Post Office Limited

IT component of management letter for the year ended 25 March 2012

ERNST & YOUNG
Quality In Everything We Do

POL00029485

1. Overview

The table below lists the IT observations identified during the audit. Further details are contained in the tables on the following pages. As Post Office management reviews these observations, management should assess the collective impact of these observations, together with other findings from within the organisation.

Control observations
1. Privileged access
2. User administration process
3. Change management process
4. Periodic user access reviews and monitoring controls
5. Generic privileged accounts
6. Password parameters
7. Logical security settings

POL00029485

2. Detailed observations

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 release. • The SAP* and DDIC accounts were not locked. This does not meet recommended practice of removing all profiles from SAP* and locking both	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 and SAP_NEW access, it is recommended that a periodic review of the activities executed by the accounts granted permanent SAP_ALL and	

			• 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. Refer to *Appendix A* for detail on the accounts identified to have privileged access to POLSAP. HNGX 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: 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	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.	

			○ 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.		
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 being adhered to.	

			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. • 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	• 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.	

			o cash centre modifications which took place after this date, we noted that this form had not been retained. o 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. Refer to *Appendix B* for details of the accounts noted 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 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.		
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	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	

			: POLSAP 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 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. HNGX	• 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 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.	

			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 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.		
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.	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	

			HNGX Whilst we have been advised that there is a new process 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 (refer to *Appendix C*). POLSAP 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.	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 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: o Whether the current access of their employees is in line with their job role o 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: o Emails to managers requesting responses o Responses from managers detailing whether changes are required (responses should be	

				○ provided whether changes are required or not) ○ 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.	
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: • 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	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. Management should also consider implementing monitoring controls to help ensure robust security practices are in place particularly those operated by third party service providers.	

			• 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 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		

POL00029485

			○ 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.		
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. 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:	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 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	

- 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:
  - 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

c) privileged accounts on the Oracle database and Linux operating system

Password setting	**Recommended configuration**
Minimum password length	6 - 8 characters
Complexity	Alphanumeric including special characters and upper/lower case
Frequency of forced password changes	90 days or less
Number of passwords that must be used prior to using a password again	5 (Should be higher if passwords changed more frequently)
Initial log-on uses a one-time password	Enabled
The number of unsuccessful log on attempts allowed before lockout	3 – 5 invalid attempts
Account lockout duration	Forever until manually unlocked

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>o 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
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 30 minutes. This does not meet the recommended setting of 60 minutes
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)</td>
<td><table>
<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></td>
</tr>
</table>

			• 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 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 for the Oracle database 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 o Idle session timeout is not set. The does not meeting the recommended setting of 30 minutes Refer to *Appendix D* for further details. Weak password settings increase the risk of unauthorised access to financial processing and data.		
7	Logical security	IT	Our review last year of the logical security settings for the infrastructure supporting the applications in	Management should consider the following:	

	settings		scope identified certain logical security weaknesses. From our review this year, we noted that these weaknesses are still 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.	• Setting an encrypted password for the LISTENER.ORA file on all Oracle databases 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.	

POL00029485

Appendix A Review of privileged access

The following observation was noted as a result of our review of privileged access across all in-scope applications:

Application: POLSAP

The following 7 dialog and service accounts were identified to be assigned privileged profiles:

User ID	Valid from date	Valid through date	User Type	User group	User Lock	Last Logon Date	Last logon time	Privileged Profiles
ADMINBATCH	03.07.2008	31.12.9999	A	SUPER	0	18.12.2011	07:12:13	SAP_ALL, SAP_NEW
BASISADMIN	03.10.2008	31.12.9999	A	SUPER	0	20.12.2011	19:26:20	SAP_ALL, SAP_NEW
DDIC	25.06.2008	31.12.9999	A	SUPER	0	08.03.2010	09:17:27	SAP_NEW, S_A.SYSTEM
OTUSER	29.04.2010	31.12.9999	S	SUPER	0	24.03.2011	10:47:55	SAP_ALL, SAP_NEW
SAP*	25.06.2008	31.12.9999	A	SUPER	0	12.05.2011	00:00:00	SAP_ALL, SAP_NEW
SOLMANPLM500	12.03.2010	31.12.9999	S	SUPER	0	20.12.2011	19:23:59	SAP_ALL, SAP_NEW
WF-ADMIN	20.11.2007	31.12.9999	A	SUPER	0	10.08.2005	09:18:25	SAP_ALL, SAP_NEW

