however, the detailed cost centre reports are reviewed on a monthly basis by the Finance Business Partner teams comparing actual costs to budgets and reviewing the employee lists. Attention is paid to leavers and joiners and queries are followed up. Agents' pay is reviewed by pay type against budget and queries followed up. Anomalies are likely to be found through these reviews. The importance of this review will be re-emphasised within the Finance team.	Based on the procedures performed in current year, it was concluded that this process has been improved and the control is now operating effectively.
9	**Employees Joiner Control**	Payroll – Sheffield	Payroll management’s process is that once an employee joiner is added to the system a secondary review is performed and an audit checklist completed to evidence this review. Based on our review, we identified a number of instances where there was no evidence of review of details being entered/removed correctly.	We recommend that the secondary check-sheets are maintained to evidence review of agent joiners and leavers.	This is actioned at Sheffield. Gaps will be closed by end of May and Period 1 picked up retrospectively. The Service Centre team were on site in Sheffield on 26th May to confirm audit findings and to look at improvement opportunities which will mirror those from the Service Centre. Currently reviewing our SLA with Sheffield which will be re-worked to	Based on our sample selected, we noted that we were able to obtain secondary check-sheets for our sample selected, and therefore concluded the control to be operating effectively.

			Without adequate review agents may be input twice, at the wrong pay amount and / or not removed resulting in overpayment.		incorporate a number of areas around controls.	
10	**Multiple Agents in One Location**	Payroll – Bolton	In prior year, management agreed with the recommendation to re-introduce the control and maintain evidence of the review of the branches which have more than one agent payment if a month, being performed. From our review this year, there is limited evidence of the review being performed for the months selected for testing. The risk of more than one salary being paid for each location is higher if this control is not in place. This then increases the risk of fraud or cash payments being made to individuals that need to be reclaimed, with the added administrative expense required.	We recommend the evidence of review is strengthened in order to support the control.	This was in place from Period 12. The front facing sheet has been enhanced to include greater detail of the work performed and any resolution of issues. This is signed by the complier and manager following a review of the work performed	We noted that for the sample selected, we saw evidence of explanations, follow up actions and review being carried out on reports produced and clear evidence of sign off.
11	**Overall Payroll Control Environm**	Payroll – Bolton	Whilst there have been some limited improvements in the control environment during the current financial year, we were again unable to rely on a	We recommend a stronger focus on the payroll control environment in terms of senior management oversight, including obtaining a better understanding of the	In overall terms it is agreed that there needs to be a greater profile around the whole area of controls. A number of actions have now been agreed by the management team and are in	We noted significant improvements in the overall control environment during our review of controls in 2010/11. It is evident that

	ent		number of key payroll controls to reduce our substantive work for the year-end audit. Further, during the course of our work we identified areas where controls were not operating as payroll management believed them to operate and where actions included in management's responses to our management letter last year had not been taken or were ineffective in addressing the deficiency identified. We believe this indicates a weakness in the overall control monitoring process. Weaknesses in the control environment may lead to errors in financial reporting or actual losses to the business.	operating effectiveness of the existing controls, encouraging a stronger control culture and more intensive control monitoring going forward.	place for Period 1 including random independent checks and KPIs on the local scorecard and on the overall HR scorecard. In addition the following has taken place / planned to address the overall recommendation and in particular encouraging a stronger control culture and intensive monitoring. Audit recommendations shared with all management team. Briefing to all managers and employees across the Service Centre in relation to on-going audit and controls. Allocation of dedicated resource to assess status of controls across all product teams as a baseline exercise. Full in house audit conducted of all controls detailed in our Internal Control Manual (ICM). Control champions for each product area. Identified gaps from ICM currently being addressed.	there has been a marked effort in order to improve the functioning and oversight of a number of key controls, most of which we now are able to place reliance on and are able to conclude that the overall payroll control environment is effective.

