Item No. 3(e) on Agenda

STAFFORDSHIRE COUNTY COUNCIL

Internal Audit Final Report

SAP Security & Administration Follow Up

Date of Issue : January 2008

Contact Auditor : John Evans

Distribution List:

Draft Report: Debbie Tams
Linda Gerrard
Eamonn McGirr

Final Report: Debbie Tams
Shirman Yip
Linda Gerrard
Eamonn McGirr
Sander Kristel – IT Director
Andrew Burns – Director of Finance

Final Internal Audit Report

SAP Security & Administration Follow Up

1 Introduction

1.1 This report summarises the results of follow-up activity, following an audit carried out during 2006/7. This follow up review was carried out as part of the 2007/08 Strategic Internal Audit Plan.

1.2 The objective of the original audit reviews was to evaluate and test the key operational and managerial controls within the SAP system and to determine the extent to which those controls can be relied upon to ensure the system objectives are achieved.

1.3 The findings of the audit review have been derived from discussions with key staff involved in the system, including Debbie Tams, Linda Gerrard and Eamonn McGirr, and an examination of available evidence to support actions reported as complete.

1.4 This report highlights remaining control weaknesses and appropriate recommendations for improvement.

1.5 I would like to take this opportunity to thank the staff involved for their assistance during the review.

2 Scope of the Audit and Significance of Findings

2.1 The purpose of the audit was to review progress in the implementation of previously agreed audit recommendations.

2.2 A summary of the scope of the original audit and significance of the remaining audit findings is provided at section 6. This shows the detailed work undertaken for each of the original system objective and identifies the number and significance of the remaining audit findings for each area of work.

3 Audit Opinion

3.1 Limited assurance (see attached list for a definition of opinion)

4 Audit Committee Reporting

4.1 All management summaries for those reports awarded a “Limited Assurance” opinion together with the management summaries of those reports where the audit has been assessed as a “high risk” area (irrespective of the actual opinion awarded) are reported to the Audit Committee. Consequently, it is important to ensure that wording contained within these summaries is factually correct and provides a balanced picture of the internal control environment under review.

4.2 Following on from the above, it should be noted that the management summary detailed for this audit will be presented to the Audit Committee by virtue of the “Limited Assurance” awarded.

4.3 All high level recommendations are reported to the Audit Committee together with progress regarding their implementation. It is important that the management response contained within the final report addresses all elements of the recommendation, includes the name of the officer responsible for implementing the recommendation and the date by which it will be implemented.

4.4 Potentially, an officer could be required to attend meetings of the Audit Committee to explain delays in implementing a recommendation.

5 Management Summary

5.1 An audit of SAP Security and Administration was carried out in February 2007, which generated recommendations, as follows:

- 7 recommendations to address high level risks
- 6 recommendations to address medium level risks

It is disappointing to report that only two audit recommendations have been brought to a conclusion at the time of this follow up. Internal Audit acknowledges that the staff responsible for SAP security have been under considerable work pressure during the year; nevertheless, substantial efforts have been made to progress the items outstanding. ICT have demonstrated their commitment to SAP security by forming the SAP Security and CRM team, with five members. However, fundamental lapses in SAP security and administration cannot be tolerated, especially with the advent of new applications such as Pisces and Hug.

5.2 The remaining paragraphs in this section of the report reproduce the items of concern, as originally reported. Immediately following each paragraph is a further section, in italics, describing the current status. The updated agreed action plan is included at Section 7, as usual, but also included is a detailed programme of work at Section 8. This detailed technical section allows a view of the reasonableness of the work completion dates to be taken, and was supplied by the ICT department. It will be seen that work to address the issues identified has already taken place. Internal audit also acknowledge that some of the issues identified will require a considerable effort to remedy; the revised completion dates are considered reasonable in the circumstances.