POL00029485

Appendix B Strengthen the user administration process

The following observations were identified as a result of our review of the user administration process across the in-scope applications:

Application: POLSAP

The following 24 POL cash centre managers have limited access to SU01:

SAP ID	Name, Job Title	User Group
ADAMSD02	David J Adams, Processing Manager	ETNA HOUSE
ALEXS01	Savarimuthu Alex, Processing Manager	ETNA HOUSE
BAILIER02	Robert Bailie, Processing Manager	BELFAST
BOORAP01	Palbinder Boora, Processing Manager	BIRMINGHAM
BROWNE03	Eric Brown, Processing Manager	GLASGOW
CONLONP02	Pat Conlon, Processing Manager	HEMEL_BUREAU
CURRIEE01	Eileen Currie, Processing Manager	BELFAST
DENTONP01	Paul Denton, Processing Manager	LEEDS
FLYNNB01	Bryan Flynn, Processing Manager	MANCHESTER
FLYNNC01	Chris Flynn, Processing Manager	MANCHESTER
GRAVENJ02	John Graven, Processing Manager	MANCHESTER
GREGORM02	Michael Gregory, Processing Manager	ETNA HOUSE
HOWARDS07	Steve R Howard, Centre Manager	HEMEL_BUREAU
HUGHESM01	Martyn Hughes, Processing Manager	BIRMINGHAM
IRWINS02	Simon Irwin, Processing Manager	POL 1254
MCINTOJ01	John McIntosh, Processing Manager	GLASGOW
MONKR01	Richard Monk, Processing Manager	HEMEL
MONKR02	Richard Monk, Processing Manager	HEMEL_BUREAU
PARMARD01	Daksha Parmar, Processing Manager	MIDWAY
PONTERG01	Gillian Margaret Ponter, Processing Manager	MIDWAY
PRESSLM01	Martin Pressland, Processing Manager	POL 1254
STEELEM01	Melanie C Steele, Processing Manager	LEEDS
WALLT01	Timothy Wall, Processing Manager	POL 1254
WOOLVEA01	Andrew Woolven, Service Desk Analyst	UK 1111

Application: POLSAP

We noted that the cash centre line manager providing approval or confirmation of appropriateness for the following new and modified users out of a sample of 27 tested had limited access to SU01:

User Name	Full Name	New User or Modification?	Date	Manager Providing Confirmation and also has access to SU01
BROOKSM06	Meg Brooks	New User (POL)	15/11/2011	Patrick A J Conlon, Processing Manager
BANDUNP01	Pradeep Banduni	Modified User (Steria)	23/09/2011	Shanmugam Sundarajan, Offshore User Admin
FIELDID01	Dave Fielding	Modified Users (POL)	13/06/2011	John Graven, Processing Manager
HAYWOOW01	Wendy R Haywood	Modified Users (POL)	31/10/2011	Daksha Parmar, Processing Manager
HOLMESM04	Max Holmes	Modified Users (POL)	08/06/2011	John Graven, Processing Manager
ILLUNGY01	Yakalu Ilunga	Modified Users (POL)	26/04/2011	Steve Howard, Bureau de Change & Coin Centre Operations Manager
LAWSOND01	Douglas Lawson	Modified Users (POL)	27/07/2011	Eric Brown, Operational Support Manager, Glasgow Cash Centre & Glasgow CViT Depot
MARTINI01	Ian Martin	Modified Users (POL)	29/09/2011	Daksha Parmar, Processing Manager
MCALLIG01	Gordon McAllister	Modified Users (POL)	17/10/2011	Eric Brown, Operational Support Manager, Glasgow Cash Centre & Glasgow CViT Depot
MCNEILH01	Helen McNeil	Modified Users (POL)	23/09/2011	Eric Brown, Operational Support Manager, Glasgow Cash Centre & Glasgow CViT Depot
MONTVIR01	Ruta Montvidaite	Modified Users (POL)	12/09/2011	John Graven, Processing Manager
OATESG01	Gail Oates	Modified Users (POL)	22/09/2011	John Graven, Processing Manager
PANTLIS01	Sharon Pantlin	Modified Users (POL)	15/09/2011	Timothy Wall, Processing Manager
ROSSIA01	Angela Rossi	Modified Users (POL)	26/08/2011	Timothy Wall, Processing Manager
ADMEDM04	Mohammed Ahmed	Modified User (POL)	08/08/2011	Timothy Wall, Processing Manager
BROCKED01	David Brockett	Modified User (POL)	25/07/2011	Eric Brown, Operational Support Manager, Glasgow Cash Centre & Glasgow CViT Depot
WILLIAJ11	Jennifer Williams	New User (POL)	25/10/2011	John Graven, Processing Manager