					ICM being updated and will be launched at the end of Quarter 1. Review of closed E&Y recommendations completed for Period 2 and scheduled for full year. Internal audit to conduct further sample checks following launch of revised ICM. All individuals have a performance objective for 2010/11 linked to controls.	
12	**Credence (back end) change process**	IT	During our walkthrough and testing of the change control procedures for the Credence application we became aware of the following issues: 1. Developers at Logica, the third party provider of application development and support for Credence, had access rights to the production environment and the database that would permit developers to move their own changes into the production environment.	Management should require that their third party service provider segregate the roles of developer and implementer. Management should also require that their third party service provider maintain complete and accurate records that support the requests for changes, testing of changes, approval to move into production and the separation of developer and implementer. Management should periodically audit the achievement of service level agreements.	This is clearly documented in OCP. There will be further work to look at requiring Logica to comply and ensure appropriate role separation. To be retested in 3 months.	Application not in audit scope for FY11. Therefore, we are not able to comment on whether management has fully addressed our comment as raised in the prior year.

			2. Documentation to approve fixes and patches that are applied to Credence outside of the release process does not always exist. We were advised by Logica personnel that for a sample of four changes selected evidence of approval to move into production did not exist and that it would not be possible to link the changes to problem tickets to record the original request for the fix / patch. Developers have access to move their own changes into production and documentation is not retained to substantiate those changes there is a risk of loss of data and application integrity due to either unauthorized, erroneous or inappropriate changeng made to the production environment.			
13	**Credence (front end) change**	IT	During our walkthrough of user administration of the front end of Credence we noted several	Changes to Credence should be requested, tested and approved by the business users. Changes	Whilst users are able to make changes to reports they "own", those which are used for business critical	Application not in audit scope for FY11. Therefore, we are not able to comment on

	process		users with administrator rights, including some generic users (this is noted below as a separate point). These users have the access rights to create and amend reports, including those which may be relied upon for audit evidence. These users can change report design, and processing without documented request, test or approval. When users have the rights to change reports that are used by the business for reconciliation, exception reporting or other processing, there is the risk that the reports are manipulated either intentionally or accidentally.	should be identifiable through system logs and an appropriate audit trail maintained of request, testing and approval documentation, Access to make such changes should be limited to authorised individuals.	processes are created globally and owned by one of the administrators. Users may be able to design their own versions of the reports but these would not be available globally, nor used for business critical processes.	whether management has fully addressed our comment as raised in the prior year.
14	**Credence (front end) configuration**	IT	We noted several control weakness in Credence front end user administration and security configuration: 1. The password configuration is not aligned with network settings or those settings required by Post Office. We noted:	Management should enhance password controls on the Credence web portal to the same standards applied to other Post Office environments. Management should consider disabling generic administrator accounts, or assigning the accounts to specific individuals to ensure	Users are not generic, but role accounts which are allocated to individuals and for which an audit trail is available. The correct procedure to be followed for the allocation and use of these roles is being re-emphasised. A full risk assessment of the Credence system	Application not in audit scope for FY11. Therefore, we are not able to comment on whether management has fully addressed our comment as raised in the prior year.

			a. there is no minimum password length b. Password complexity rules are not applied c. users are not required to change their password d. password history is not retained e. idle session time-outs are not in place 2. There are three generic administrator accounts without specific users assigned to these accounts. One of the three accounts has not been used since April 2009. 3. The process for requesting and granting user access rights to Credence does not maintain documentation to record evidence of request or approval of access rights. 4. There is no process in place for the revocation of user access rights when a user separates from the organisation or moves to a new role no longer requiring	accountability over the use of the administrator accounts. Management should consider establishing user administration controls which are in-line with the processes used for other Post Office applications.	is being undertaken later this year and this aspect will be reviewed. Although system-based credential control does not fully match POL standards, user guidelines and procedures do. The whole user management piece is due to be reviewed during the planned risk assessment.	

			5. access rights to Credence. Without effective logical access controls there is the risk of inappropriate or unauthorised access to the Credence reports.			
15	**Horizon (back end) user administration**	IT	During our testing of the appropriateness of users with access to the Horizon back end environment we noted one user whose access was no longer required due to a change in job responsibilities. When users have access to environments which are not appropriate for their job function there is the risk that users may inappropriately or accidentally use the access leading to loss of application or data integrity.	Post Office management should request periodic evidence from Fujitsu that demonstrates that the user population with access to the Horizon environment has been reviewed and access validated. Additionally, Post Office should consider requesting Fujitsu to establish controls relating to temporary access.	A note has been sent to Fujitsu on their responsibilities in this area. Although the note has been sent to Fujitsu, it is likely this will be covered in their up-coming ISO27001 audit and compliance work. This is going to be an agenda item on the monthly ISMS and considered for inclusion in monthly reporting.	Whilst Horizon has been upgraded to HNGX during the audit period, this issue is still relevant for the HNGX estate based on procedures performed in the current year. Refer to #5 in the current year recommendations section.

