FUJ00086945

oung

Post Office Limited

Management letter for the year ended 27 March 2011

ERNST & YOUNG

Quality In Everything We Do

1. Current Year Recommendations

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: ○ Three accounts belonging to terminated Fujitsu employees whose access to POLSAP was no longer required;	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

			○ Seven accounts belonging to CSC 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: ○ We noted 122 accounts with access to	• 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)

			○ deploy automated counter changes via TCM; ○ We noted 114 accounts with access to deploy automated back end changes via TPM; ○ 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: ○ Authorisation prior to development for five changes; ○ 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	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 PO L approval at each stage.

			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.	• management reasonable assurance 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.	Classification of maintenance and fix changes, and responsibilities and 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

			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.		management principles are being applied. POL to review the current BAU governance to ensure the change management principles are being applied and monitored.
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: ○ ADMINBATCH ○ 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

			○ DDIC (SAP_ALL only) ○ OTUSER ○ OSS508140 ○ SAP* ○ SOLMANPLM500 ○ 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. HNGX • 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.

FUJ00086945

			• HNGX: ○ System privileges assigned to the APPSUP role and OPS$TPS account are inappropriate; ○ The following accounts associated to the DBA role are no longer required: ▪ CFM_DBA ▪ SPLEX_ROLE_BOTH ○ The following accounts have inappropriate access to user administration functionality via the Admin access parameter 'ADM is set to yes': ▪ OPS$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: POLSAP • 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

FUJ00086945

			• From our sample of 25 profile additions on POLSAP we noted the following: ○ 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 ○ 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. HNGX • 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: ○ One instance of access being requested via a TFS call rather than	POLSAP • 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); HNGX • 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.

			○ via an access request form per the standard user administration process; ○ Three instances of additional access being granted to a user without supporting evidence; ○ 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: ○ 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.

			○ place to restrict root login to the console; ○ 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: ○ 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.

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>○ password must not be permitted for either a specified time or until at least 4 other passwords have been used'; and
○ 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;</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>Fujitsu will cascade to all users, 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>
<ul>
<li><ul>
<li>Maximum password age is set at 99999 days. This does not meet RMGA Information Security Policy guideline that passwords must expire in 30 days;</li>
<li>Minimum password age is set to 0 days. This does not meet the recommended setting of 1 day;</li>
<li>Account lockout after failed login attempts is not set. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts;</li>
<li>Password history is not set. This does not meet the recommended setting of 5 passwords; and</li>
<li>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.</li>
</ul></li>
<li>There are password setting weaknesses on the Windows 2003 Active Directory Controller supporting HNGX:
<ul>
<li>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;</li>
<li>Account lockout reset counter is set to</li>
</ul></li>
</ul>
</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>

FUJ00086945

			○ 30 minutes. This does not meet the recommended setting of 60 minutes; and ○ Account lockout duration is set to 30 minutes. This does not meet the recommended setting whereby an Administrator is required to unlock the account. • There are password setting weaknesses at the Oracle database level on the database servers supporting POLSAP (R3D)and SAP XI (XID) and on the branch database server (BDB) and transaction processing system server (DAT) supporting HNGX : ○ Minimum password length is not set. This does not meet the RMGA Information Security Policy guideline of a minimum of 7 characters; ○ Password composition is not set. This does not meet the RMGA Information Security Policy guideline of alphanumeric; ○ Frequency of forced password changes does not meet RMGA Information Security Policy guideline of 30 days or less; ○ The number of unsuccessful log on attempts allowed before lockout is set		

			○ to set to 10. This does not meet the RMGA Information Security Policy guideline of 3 failed login attempts; ○ Account lockout duration is not defined. This does not meet recommended practice of at least 5 days; ○ 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 ○ 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)

FUJ00086945

			• 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	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

	Rating: Low		• 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.		Management processes. 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.

2. Prior Year Comments – Update

	Issue	Location	Background	Recommendation	Management Comment	Current Year Update
1	**Credence (back end) change process**	IT	a. 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. 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.	**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.**		Application not in audit scope for FY11. Logica to use named user log on only. These users are administered by the MI team in POL Logica ensure Administrator users use individual login details which are recorded, maintained and reviewed in the Service Delivery forums. All changes,

			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.			fixes and system updates are logged via the Operational Change process and routed to key stakeholders by the Change Control Team. The OCP register is also regularly reviewed and prioritised via the POL / Logica weekly forum. No unauthorised changes take place . All changes go by the OCP route.
2	**Credence (front**	IT	During our walkthrough of user administration of the front end of	Changes to Credence should be requested, tested and approved	Whilst users are able to make changes to reports	Application not in audit scope

	end) change process		Credence we noted several 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.	by the business users. Changes 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.	they "own", those which are used for business critical 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.	for FY11. A new procedure has been implemented across all users (1) MI developers now log on as named users using their named access id. There are four of these with administrator privileges against the named user id (2) A separate CMC admin role is now used for user and operational console management. Owned by Guy Linacre BAU