Application: POLSAP

Based on our sample of 25 new and modified user access requests to the POLSAP application we noted:

- For the following cash centre user modification, which took place after the new process was implemented on 01/10/11 whereby a form is required to authorise the temporary assignment of roles to cash centre users, this form was not retained:

User Name	Full Name	Job Title
HAYWOOW01	Wendy Haywood	Midway Cash Centre

- For the following cash centre user access 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:

User Name	Full Name	Job Title
PANTLIS01	Sharon Pantlin	London East Cash Centre

Application: POLSAP

Based on our walkthrough of the removal of access process for the POLSAP application, we noted that access to POLSAP was not revoked until over 3 months after the termination date of the following leaver:

User Name	Full Name	Job Title
ALLCOCJ01	John Allcock	CHD, Birmingham Merlin Coin

Application: POLSAP

Based on our reconciliation of the Fujitsu and Post Office terminated employee listings to the POLSAP user listing we noted the following four terminated employees' whose user accounts remained active:

User Name	Full Name	Job Title
Keith Spencer	SPENCEK01	Customer Service Consultant
Stuart Moore	MOORES04	Dartford CIT Manager
Robin Hayes	HAYESR01	Birmingham CIT
Vijay Samplay	SAMPLAV01	North Inventory Team

Application: HNGX

Based on our walkthrough of the new user, modified user and removal of access processes on the HNGX estate, we noted the following:

- No evidence to support the authorisation for the creation of the following new user account:

User ID	User Name	Job Title	Active Directory Group
aflac01	Alan Flack	Release Manager	SMC Users

- No evidence to support the authorisation of the removal of an Active Directory group membership for the following modified user account:

User ID	User Name	Job Title	Active Directory Group
wbrag01	Wayne Bragg	SSC Support Engineer	MSS

POL00029485

- Access to HNGX was not revoked until four months after the termination date of the following leaver:

User ID	User Name	Job Title	Active Directory Group
jball01	John Ballantyne	SSC Support Engineer	smc technicians ssc SMC Users emdb equipment admin virtualserveroperators

Application: HNGX

Based on our reconciliation of the Fujitsu RMGA terminated employee list to the Active Directory listing controlling access to HNGX, we noted the following:

- Access to HNGX was not revoked for the following leaver:

User ID	User Name	Job Title	Active Directory Group
dwilc01	David Wilcox	Technical Manager	rdt Pathway rdmcgroup

POL00029485

Appendix C Implement periodic user access reviews and monitoring controls

The following observation was identified as a result of our review of appropriateness of user access to the HNGX estate:

Application: HNGX

One out of a sample of 25 Active Directory accounts tested one account belonged to an employee whose access to the HNGX estate was no longer required:

User ID	User Name	Job Title	Active Directory group
Mtong01	Martin Tonge	Customer Solution Architect	SMC Technicians

Appendix D Strengthen the password parameters

We noted the following password weaknesses as part of our review of password settings across the in-scope applications and their supporting infrastructure:

Platform/Technology (Application)	Password Parameter	Recommended Practice	RMGA Information Security Policy	Current Setting
POLSAP (Application Level)	Idle session time out	1800 seconds / 30 minutes	15 minutes	Noted from RSPARAM report via transaction code SE38: rdisp/gui_auto_logout = 3600
R3A/Linux (POLSAP) BAL/Linux (HNGX)	Minimum password length	6 – 8 characters	7 characters	Noted from etc/login.defs file: PASS_MIN_LEN = 5
	Maximum password age	90 days	30 days	Noted from etc/login.defs and etc/pam.d/system-auth files: PASS_MAX_DAYS = 9999
	Minimum password age	1	n/a	Noted from etc/login.defs and etc/pam.d/system-auth files: PASS_MIN_DAYS = 0
	Number of failed login attempts before account lockout	3 - 5 failed login attempts	3 failed login attempts	Noted from etc/pam.d_login file: pam_tally.so is not defined faillog file does not exist
	Password history	5	4	Noted from etc/pam.d/system-auth file: password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
R3A/Linux (POLSAP)	Idle session time out	1800 second / 30 minutes	15 minutes	Noted from etc/profile file: TMOUT is not defined TIMEOUT is not defined
ACD/Windows (HNGX)	Number of failed login attempts before	3 - 5 failed login attempts	3 failed login attempts	Noted from the Password Policy defined in Active Directory: Account lockout threshold = 6 failed login attempts