3. Current Year Recommendations – non IT related

	Issue	Location	Background	Recommendation	Management Comment
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.	Agreed We have continued to strengthen the review of old purchase orders to validate the GRNI accrual and will maintain focus on this review. The system and process are group led but we note the opportunity to improve after separation,
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 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	We recommend that HR reviews the results of the trial run of the employee asset check and ensure that 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.	Agreed a) Employees – the final verification of our structure will in effect 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

			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.		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.
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 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.	We recommend that the change from a "contractual" change request to a "non-contractual" change request 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.	Agreed – Now in place a) Additional column has now been included on our spreadsheet to 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.
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	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 Control Manual so should

			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 adequate review of the process is occurring and that the leaver is correctly removed from the system to avoid overpayment.		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 all variances identified that period which will form part of the team leader sign off.

4. Current Year Recommendations – IT Specific

Ref	Observation	Location	Background	Recommendation	Management Comment
1	Improve governance of outsourcing application management *Rating: High*	IT	The outsourcing of Post Office Limited's (POL) IT function to a third party service provider (Fujitsu) creates a degree of complexity and difficulty for POL in gaining assurance that there are adequate IT general controls in place around POL's business critical systems. This is further complicated by the changes within Fujitsu's support structure whereby certain functions within the RMGA business unit have been further outsourced internally to shared services provided by Fujitsu. This second layer of the outsourcing arrangement further increases the complexity and difficulty of gaining assurance that adequate IT general controls are in place and operate effectively. Despite the outsourced IT environment, POL is responsible for the governance, risk and control framework over its business critical systems, and should have visibility and assurance over their design and operating effectiveness.	Whilst we do recognise that the current outsourcing model has been pursued to successfully deliver very significant commercial benefits to POL, there is a need to implement additional governance measures to reflect the shared service nature of Fujitsu's provision. We recommend that POL's approach to this should include the following: POL should take ownership of the effectiveness of the control environment with Fujitsu, requiring Fujitsu to implement a control framework devised by POL (including standards and requirements) and to provide assurance (independent or otherwise) over its continued effective operation Whilst Fujitsu has indicated that the provision of an ISAE 3402 (formerly SAS70) report would be excessively costly and the preference within POL at present is to focus on improving the existing audit process going forward, POL should keep the ISAE 3402 option under consideration over time, as there are indications that Fujitsu will adopt an increasingly global approach to service provision, further	Work on improving the governance of outsourcing with Fujitsu has already commenced and we have already established an approach. Regular meetings underway and plans to share the approach with E&Y by July 2011. Application of control reviews will be monitored through an Audit Control Governance Board fed by the regularly scheduled embedded BAU interactions with Fujitsu. This governance board to be established by July 2011. Monitoring controls and measures will be defined between POL and Fujitsu for embedded BAU management purposes. The POL and Fujitsu approach is an optimised control framework to manage controls and evidence requirements (see point 1 above)

