

AUDIT COMMITTEE 18 MARCH 2010

ANNEX B

External audit report recommendations previously agreed by the Committee.

Final Accounts Memorandum: Agreed by Audit Committee 13 November 2008

Finding	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
<p><i>Annual reconciliation of pensioners between payroll system and the pensions AXIS database</i></p> <p>This had not been carried out for the 2007/08 financial year as at 24 July 2008. There is no confirmed date as to when this will take place.</p>	R1 Ensure the annual reconciliation is undertaken.	3	Head of Finance	Yes	<p>The reconciliation of pensioners between the payroll system and the pensions AXIS database has been delayed due to the work involved in bringing in the new payroll system. The new payroll system will bring enhanced reporting tools which will facilitate the completion of this type of reconciliation. Our aim is to complete the reconciliation early next year.</p> <p>The reconciliation of the active members has commenced and we are working through the exceptions (Ruth Gilbert)</p> <p><i>2/3/10 Update (Ruth Gilbert) - First reconciliation complete. To be reconciled again during March 2010. This now forms part of our business process.</i></p>	<p>31/01/09 Revised to 31/03/09</p> <p>2/3/10 – UPDATE - COMPLETED</p>

Report to those charged with Governance: Agreed by Audit Committee 10 November 2009

Ref	Recommendation	Agreed Yes/No	Proposed Action or reason for disagreement	Responsibility	Timetable for Action
1	<p>SAGE and Network</p> <p>All Sage and Network passwords should:</p> <ul style="list-style-type: none"> • be 6-8 characters in length, and contain at least one number; • have a forced change frequency of 30-60 days; • be disallowed if they have been used in the past 12 times; and • be locked out after three failed attempts. 	No	<p>It is accepted that the recommendation represents best practise in password management for systems that are protected by a single authentication method.</p> <p>Sage passwords were compliant with forced change frequency at the time of audit; the password length and history have now been implemented. The Sage system already locks users out after three failed attempts.</p> <p>Network passwords were compliant with password length and change frequency at the time of audit. We will increase the history of changed passwords from 5 to 12. We do not have the granularity to enforce a single numeric; we would need to enforce "complex passwords". Given that we currently receive up to twenty calls per day to the Help Desk relating to users forgetting the network passwords. Most of these are from operational officers and the impact, out of office hours, is to prevent these officers from accessing the systems they need to support effective policing. Increasing password complexity will increase the probability of compromised policing by failure to access systems legitimately.</p> <p>Proposed actions are:</p> <ol style="list-style-type: none"> 1. Increase network password history to 12. 2. Seek funding to implement sign on to systems based on warrant/id card and pin number during financial year 2009/10. 3. Seek funding to implement single sign-on such that warrant/id card credentials passed from network logon to Sage avoiding separate sign on. <p><i>(2) & (3) above - 18/2/10 Update (Tim Glover) – Funding only available to support confidential / PND workstations</i></p> <ol style="list-style-type: none"> 4. If 2 and/or 3 not available, further review of network logons. 	<p>Tim Glover</p> <p>Tom Reynolds</p>	<ol style="list-style-type: none"> 1. Increase network password history to 12 by October 2009. 18/2/10 – UPDATE – ACTION COMPLETED 2. Funding for two factor authentication by April 2010. Implementation by April 2011. 18/2/10 – UPDATE – ACTION ONGOING 3. Funding for single sign on by April 2010. Implementation by April 2011. 18/2/10 – UPDATE – ACTION ONGOING 4. By April 2010.

Ref	Recommendation	Agreed Yes/No	Proposed Action or reason for disagreement	Responsibility	Timetable for Action
2	Test restores should be performed on a regular basis, perhaps on a rolling schedule.	Yes	<p>There will be an annual test restore. A previous restore test was successful.</p> <p><i>1/3/10 Update (Andrew Dale) – Sage is backed up daily and a scheduled annual test restore is carried out. The last restore was successfully completed and a further test restore is scheduled for w/c 1/3/10</i></p>	<p>Andrew Dale</p> <p>Tim Glover</p>	<p>31 March 2010.</p> <p>1/3/10 – UPDATE - ONGOING</p>
3.	<p>Sage and Network</p> <p>The Authority should undertake a formal review of user activity and use access on at least a bimonthly basis to ensure that:</p> <ul style="list-style-type: none"> • access privileges are up to date; • unusual activity such as failed logins and unusual time login are detected; • action is taken to address any risks identified; and • a review should be carried out with immediate effect to remove all inappropriate personnel from the access listing. 	Yes	<p>Network – Review of users will be complete by October 2010.</p> <p>Sage – Functionality to check access privileges/unusual activity is in place for Finance Dept to use as resources permit.</p> <p>Corporate Finance to conduct an immediate review of Sage Users. However, it should be noted that the ‘leavers’ on payroll are checked against the Sage User list each month.</p> <p>Failed log-ins on Sage can now be logged following the setting change in (1) above.</p> <p><i>1/3/10 Update (Andrew Dale) - Immediate review was completed and regular monthly review of leavers is taking place.</i></p> <p><i>Failed log-ins can be picked up in two ways – (1) if three failed log-ins cause a user account to be locked, Corporate Finance are required to unlock the account and (2) a report is available for a manager user that does not use the “FS1” form set within Sage – the report logs <u>all</u> failed log-ins whether the account was locked or not.</i></p>	<p>Tim Glover</p> <p>Andrew Dale / Muhammad Patel</p>	<p>31 October 2010.</p> <p>3/1/10 - UPDATE - ONGOING</p> <p>30 September 2009.</p> <p>3/1/10 – UPDATE – COMPLETED</p>