FUJ00086945

						team manager (3) The BOXI administrator user ID will only be used for override purposes. i.e. when a named admin role is not available to carry out urgent development work All users are granted specific access rights to their own Directorate folders which stop any intentional or accidental manipulation of other directorate's reports. We have also hidden certain

						sensitive areas of the reporting structure where appropriate.
3	**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: 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	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 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.	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 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.	Application not in audit scope for FY11. 1. This is now resolved. Passwords have been assigned throughout the Credence community inline with the business security standards. 2. Redundant accounts have been removed but due to OR this is an on going activity. 3. User access is granted via the SR route which is

			4. documentation to record evidence of request or approval of access rights. 5. 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 access rights to Credence. Without effective logical access controls there is the risk of inappropriate or unauthorised access to the Credence reports.			documented and histories are recorded in Remedy. We also maintain an external log of users and access rights granted. 4. A full sweep of all users' accounts has been made and accounts no longer required have been ring fenced and locked.
4	**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	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	Whilst Horizon has been upgraded to HNGX during the audit period, this issue is still relevant for the HNGX estate

			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.		on the monthly ISMS and considered for inclusion in monthly reporting.	based on procedures performed in the current year. Refer to #5 in the current year recommendations section.

FUJ00086945

Appendix A Segregation of duties in the manage change process

The following issues were identified as a result of our review of segregation of duties in the manage change process across all in-scope applications:

Application: POLSAP

The following 20 active SAP accounts have 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):

SAP ID	Name
IRRELEVANT	Navtej Achall
	Madan Agrawal
	Sundeep Alapati
	User ID for PRISM SAP TCE
	Diane Denis-Warren
	Kshitiz Goyal
	Ben Greenfield
	John Hughes
	Kalpana Kotakonda
	Ramakrishna Mandra
	Dave Marshall
	Eamon McElroy
	Bimal Metha
	Ismail Mohammed
	Mohammed Naveed
	Vishal Rajmane
	Depala Sadanand
	HIMANSHU SINGH
	Peter Tombs
	Ashwin Upadhyaya

Application: POLSAP

The following 10 accounts were identified to have inappropriate access to STMS. Specifically:

- Three accounts belonging to terminated Fujitsu employees whose access to POLSAP was no longer required.
- Seven accounts belonging to CSC users that were no longer required.

SAP ID	Name and Job Title
IRRELEVANT	Madan Agrawal, Fujitsu Basis Team
	CSC Basis Team, CSC access to support POLSAP migration, no longer required.
	Diane Denis-Warren, Fujitsu Basis Team
	Kshitiz Goyal, Fujitsu Basis team
	Kalpana Kotakonda, CSC access to support POLSAP migration, no longer required.
	Ramakrishna Mandra, CSC access to support POLSAP migration, no longer required.
	Eamon Mcelroy, CSC access to support POLSAP migration, no longer required.
	Ismail Mohammed, CSC access to support POLSAP migration, no longer required.
	Depala Sadanand, CSC access to support POLSAP migration, no longer required.
	Himanshu Singh, CSC access to support POLSAP migration, no longer required.

Application: POLSAP

We identified 5 users with access to DEVACCESS in the development environment who also promoted a total of 30 transports into the production environment from the period 01/04/2010 to 26/11/10:

SAP ID	Name and Job Title
IRRELEVANT	Ashwin Upadhyaya, XI Developer
	Navtej Achall, XI Developer
	John Hughes, Xi Developer
	Bimal Metha, XI Developer
	Mohammed Naveed, XI Developer

FUJ00086945

Application: HNGX

The following three developers were identified as having 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:

Name	Active Directory Group	Position	Active Directory Last Login
Andrew Aylward	IS-DBA	Senior Oracle DBA, App Dev and Integration team	31/01/11
Andrew Beardmore	IS-DBA	Senior Software and Solutions Design Architect, App Dev and Integration team	03/11/10
Dave Tanner	Administrators	Technical Design Authority, App Development and Integration team	31/01/11

Application: HNGX

The following 122 accounts were identified to have access to deploy automated counter changes via TCM:

TCM User ID
IRRELEVANT

FUJ00086945

IRRELEVANT

FUJ00086945

IRRELEVANT

IRRELEVANT	

Application: HNGX

The following 114 accounts were identified to have access to deploy automated back end changes via TPM:

User Name	Name
IRRELEVANT	Allen, Aston
	Beardmore, Andy
	Chambers, Anne
	Chambers, Adrian
	Das, Ashrita
	Gibson, Andrew
	Jain, Anjali
	Keil, Andrew
	Thom, Andrew
	Williams, Andrew
	gallacher, Brian
	Brooks, Colin
	Bryson, Chris
	Card, Cheryl
	Dowsett, Clair
	Hawkes, Chris
	Jackson, Clare
	Kell, Chris
	Obeng, Catherine
	Pawashe, Changdev
	Chakraborty, Ratul
	Turrell, Clive
	Yerram, Chandrasekhar
	Allen, Dave
	Anderson, Damien
	Avenall, Darren

FUJ00086945

IRRELEVANT	Cooper, David
	Goad, Dan
	Johnston, David
	Laker, Dave
	McKerrigan, Donald
	Sale, Dave
	Seddon, Dave
	Tremers, David
	Ashford, Ed
	Thomas, Eldhose
	Trueman, Emma
	Griffiths, Ged
	Jennings, Graham
	Maxwell, Gary
	Simpson, Garrett
	Rajashekaraiah, Harsha
	Renwick, Helen
	Bowen, Ian
	Ballantyne, John
	Bradley, John
	Charlton, John
	Diffin, Joe
	Harrison, Joe
	Leskshmidas, Jishnu
	Jonnalagadda, Naresh
	Palanisamy, Jayakumar
	samuel, joshua
	Simpkins, John
	Spencer, Jonathan
	Young, James
	Ashley, Kevin
	Miller, Kevin
	Schlatter, Karen
	Sugoor, Keerthi
	Elliott, Lorraine
	Kiang, Lina
	Machin, Leighton
	Brosnan, Mark
	Conneely, Mike
	Croshaw, Mike
	greene, michael
	Grover, Manoj
	Hobson, Matthew

IRRELEVANT	McCoy, Marie-Claire
	Melpally, Maneesh
	Peach, Mik
	Prasad, Madhukar
	Radhakrishna, Manu
	tabr, m
	Tonge, Martin
	Wright, Mark
	Ganguly, Nilanjana
	Hafeez, Nafasat
	Jonnalagadda, Naresh
	Suseendran, Narayan
	Vincent, Niall
	Otra, Santhosh
	Carroll, Pat
	Ives, Phil
	Johnston, Paul
	Kiggal, Pruthviraj
	mayu, p
	McAtasney, Paul
	Parmar, Rajdeep
	Stewart, Paul
	Variyam, Parthasarathy
	Binnie, Rebecca
	Hawkes, Ryan
	Kuppuramaseshan, Rajaram
	Nagaraju, Rohini
	o'kane, rory
	Rangam, Omkar
	snell01, snell01
	Parker, Steve
	Pinder, Shuan
	Ramalingam, Sathish
	Saha, Saptarshi
	Sahu, Subhendu
	Selwyn, Sarah
	Sur, Sudip
	Wood, Shaun
	Shaik, Anwar
	Atkinson, Tony
	tioappadmin, tioappadmin
	Mullapudi, Vijaya
	Narasaiah, Vinay

FUJ00086945

IRRELEVANT		Ramachandran, Vishnuvardhan
		Bragg, Wayne

Application: HNGX

The following 11 out of twenty five 25 sampled accounts tested were identified to have inappropriate access to the TPM and TCM due to the following reasons:

Tool	User ID	User Name	Reason
TCM	IRRELEVANT	Chloe Bardell	Access was not revoked for this terminated Fujitsu employe
TCM		Carla Law	Access was not revoked for this terminated Fujitsu employee
TCM		Gary Rogers	Access was not revoked for this terminated Fujitsu employee
TCM		Jason Auburn	Access was not revoked for this terminated Fujitsu employee
TCM		Pruthviraj Kiggal	Access was not revoked for this terminated Fujitsu employee
TCM		Sinteja Kalagampudi	Access was not revoked for this terminated Fujitsu employee
TPM		Leskshmidas, Jishnu	Access was not revoked for this terminated Fujitsu employee
TPM		mohammed Tabrez	Access was not revoked for this terminated Fujitsu employee
TPM		Palherkar Mayur	Access was not revoked for this terminated Fujitsu employee
TPM		Schlatter, Karen	Access was not revoked for this user that had left the Fujitsu RMGA account
TPM		Maxwell, Gary	Access was not appropriate based on this user job responsibility.