				complicating the process of gaining audit evidence.	
2	Segregation of duties within the manage change process *Rating: High*	IT	We reviewed the logical and organisational controls in place to segregate the development and migration of changes as part of the review of the manage change process for all applications in scope. Our examination of this process revealed the following: <u>POLSAP</u> The transport selected for our walkthrough was implemented by a user (NAVEEDM01) who was also identified to have access to the development environment via DEVACCESS in the development environment; 20 active SAP accounts with access to develop changes (via DEVACCESS in the development environment) and access to release transports into production (users with access to STMS in the production environment); and 10 out of 29 accounts were identified to have inappropriate access to STMS in the production environment. Specifically: o Three accounts belonging to terminated Fujitsu employees whose access to POLSAP was no longer required; o Seven accounts belonging to CSC	The following improvements are recommended: Developers should not be given access to migrate changes to production to minimise the risk of developing unauthorised changes and promoting these changes to the live environment. As such a review of access to release changes into the POLSAP (via STMS) and HNGX (via TPM, TCM and active directory) production environment is required to determine whether developers require access to migrate changes. The review should also assess whether access to deploy is appropriate based on the user's job responsibilities. A review of appropriateness of access to the terminals used to send changes from Dimensions/PVCS to the DXE server as part of the deployment process to the live HNGX estate should also be performed; All inappropriate access as a result of the review should be revoked. If it is determined that developer access is	A Fujitsu project has been established to review all user management areas and is being led by the CISO of the RMG account. Fujitsu will provide and agree with POL a clear segregation of duties guideline for Senior Management and Line managers/Assignment managers to ensure that development and test are clearly separated from live in all technological and staff areas. If it is not possible to do this then risks identifying why this is not the case should be documented and assessed and communicated to POL for agreement. Third parties including other parts of Fujitsu outside of RMG BU also should have obligations upon them to ensure the segregation of Development and Test systems, a review by Fujitsu of OLA's, SLA's , NDA's and Contractual agreements is required to ensure adequate

			o users that were no longer required; Whilst we obtained confirmation from the POLSAP Programme Manager at Fujitsu that the remaining accounts with access to STMS were appropriate, we identified five users with access to DEVACCESS in the development environment who also promoted a total of 30 transports into the production environment from the period between 01/04/2010 to 26/11/10. HNGX Three developers out of 36 user accounts were identified to have access to deploy changes manually to the HNGX live estate via privileged access within active directory. Whilst we confirmed with their manager that access is required for their support roles, we were unable to obtain authorised documentation to support the last login activity for each user; There are an excessive number of accounts with access to deploy automated changes to the live HNGX estate via the Tivoli Provisioning Manager (TPM) and Tivoli Configuration Manager (TCM) tools. We also identified inappropriate access to deploy automated changes to HNGX via TPM and TCM. Specifically: o We noted 122 accounts with access to deploy automated counter changes via	required, evidence to support the request and authorisation to grant developers access to promote changes should be retained. A control should be implemented to monitor the use of accounts that are used to deploy changes manually to the live HNGX estate and evidence to support this control should also be retained; and Implementing a change monitoring control for the in-scope applications whereby system generated list of changes made to production are independently reviewed by POL on a periodic basis to determine that changes have been authorised, tested and approved prior to migration. This will help POL gain assurance that changes implemented by third party service providers have been approved by POL management. Management should implement monitoring controls to help ensure that controls operated by third party service providers are in place and are in operation for example, monitoring	control. POL is to ensure through a periodic sample and exception review that changes have been authorised tested and approved prior to deployment. (see ref 1)

			o TCM; o We noted 114 accounts with access to deploy automated back end changes via TPM; o 11 out of 25 sampled accounts tested were identified to have inappropriate access to the TPM and TCM due to the following reasons: ▪ Access was not revoked for nine terminated Fujitsu employees; ▪ Access was not revoked for one user that had left the Fujitsu RMGA account; ▪ Access was not appropriate for one user based on his job responsibilities. The EUROPE\Domain Admins active directory group was identified to have inappropriate access at the operating system level to the terminals used to send changes from Dimensions/PVCS to the DXE server as part of the process to deploy changes to the HNGX live estate. Refer to Appendix A for detail of the accounts identified to have inappropriate access to POLSAP and HNGX.	that there are no developers with access to promote changes to production.	