Ref	Recommendation	Agreed Yes/No	Proposed Action or reason for disagreement	Responsibility	Timetable for Action
4.	<p>Intruder Detection System</p> <p>The Authority should investigate the benefits of having an intruder detection system on the Authority's network.</p>	No	<p>We are currently re-accrediting the network to RESTRICTED. This was considered during this work and it was felt to be unnecessary.</p> <p>However, if there is a view that Sage requires extra protection, we will undertake this investigation and present a business case to consider implementation during 2010/11.</p>	Tom Reynolds	<p>March 2010.</p> <p>3/1/10 – UPDATE - ONGOING</p>
5	<p>Password Changes – Sage</p> <p>Staff should be reminded of the importance of changing Sage password after a password reset.</p>	Yes	Corporate Finance will set generic passwords (e.g. 'password1234') and request that the user changes the password on first log-on. A reminder email to be sent to all Sage users reinforcing this as the Sage system does not have the capability to enforce a password change following a reset.	Andrew Dale	<p>Implemented.</p> <p>COMPLETED</p>
6	<p>System Administrators – Network</p> <p>Access should be governed by unique user access ID.</p>	No	Access to network system administration facilities is by individuals' collar numbers and actions can be attributed to individuals.		<p>In place.</p> <p>COMPLETED</p>
7	<p>Leavers – Network</p> <p>Names should be added to the active directory to enable assignment of collar numbers of individuals.</p>	No	Names were in active directory at the time of the audit.		<p>In place.</p> <p>COMPLETED</p>
8	<p>Oracle Database</p> <ul style="list-style-type: none"> auditing functionality should be enabled; separate environments should exist for production, testing and development; and all security patches should be applied when released following successful testing. 	No	<p>There is a restriction in the application that prevents database read/writes being attributed to individual users. We will explore the cost/viability of changing this restriction and enabling auditing at the database level.</p> <p>We do not do development but accept it is best practise to maintain a test environment. We have test environments for the database and application and will explore the costs of creating a separate Oracle environment to enable patching and version changes to be tested.</p>	Tim Glover	Under investigation part by PART April 2010.

Ref	Recommendation	Agreed Yes/No	Proposed Action or reason for disagreement	Responsibility	Timetable for Action
9	<p>Operational Failures and Security Incidents</p> <p>A formal record is recommended to be held for such incidents to comply with requirements of the Information Commissioner.</p>	Yes	<p>Information Security – a security breach register is currently in development that will allow all staff to report a breach via the intranet. Access to the reports submitted is still being developed but will be by nominated individuals who are responsible for a particular area of business.</p> <p><i>3/1/10 Update (Fiona Linton) - The Security Breach Register has now been built with guidance attached. There are a few minor issues to resolve before publishing on the intranet. A marketing campaign will begin in April 2010 to promote its use and key individuals briefed on their requirement.</i></p>	Fiona Linton	<p>30 September 2009 – to be checked by ACC.</p> <p>3/1/10 – UPDATE - COMPLETED</p>
10	<p>Useful Economic Lives</p> <p>The Authority should consider performing a review of assets that have been fully depreciated to residual value and fleet vehicles lives to ensure that assets are given an appropriate useful economic life.</p>	Yes	<p>A review of the assets which have been fully depreciated will be undertaken during 2009/10 to ensure that assets are given an appropriate useful economic life.</p>	Ruth Gilbert	<p>30 June 2010.</p> <p>3/1/10 – UPDATE - ONGOING</p>
11	<p>Payroll Reconciliation</p> <p>The Authority should consider introducing a high-level reconciliation between the payroll and general ledger system at year end.</p>	Yes	<p>Consideration will be given to introducing a high level reasonableness check between the payroll and general ledger system at the year end. This will be dependent on being able to extract the data in the required format.</p>	Ruth Gilbert	<p>30 June 2010.</p> <p>3/1/10 – UPDATE - ONGOING</p>