FUJ00086945

Appendix B Review of privileged access

The following issues were identified as a result of our review of privileged access across all in-scope applications:

Application: POLSAP

The following 8 dialog and service accounts were identified to be assigned to the SAP_ALL and SAP_NEW profiles:

User ID	Valid from date	Valid through date	User Type	User group	User Lock	Last Logon Date	Last logon time	Privileged Profiles
IRRELEVANT	03.07.2008	31.12.9999	A	SUPER	0	07.12.2010	09:36:40	SAP_ALL, SAP_NEW
	03.10.2008	31.12.9999	A	SUPER	0	06.12.2010	04:25:01	SAP_ALL, SAP_NEW
	25.06.2008	31.12.9999	A	SUPER	0	08.03.2010	09:17:27	SAP_ALL
	11.11.2010	18.11.2010	A	TEST	0	15.11.2010	17:22:21	SAP_ALL, SAP_NEW
	29.04.2010	31.12.9999	S	SUPER	0	10.05.2010	13:04:56	SAP_ALL, SAP_NEW
	25.06.2008	31.12.9999	A	SUPER	0	00.00.0000	00:00:00	SAP_ALL, SAP_NEW
	12.03.2010	31.12.9999	S	SUPER	0	06.12.2010	12:32:15	SAP_ALL, SAP_NEW
	20.11.2007	31.12.9999	A	SUPER	0	10.08.2005	09:18:25	SAP_ALL, SAP_NEW

Appendix C Implement periodic user access reviews and monitoring controls

The following issues were identified as a result of our review of appropriateness of user access across all in-scope applications:

Application: HNGX

The following 2 out of a sample of 25 active directory accounts tested belonged to terminated employees whose access to the HNGX estate was no longer required:

User ID	User Name	Job Title	Active Directory group	Manager
IRRELEVANT	Madan Agrawal	SAP Support Analyst	SAP, External Ops	Eveline Bunce
	Nafasat Hafeez	SMC Engineer, India	SMC Users	Saha Saptarshi

Application: HNGX

The following account out of a sample of 25 active directory accounts tested had inappropriate access to the **ikey-exemptou-users** group:

User ID	User Name	Job Title	Manager
IRRELEVANT	Susanne Doggart	Database Administrator, IRE11	Adrienne Thompson

Appendix D Strengthen the user administration process

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

Application: POLSAP

The following 26 POL cash centre line managers have limited access to SU01:

SAP ID	User's name(s) and job title(s)	User Group
IRRELEVANT	David Adams, Processing Manager	ETNA HOUSE
	Savarimuthu Alex, Processing Manager	ETNA HOUSE
	Robert Bailie, Processing Manager	BELFAST
	Palbinder Boora, Processing Manager	BIRMINGHAM
	Eric Brown, Processing Manager	GLASGOW
	Pat Conlon, Processing Manager	HEMEL_BUREAU
	Eileen Currie, Processing Manager	BELFAST
	Barbara Dealey, Processing Manager	HEMEL_BUREAU
	Barbara Dealey, Processing Manager	HEMEL
	Paul Denton, Processing Manager	LEEDS
	Bryan Flynn, Processing Manager	MANCHESTER
	Chris Flynn, Processing Manager	MANCHESTER
	John Graven, Processing Manager	MANCHESTER

IRRELEVANT	Michael Gregory, Processing Manager	ETNA HOUSE
	Salma Hirji, Processing Manager	POL 1254
	Michael Howard, Centre Manager	POL 1254
	Steve R Howard, Centre Manager	HEMEL_BUREAU
	Martyn Hughes, Processing Manager	BIRMINGHAM
	Simon Irwin, Processing Manager	POL 1254
	John McIntosh, Processing Manager	GLASGOW
	Richard Monk, Processing Manager	HEMEL
	Daksha Parmar, Processing Manager	MIDWAY
	Gillian Margaret Ponter, Processing Manager	MIDWAY
	Melanie Steele, Processing Manager	LEEDS
	ANDREW STEWART, Processing Manager	HEMEL
	Timothy Wall, Processing Manager	POL 1254

Application: POLSAP

We were unable to obtain evidence to support the level of access requested and that access had been authorised by an appropriate individual for the following 24 profile additions out of a sample of 25 tested:

User Name	Full Name	New User or Modification of Access	Profile addition date
IRRELEVANT	Savarimuthu Alex	New User (SAP ADS Migration)	03/08/2010
	Jean Bonfield	New User (SAP ADS Migration)	03/08/2010
	Gregory Collins	New User (SAP ADS Migration)	28/08/2010
	Alfredo De LaCruz	New User (SAP ADS Migration)	28/08/2010
	Jaya Gangadharan	Modification	28/08/2010
	Jean Horridge	New User (SAP ADS Migration)	28/08/2010
	David Leeks	New User (SAP ADS Migration)	03/08/2010
	-	Modification	05/11/2010
	Ian Martin	New User (SAP ADS Migration)	03/08/2010
	Janet Mayor	New User (SAP ADS Migration)	28/08/2010
	Angela McLaughlin	Modification	13/10/2010
	Helen McNeil	New User (SAP ADS Migration)	28/08/2010
	Norman Meredith	Modification	01/10/2010
	Loretta Moran	New User (SAP ADS Migration)	03/08/2010
	-	Modification	28/08/2010
	Roy Nepoleon	New User (SAP ADS Migration)	03/08/2010
	-	New User	28/08/2010
	David Patrick	Modification	05/11/2010
	Keith Spencer	Modification	28/08/2010
	-	New User	07/04/2010
	Stephen Stenson	New User (SAP ADS Migration)	03/08/2010
	Les Tyrrell	Modification	28/08/2010
	Abul Uddin	Modification	30/12/2010
	Ruth Pearson	New User	08/06/2010

Application: POLSAP

We noted that the cash centre line manager providing confirmation of appropriateness for the following 14 profile additions out of a sample of 25 tested had limited access to SU01:

FUJ00086945

User Name	Full Name	New User or Modification?	Date	Manager Providing Confirmation and also has access to SU01
IRRELEVANT	Savarimuthu Alex	New User (SAP ADS Migration)	03/08/2010	Timothy Wall, Processing Manager
	Jean Bonfield	New User (SAP ADS Migration)	03/08/2010	Timothy Wall, Processing Manager
	Gregory Collins	New User (SAP ADS Migration)	03/08/2010	Daksha Parmar, Processing Manager
	Alfredo De LaCruz	New User (SAP ADS Migration)	03/08/2010	Daksha Parmar, Processing Manager
	Jaya Gangadharan	Modification	28/08/2010	Timothy Wall, Processing Manager
	Jean Horridge	New User (SAP ADS Migration)	03/08/2010	John Graven, Processing Manager
	David Leeks	New User (SAP ADS Migration)	03/08/2010	John Graven, Processing Manager
	Ian Martin	New User (SAP ADS Migration)	03/08/2010	Daksha Parmar, Processing Manager
	Angela McLaughlin	Modification	28/08/2010	Martyn Hughes, Processing Manager
	Helen McNeil	New User (SAP ADS Migration)	03/08/2010	Eric Brown, Processing Manager
	Norman Meredith	Modification	28/08/2010	John Graven, Processing Manager
	Loretta Moran	New User (SAP ADS Migration)	03/08/2010	John Graven, Processing Manager
	Roy Nepoleon	New User (SAP ADS Migration)	03/08/2010	Timothy Wall, Processing Manager
	Abul Uddin	Modification	28/08/2010	Timothy Wall, Processing Manager

Application: HNGX

From our sample of 9 active directory user accounts created during the audit period we noted the following:

- One instance of access being requested via a TFS call rather than via an access request form per the standard user administration process:

User ID	User Name	Job Title	Active Directory Group
IRRELEVANT	Srinivasa Lakshmanan	Senior Security Consultant	ipsops

- Three instances of additional access being granted to a user without supporting evidence:

User ID	User Name	Job Title	Active Directory Group
IRRELEVANT	Manu Radhakrishna	SMC Systems Engineer	smc technicians, ikey-exemptou-users
	Siddalingeshwar Goshimath	SMC Systems Engineer	SMC Users
	Rajbinder Bains	Prosecution Support Analyst	audit_admin

- One instance of a system account being granted inappropriate access to the “pathways” active directory group:

User ID	User Name	Job Title	Active Directory Group
IRRELEVANT	system account	system account	pathway

Appendix E 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)	Minimum password length	6 – 8 characters	7 characters	Noted from RSPARAM report via transaction code SE38: login/min_password_lng = 6
	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

FUJ00086945

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 account lockout	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 reset counter = 30 minutes Account lockout duration = 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 F Improvements to the problem and incident management process

The following issues were noted as part of our review of the problem and incident management process for all in-scope applications:

Application: POLSAP, SAP ADS, POL FS, HNGX, Horizon

FUJ00086945

The following two problems, out of 5 sampled for testing, were incorrectly classified as problems when they should have been raised as incidents:

Application	TFS #	Description	Ticket Raised	Resolution	Days to close
Horizon	2656703	WFEACE01 in Bra01 has gone dead	30-Jul-10	23-Sep-10	54
Horizon	2438237	New user for SYSMAN2 (Horizon)	08-Jun-10	23-Sep-10	105