			There is an increased risk of inappropriate/unauthorised programme changes being migrated to production if there are inappropriate users with access to deploy and/or users are granted with access to both develop and deploy into production. This risk of inappropriate/unauthorised changes remaining undetected is enhanced as there is no control in place to perform an independent periodic review of a system generated list of all changes migrated into the POLSAP and HNGX production environment to determine that changes have been authorised, tested and approved prior to migration.		
3	Strengthen the change management process *Rating: High*	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 all applications in scope. Our examination of this process revealed the following: <u>POLSAP</u> Based on a testing sample of 18 changes made to the POLSAP production environment during the audit period we were unable to obtain evidence of the following: o Authorisation prior to development for five changes; o Testing for nine changes; and	Management should enhance the current change management process/policy to include: The level of documentation retained to evidence that POL are involved in testing and approving changes made to the in scope applications. In particular, evidence to support POL and third party service provider's authorization of the change prior to development and POL approving HNGX counter changes prior to deployment across the counter estate should be retained. This will provide management reasonable assurance	Work has commenced on the strengthening of the change management process. Centralisation of approvals for change for POL within Fujitsu is to be established, which is accessible to all relevant staff and is to be applied throughout the development, testing and release process to evidence POL approval at each stage. Classification of maintenance and fix changes, and responsibilities and

			o POL approval prior to implementation for four changes. For one of these changes POL approval was not required per the Fujitsu process as the nature of the change was a configuration change and as such internal approval within Fujitsu was deemed to be appropriate. HNGX Based on a testing sample of 15 back end changes, ten counter changes and five manual changes deployed to the HNGX live estate during the audit period we noted the following: o For 15 back end changes, ten counter changes and five manual changes, evidence of testing by POL was not retained; o For ten counter changes, evidence of POL approval of the change to be deployed across the counter estate was not retained; o For one manual change, evidence of POL authorisation to begin development (i.e. a signed off CT document) was not retained; and o For one manual change, approval was not obtained from POL prior to the change being implemented.	that program changes being implemented into the production environment have been tested and approved prior to deployment and that HNGX counter changes are approved prior to roll out to all counter/branches. Please note that all documentation should be retained; Definitions of the responsibilities of all parties involved in the authorization, 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 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; and Management should implement monitoring controls to help ensure that controls operated by the third party service providers are in place and are in operation.	control levels required are to be agreed between POL and Fujitsu. POL is to ensure management and control of this change process through the embedded BAU process to ensure the correct level of engagement for user testing. Regular joint sessions are required to ensure that the change management principles are being applied. POL to review the current BAU governance to ensure the change management principles are being applied and monitored	

			All in-scope applications We noted that POL are not usually involved in testing fixes or maintenance changes to the in-scope applications; We were unable to identify an internal control with the third party service provider to authorise fixes and maintenance changes prior to development for the in-scope applications. 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.		
4	Review of privileged access *Rating: High*	IT	We reviewed privileged access to IT functions including access to user administration functionality across all in-scope applications and their supporting infrastructure. Our examination revealed: POLSAP The following eight dialog and service accounts were identified to be assigned to the SAP_ALL and SAP_NEW profiles: o ADMINBATCH o BASISADMIN	We recommend that management conducts a review of privileged access to IT functions across all 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	A Fujitsu project has been established to review all user management and is being led by CISO for the RMG account (see ref 2) Fujitsu will cascade to all areas of the account to advise them of the process for new joiners, movers and leavers and will ensure appropriate compliance. Reporting and evidence to be

			o DDIC (SAP_ALL only) o OTUSER o OSS508140 o SAP* o SOLMANPLM500 o WF-ADMIN Users with SAP_ALL access allow unrestricted access to POLSAP including the capability to process and approve financial transactions. The SAP_NEW profile provides general access to any new profiles and authorisations which are included in a new SAP release. The SAP* account was not locked. This does not meet recommended practice of removing all profiles from SAP* and locking the account. <u>HNGX</u> 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	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 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.	agreed (see ref 1) regarding BAU reports of Privileged Access abuse to provide POL with the assurances they require. As part of the embedded BAU process management will review adequacy and regularity of the controls in place.

			HNGX: o System privileges assigned to the APPSUP role and OPS$TPS account are inappropriate; o The following accounts associated to the DBA role are no longer required: ▪ CFM_DBA ▪ SPLEX_ROLE_BOTH o The following accounts have inappropriate access to user administration functionality via the Admin access parameter ‘ADM is set to yes’: ▪ OPS$TPS ▪ SPLEX_ROLE_BOTH Refer to Appendix B for detail on the accounts identified to have privileged access to POLSAP. Unrestricted access to privileged IT functions increases the risk of unauthorised/inappropriate access which may lead to the processing of unauthorised or erroneous transactions.		
5	Implement periodic user access reviews	IT	We noted that there is currently no process to review POLSAP user accounts or HNGX back end user accounts on a periodic basis to determine that	Management should consider the implementation of a POL owned periodic review of appropriateness of access to in-	A Fujitsu project has been established to review all user management and is being led by