	account lockout			Account lockout reset counter = 30 minutes
	Account lockout reset counter	60 minutes	30 minutes	
	Account lockout duration	Until administrator reset	Until administrator reset	
R3D/Oracle (POLSAP) XID/Oracle (SAP XI) BDB/Oracle (HNGX) DAT/Oracle (HNGX)	Minimum password length	6 – 8 characters	7 characters	Noted from the DBA_PROFILES table: Password verify function is set to NULL.
	Password Complexity	Alphanumeric including special characters and upper/lower case	Alphanumeric	Noted from the DBA_PROFILES table: Password verify function is set to NULL.
	Password expiry	90 days	30 days or less	Noted from the DBA_PROFILES table: Password_life_time = UNLIMITED
	Number of failed login attempts before account lockout	3 - 5 failed login attempts	3 failed login attempts	Noted from the DBA_PROFILES table: Failed_login_attempts = 10
	Account lockout duration	5 days or less	Unit administrator reset	Noted from the DBA_PROFILES table: Password_lock_time = UNLIMITED
	Password history	5	4	Noted from the DBA_PROFILES table: Password_reuse_max = UNLIMITED
	Idle session time out	30	15 minutes	Noted from the DBA_PROFILES table: IDLE_TIME = UNLIMITED

Appendix E Strengthen the change management process

Application: POLSAP

Based on a testing sample of 17 changes made to the POLSAP production environment during the audit period we noted the following:

- Six changes where the name of the person who performed the testing was not recorded.

Transport	Date	Description
PLDK913168	03/06/2011	AB: CR2223 TT -> POLSAP interface change 170511
PLDK913389	28/10/2011	AB: Trading Statement - Reverse Docs v3.0
PLDK913166	25/11/2011	AB: CMS Billing Undo fix because of master data 120511
PLDK913205	25/11/2011	AB: CMS Bank Holiday change DC 100611
PLDK913427	25/11/2011	AB: Trading Statement line 34 fix
PLDK913263	08/12/2011	FI-FY_Variant_ZL_Local Scheme(by week) till 2015-16

- Four changes where, 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:

Transport	Date	Description
PLDK913323	21/10/2011	AB: CR 2206 Flexible plannig screen changes v1.0
PLDK913342	21/10/2011	AB: CR 2206 Flexible plannig screen changes v2.0
PLDK913398	11/11/2011	BS SJ PR4783843 Auth added to Z:L9999:POESSPROPOSE
PLDK913427	25/11/2011	AB: Trading Statement line 34 fix

- For one change, we were unable to obtain evidence that the change had been authorised by POL or Fujitsu prior to development

Transport	Date	Description
PLDK913263	08/12/2011	FI-FY_Variant_ZL_Local Scheme(by week) till 2015-16

- For one change, we were unable to obtain evidence that it had been approved by POL prior to deployment into the production environment

Transport	Date	Description
PLDK913263	08/12/2011	FI-FY_Variant_ZL_Local Scheme(by week) till 2015-16

Application: HNGX

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) prior to implementation, the name of the member of the POL Change Control team who provided the approval was not recorded.

Baseline	Type	Date	Description
MS_SEC_UPD_W2K3_KB2538814_CONFIG_NA_D001	Back end	03/10/2011	Infrastructure Patches - Microsoft Security Update
RHEL_4_5_32_64_SEC_UPD_NA_D016-D015A	Back end	09/10/2011	Infrastructure Patches - Microsoft Security Update
POA:SOL_10_PATCHES_PRIMEPOWER_GROUP1_CONFIG_NA_D020-D019	Manual	N/A	Infrastructure Security - Anti-Virus update
POA:WIN_TEM_SWPACKAGE_0506_D005-D004	Manual	N/A	Tivoli Endpoint Manager Upgrade
MS_SEC_UPD_XP_W2K3_KB2476687_CONFIG_NA_D001	Back end	03/04/2011	Microsoft Security Update

- For 28 changes we were unable to obtain evidence of testing performed by POL.