5.3 Although a small team within the SAP Support section deal with SAP security administration, they have no written guidance or procedures to follow, other than a flowchart provided by the SAP training team. The security team exercise their own discretion in dealing with access requests. It is understood that a draft SAP Security Policy was developed some time ago, but this has not been agreed nor approved.
The SAP modules are of such great importance to the Council that it is vital that the SAP Support section have the support of a policy and related procedures to regulate access requests, and that these are readily available to all team members. It is to the credit of those currently involved in SAP security administration, that they have exercised common sense in executing their tasks, in the absence of written guidance.

The SAP security team understand that the existing draft policy is not fit for the purpose intended. The policy will be modified, approved and made available to all staff.

5.4 One element of maintaining effective security within SAP is to ensure that the database of user records is properly and promptly maintained.

An important aspect of this maintenance is to ensure that leavers are promptly removed, or deactivated on the system. Audit testing has revealed that the majority of leavers in the last three months have not been deactivated. The Council therefore remains vulnerable to accidental or malicious actions by leavers until deactivation takes place immediately upon departure. For users of R3, leavers are detached from their directorate position number, thus detaching the user id form any access to roles, but the majority of EBP and BW users gain access via the portal, where this form of protection is not available.

The SAP security team have developed a program to de-activate recent leavers, and audit testing has revealed that this program is operating correctly. Leavers are assigned to position code 999999, which effectively renders them unusable. Although it is tempting to delete the user access for leavers, this can often lead to further problems. Deactivation is a much safer option.

The two methods of SAP access, SAP login and SAP portal, provide differing levels of access security assurance. Users of the SAP login method are required to adhere to password construction rules, and to change their password regularly. Users of the SAP portal method are not subject to the same constraints. There is no control of the construction of the SAP portal password, nor any requirement to change it. It is understood that newer releases of the portal software address both these issues. The portal users also contribute to a further problem for SAP login users. Good practice suggests that users who remain inactive for over a year should be deactivated. However, all portal users show this inactivity, even though their use of the system continues. It is therefore difficult to deactivate the appropriate users, as they may well turn out to be live portal users.

A new release of the portal system will enable the construction of passwords to mirror that required by the rest of the system, and will also eliminate the problems created in the inactivity of current users. Internal Audit acknowledge that installing a new release is a major undertaking, and that work on these security issues cannot start until the installation is complete.

All software packages provide a few profiles which give access to the most powerful facilities within the package (e.g. to amend system parameters, or change data). Within the SAP software, the most powerful profiles are SAP ALL and SAP NEW, and these profiles can execute any facility within the software. Best practice suggests that these profiles are severely restricted, ideally to no more than one or two users. Audit investigation has shown that there are forty users with this level of capability at the Council. The majority of these are SAP support staff, who do require a level of capability beyond that of an ordinary user. However, the SAP ALL/SAP NEW profiles are much too powerful for this. It would be possible to develop subsidiary profiles to allow support tasks to take place, but without using SAP ALL or SAP NEW.

Although substantial efforts have been made in the area of Human Resources, there are still around thirty non-system user profiles with the SAP ALL attribute. This is far too many; the target should be two to five at the most. Internal Audit acknowledges that most of the remaining staff with this level of authority are SAP system developers, or support staff, and us such, the risk is now reduced. None the less, this type of authority is too great, even for these staff. The elimination of SAP ALL user profiles is a major task, and likely to take some time.

Good security practice suggests that users should retain a single user identity, and that generic user identities should not be used. Audit investigation has revealed that some users do have two identities, but it is acknowledged that this is required to enable them to perform their duties. There was no evidence of the use of generic identities in the live system.

5.5 One of the features controlled by SAP configuration files is the length of password required at sign on. Although the Council's IT Security Policy mandates a password length of eight, the SAP modules currently require a length of only six.

Current SAP restrictions mean that the maximum length enforceable is seven. However, new versions of SAP, which are planned for installation during 2008/9, may allow further control. The features of the new versions will be investigated, then management will decide whether to implement the immediate solution, or to wait for the longer term solution.

As part of audit testing, the settings in the configuration files relating to security were compared to current best practice. Ten settings in three files did not conform to best practice. However, it is acknowledged that these settings may have been chosen to reflect local needs, and reflect local requirements. Our recommendation is therefore restricted to

a careful examination of these settings, to ascertain the reasons for their current values, and to consider the effects of a possible change to best practice values.