	and monitoring controls *Rating: Medium*		user access is appropriately granted given the job responsibilities. As a result, our review revealed the following: Two out of a sample of 25 active directory accounts belonged to terminated employees whose access to the HNGX estate was no longer required; and One account out of a sample of 25 active directory accounts have inappropriate access to the ikey-exemptou-users active directory group within HNGX. We also noted that there is no process to monitor privileged access to POLSAP and HNGX on a periodic basis. Specifically: Whilst we noted that there was a monitoring control in place for privileged access to POLSAP whereby accounts associated to the SAP_ALL profile are reviewed and monitoring of failed and successful login attempts for SAP*, DDIC and BASISADMIN accounts is performed, this control does not include accounts associated to the SAP_NEW privileged profile. As part of our walkthrough, we also noted that there was no POL representative present for the December monthly security meeting where the documentation supporting the monitoring	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 terminated users with continued access to the financial 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; and 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	CISO for the RMG account (see ref 2). Fujitsu will review User Management Process SVM/SEC/PRO/00012 RMGA User Management Process Guide and SVM/SEC/PRO/0006 RMGA Application for Access to the Live Network to ensure that the requirements are documented. Fujitsu senior management to include responsibilities on all Line managers/Assignment Managers to review rights of their staff and their appropriateness every quarter. Quarterly BAU Assurance reports to POL concerning reviews that have occurred across the account will be governed by the Audit Control Governance Board.

			controls are reviewed; and There are no monitoring controls in place for privileged IT access to HNGX. Furthermore, we were unable to obtain evidence of the quarterly review of access to the data centre housing the infrastructure supporting POLSAP and HNGX. Refer to Appendix C for accounts identified to have inappropriate access to HNGX. 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.	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 whether changes are required (responses should be provided whether changes are required or not); and 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 the following: Expanding the scope of the	

				current monitoring control for POLSAP to include accounts associated to the SAP_NEW profile; 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 facilitate the audit of these processes.	
6	Strengthen the User Administration Process *Rating: Medium*	IT	Our examination of the user administration process implemented for all applications in scope revealed the following: <u>POLSAP</u> We noted that the existing user administration process for the granting, modification and removal of Supply Chain users access to POLSAP do not include Cash Centre staff. In addition, we confirmed that POL Cash Centre managers are granted limited access to user administration in POLSAP via 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;	The following improvements are recommended: Reviewing the current logical access policy to include definitions of the responsibilities of all parties involved in the user administration process. The policy should also include a description of the overall user administration process; Strengthen the existing user administration process implemented within POL and with the third party service providers so that documentation supporting the request, approval and setup/removal of access are retained for all applications in-scope;	A Fujitsu project has been established to review all user management and is being led by CISO for the RMG account (see ref 2). Fujitsu will review User Management Process SVM/SEC/PRO/00012 RMGA User Management Process Guide and SVM/SEC/PRO/0006 RMGA Application for Access to the live network to ensure that the requirements are documented (see ref 5). Third parties including other parts of

			From our sample of 25 profile additions on POLSAP we noted the following: o For 24 users we were unable to obtain evidence to support the level of access requested and that the access had been authorised by an appropriate individual. From these users we noted that three (3) of these users' access was granted and authorised by CSC with no involvement from POL; and o For 14 users we noted that the Cash Centre line manager providing confirmation of appropriateness of access has limited access to user administration functionality via access to SU01. <u>HNGX</u> The "Change of Access to Live Network" form for the modified user selected for our walkthrough was not authorised by a line manager prior to the request being actioned; From our sample of nine active directory user accounts created during the audit period we noted the following: o One instance of access being requested via a TFS call rather than via	<u>POLSAP</u> Review the current user administration process for POLSAP business users to incorporate Cash Centre users. As part of this review, determine how segregation of incompatible duties can be maintained within the user administration process. Where segregation of duties is impractical, management should consider implementing a monitoring process around the activities of privileged users (i.e. Cash Centre managers with access to SU01); <u>HNGX</u> Implementing a standard user administration process to include all creations, modifications and removal of access to HNGX; A review of documentation involved in the HNGX user administration process (specifically the access request forms and the AD mapping document) to help ensure that access assigned is consistent with the roles defined in the documentation. In situations, where access requests are not defined in the AD mapping document or request forms, management should ensure	Fujitsu outside of RMG BU also should have obligations upon them to ensure user administration is in place, therefore a review of OLA's, SLA's , NDA's and Contractual agreements is required by Fujitsu to ensure this. Quarterly BAU Assurance reports to POL concerning reviews that have occurred across the account will be governed by the Audit Control Governance Board (see ref 5). Post Office is currently reviewing segregation of duty activities within the cash centre system administration processes. Processes policies and guidelines will be produced and monitored on a regular basis.