Baseline	Type	Date	Description
WIN_NCO_PROBEWIN_CFG_0410_D043	Back End	03/04/2011	Infrastructure Event Monitoring - Configuration Change
MS_SEC_UPD_XP_W2K3_KB2478960_CONFIG_NA_D001	Back End	04/04/2011	Infrastructure Patches - Microsoft Security Update
QVAS_RHL_CONFIG_0300_D005	Back End	01/06/2011	Infrastructure Event Monitoring - Configuration Change
SOP_AV_WIN_APP_95_NA_D012	Back End	03/06/2011	Infrastructure Security - Anti-Virus update
LIVE_PLATFORM_SET_PRODUCT_TAGS_NA_D260	Back End	17/06/2011	Change to branch router configurations
LIVE_PLATFORM_SET_PRODUCT_TAGS_NA_D264	Back End	03/07/2011	Infrastructure Event Monitoring - Configuration Change
SOP_AV_WIN_APP_95_NA_D018	Back End	13/07/2011	Infrastructure Security - Anti-Virus update
LINUX_32BIT_24_ACQUIRE_V820_CONFIG_INT14_D009-D008A	Back End	04/08/2011	Standard Platform Build
MS_SEC_UPD_W2K3_KB2538814_CONFIG_NA_D001	Back End	03/10/2011	Infrastructure Patches - Microsoft Security Update
RHEL_4_5_32_64_SEC_UPD_NA_D016-D015A	Back End	09/10/2011	Infrastructure Patches - Microsoft Security Update
COUNTER_X0500 65_1 (COUNTER_APP 65_1)	Counter	21/09/2011	Counter Release - Multiple Fixes
COUNTER_X0500 65_1 (COUNTER_APP_LIB 65_1)	Counter	21/09/2011	Counter Release - Multiple Fixes
COUNTER_X0500 65_1 (COUNTER_APP_LIB 65_1)	Counter	22/09/2011	Counter Release - Multiple Fixes
CNIM2_APP 61_7	Counter	18/10/2011	Counter Release - Multiple Fixes
COUNTER_APP 68_1	Counter	22/11/2011	Counter Release - Multiple Fixes
COUNTER_APP 68_1	Counter	22/11/2011	Counter Release - Multiple Fixes

COUNTER_X0500 65_1 (COUNTER_DATA 65_1)	Counter	21/09/2011	Counter Release - Multiple Fixes
COUNTER_APP 68_1	Counter	22/11/2011	Counter Release - Multiple Fixes
PROBE_HB UP	Counter	01/07/2011	Netcool monitoring probe
PPINPAD_OPEN 41_2II	Counter	27/07/2011	Pinpad hardware replacement
HNGX_QOS 61_2	Counter	01/07/2011	Maintenance Fix - Quality of Service Monitoring
COUNTER_HOUSEKEEPING 56_1	Counter	27/07/2011	Counter Release - Multiple Fixes
POA:SOP_AV_NT4_APP_NA_D059	Manual	n/a	Infrastructure Security - Anti-Virus update
POA:SOP_AV_NT4_APP_NA_D053	Manual	n/a	Infrastructure Security - Anti-Virus update
POA:SOP_AV_NT4_APP_NA_D047	Manual	n/a	Infrastructure Security - Anti-Virus update
POA:SOL_10_PATCHES_PRIMEPOWER_GROUP1_ CONFIG_NA_D020-D019	Manual	n/a	Infrastructure Security - Anti-Virus update
POA:WIN_TEM_SWPACKAGE_0506_D005-D004	Manual	n/a	Tivoli Endpoint Manager Upgrade
MS_SEC_UPD_XP_W2K3_KB2476687_CONFIG_NA_D001	Back End	03/04/2011	Microsoft Security Update

- For one change we were unable to obtain evidence of testing performed by Fujitsu.

Baseline	Type	Date	Description
POA:SOP_AV_NT4_APP_NA_D047	Manual	n/a	Infrastructure Security - Anti-Virus update

- For one change we were unable to obtain evidence of POL approval prior to implementation in the live environment.

Baseline	Type	Date	Description

POL00029485

SOP_AV_WIN_APP_95_NA_D012	Back end	03/06/2011	Infrastructure Security - Anti-Virus update