			o an access request form per the standard user administration process; o Three instances of additional access being granted to a user without supporting evidence; o One instance of a system account being granted inappropriate access to the “pathways” active directory group. Refer to Appendix D for detail on the accounts outlined above. 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 unauthorized/unnecessary access to systems. Furthermore, this risk is enhanced by inadequate segregation of duties between the approval and setup of access.	that evidence to support authorisation of any modifications to access is retained. 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.	
7	Improvements to logical security settings *Rating: Low*	IT	We reviewed the logical security settings for the infrastructure supporting all applications in scope. Our examination revealed the following logical security weaknesses: For the operating systems of the Linux application servers (R3A) supporting the POLSAP application and on the Branch Access Layer (BAL) Linux application servers supporting HNGX: o We noted that there is no setting in	Management should consider the following: Restricting root login to the console on all Linux servers supporting the in-scope applications; Disallowing non-local login to privileged accounts on all Linux servers supporting the in-scope applications;	A technical architectural review of all applications, operating systems and access and authentication tools is to be undertaken by Fujitsu and findings and recommendations will be shared with POL. Fujitsu will perform a periodic scan of passwords to be made as part of a regular Pen Test Exercise.

			o place to restrict root login to the console; o We noted that there is no setting in place to disallow non-local login to privileged accounts. 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. Within the Active Directory server controlling access to the HNGX estate (ACD), we noted that the default Administrator account exists. Inadequate system security settings increase risk of unauthorised access to financial data.	Setting an encrypted password for the LISTENER.ORA file on all Oracle databases supporting the in-scope applications; Disable the default Administrator account and create a new Administrator account with a strong password. Management should consider implementing monitoring controls to help ensure robust security settings are in place particularly those operated by third party service providers.	Findings and exceptions outside of best practice to be raised at the regular embedded BAU monitoring sessions within the existing BAU governance process within POL and to be supported by the Audit Control Governance Board.
8	Strengthen the password parameters *Rating: Low*	IT	We reviewed the password configurations for all in scope applications and the infrastructure supporting these applications. Our examination revealed: There are password setting weaknesses within the RMGA Information Security Policy: o Number of passwords that must be used prior to using a password again is defined as 'Re-use of the same	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 are still recommended to further strengthen the control environment a) Review and update the 'RMG	The SVM/SEC/POL/0003 RMG BU Security Policy requires amendment to section 11.2.5 in the next review subject to architectural agreement. Any risks for non compliance to be identified and communicated to POL. Fujitsu will cascade to all users,

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>o password must not be permitted for either a specified time or until at least 4 other passwords have been used'; and
o 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:
o Minimum password length is 6 characters. This does not meet RMG Information Security Policy guideline of a minimum of 7 characters;
o Idle session time out is set to 3600 seconds. This does not meet the recommended setting of 1800 seconds or less;
o 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) :
o Minimum password length is 5 characters. This does not meet RMGA Information Security Policy guideline of a minimum of 7 characters;</td>
<td>b) Information Security Policy' to meet the recommended good practice password settings outlined below.
c) Configure all network, application and supporting infrastructure components in line with the policy requirements.
<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 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</td><td>Enabled</td></tr>
</table>
</td>
<td>especially SAP and Linux to advise them of the policy and guidelines, and will ensure appropriate compliance.
Monitoring and communication will be provided to POL through the regular embedded BAU process to ensure access control management is robust.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>
o Maximum password age is set at 99999 days. This does not meet RMGA Information Security Policy guideline that passwords must expire in 30 days;
o Minimum password age is set to 0 days. This does not meet the recommended setting of 1 day;
o Account lockout after failed login attempts is not set. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts;
o Password history is not set. This does not meet the recommended setting of 5 passwords; and
o 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:
o 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;
o Account lockout reset counter is set to
</td>
<td>
<table>
<tr><td>password
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>
</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></td>
</tr>
</table>

			o 30 minutes. This does not meet the recommended setting of 60 minutes; and o 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 : o Minimum password length is not set. This does not meet the RMGA Information Security Policy guideline of a minimum of 7 characters; o Password composition is not set. This does not meet the RMGA Information Security Policy guideline of alphanumeric; o Frequency of forced password changes does not meet RMGA Information Security Policy guideline of 30 days or less; o The number of unsuccessful log on attempts allowed before lockout is set		

			o to set to 10. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts; o Account lockout duration is not defined. This does not meet recommended practice of at least 5 days; o 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; and o Idle session timeout is not set. The does not meeting the recommended setting of 30 minutes. Refer to Appendix E for actual, recommended and policy requirement settings for the above listed applications, operating systems and databases. Weak password settings increase the risk of unauthorised access to financial data.		
9	Review of generic privileged accounts *Rating: Medium*	IT	As part of our review of privileged access to all in-scope applications and their supporting infrastructure we noted multiple generic privileged accounts where knowledge of the password to these accounts is shared between individuals:	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 accounts to promote accountability.	A Fujitsu project has been established to review all user management. This is to include all system/s, accounts and privileges (see ref 2).

			We determined that the password to the privileged SYSTEM account on the Oracle database on the BDB server and DAT servers supporting HNGX is known to 4 of the 12 members of the IRE11 TST DBA team. We also noted that the SYSTEM account on the XID and R3D servers supporting SAP XI and POLSAP applications is known to the SAP Basis team; We determined that 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 4 of the 12 members of the IRE11 TST DBA team respectively. The DBA account on the XID and R3D Oracle database servers supporting the SAP XI and POLSAP applications is known to the SAP Basis team. We determined that the password to the privileged SYS default account on the Oracle database on the BDB and DAT servers supporting HNGX is known to 4 of the 12 members of the IRE11 TST DBA team respectively. The SYS account on the XID and R3D Oracle database servers supporting SAP XI and POLSAP applications is known to the SAP Basis	Management should consider implementing monitoring controls to help ensure robust security practices are in place particularly those operated by third party service providers.	Monitoring and communication will be provided to POL through the regular, embedded BAU process to ensure access control management is robust. (see ref 8)

			team. We determined that the password to the following accounts with the SAP_ALL privileged profile on POLSAP was known to the 4 members of the Fujitsu Basis Consultants team: o ADMINBATCH o BASISADMIN o OTUSER o SOLMANPLM500 We determined that the password to the default privileged Administrator account on the Active Directory server controlling access to the HNGX estate was known to the 10 members of the IRE11 NT team; and The use of generic accounts prevents the accountability of its use from being determined and can lead to unauthorised access to financial data.		
10	Improvements to the problem and incident management process *Rating: Low*	IT	We reviewed the processes implemented to determine that problems and incidents are identified, resolved, reviewed and analysed in a timely manner for all in-scope applications. Our examination of these processes revealed the following:	Management should consider a regular review of the problem and incident management process to ensure that problems and incidents are correctly classified and resolved in a timely manner.	Agreement of the classification and timescales for the identification, resolution, review and analysis of incidents is to be documented in a review of SVM/SDM/PRO/0001 and SVM/SDM/PRO/0018 Incident Management processes.

			Two out of five problems were incorrectly classified as problems when they should have been raised as incidents. We also noted that they were not resolved in a timely manner. There is an increased risk of disruption of key business operations if problems and incidents are not classified correctly and not resolved, reviewed and analysed in a timely manner.		As part of the regular embedded BAU process POL will sample review classification of problems and incidents to ensure they are correctly classified. This will be subject to a six monthly review.