Some approaches have been made to the SAP Basis team, to achieve a better understanding of the settings, and their current settings. Work continues to evaluate the audit suggestions and decide on a way forward.

5.6 SAP, along with most modern software packages, logs usual and unusual events. However, no use is made of these logs to identify unusual security events, nor to review the security status of the package. It is undoubtedly true that such logs record so many events that it is not possible to print them and examine them by eye. However, it would be possible to develop some simple programs to select records of interest, and provide an analysis. Such an analysis could show, for instance, where concentrated efforts are being made to guess passwords, or where the software is regularly in use for extended periods out of office hours.
Internal Audit recommends that use be made of the SAP logs for this purpose; that a regular review of SAP security events should take place; and that security events of significance should be reported to senior management for consideration of further action. The diverse and disparate nature of the Council's computer users means that use of these logs may provide the only indication of attempts to breach security.

Some *progress has been made with this recommendation so far. Internal Audit understands that the security team might contact other authorities who use SAP. It is possible that they may have already developed solutions to address this issue.*

6 Recommendations

6.1 The recommendations still outstanding from the reviews (or re-instated) are ranked according to their level of priority and are shown in the action plan attached at section 6. In addition, the plan includes a column for the client response, the responsible officer and the time scale for implementation of all agreed recommendations:

High - matters that are considered fundamental, to senior management that require immediate attention and priority action.
Medium – Matters that are considered significant, that should be addressed within 6 months.
Low – Matters that merit attention and would improve overall control levels.
Good Practice/Added Value – For consideration only (does not affect the opinion).

7. Detailed Scope of the Audit and Significance of Audit Findings

Scope of the Audit		Audit Findings		
System Objective	**Detailed Area of Work / Risk**	**Recommendation Made (H/M/L)**	**Progress To Date (N/U/S)**	**Satisfactory**
2.1.1	To ensure appropriate security procedures have been developed and approved.	a) **H**	**U**	
	To ensure the security procedures are readily available to all staff.	b) **M**	**N**	
	To ensure SAP security administrators adhere to the documented security procedures.	c) **M**	**N**	
2.1.2	To ensure users who have left are removed or deactivated on the system.			✓
	To ensure users who have never been active, or who have remained inactive for a prolonged period, are removed or deactivated.	e) **H** f) **H**	**U** **U**	
	To ensure users with SAP ALL or SAP NEW authority are few in number, and require the powerful facilities these authorities provide.	g) **H**	**U**	
	To ensure users have no more than one user identity.			✓
	To ensure generic user identities are not in use.			✓
2.1.3	To ensure access to maintain the parameters is severely restricted.			✓
	To ensure the parameters are set to reflect the Council's Information Security Policy.	i) **M**	**U**	
	To ensure the parameters conform to current best practice.	j) **M**	**S**	
2.1.4	To ensure SAP security events are recorded in the system log.	k) **H**	**U**	
	To ensure the security events are reviewed regularly.	l) **M**	**U**	
	To ensure significant security events are brought to the attention of management.	m) **M**	**U**	

Progress to date:

N – Not started
U – Under way
S – Substantially Complete

7. Action Plan

Evaluation of Findings	Recommendation		Client Response (including responsible officer & timescale for implementation)	Current Situation
	Risk Assessment H/M/L	Recommendation		
Objective 2.1.1				
a) There is no policy or procedures to provide guidance to SAP support staff in the implementation and maintenance of SAP security.	H	Revise, finalise and agree the SAP security policy that currently exists only in draft form. Develop and adopt security procedures based on the policy, for the guidance and protection of SAP support staff.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End February 2008
b) The necessary policies and procedures are not available to all staff.	M	Publish the agreed policy and procedures to all staff, so that they may be readily referred to, when required.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End March 2008
c) It was not possible to check whether the work of the SAP security administrators adhered to documented procedures.	M	Once the policy and procedures have been published, institute a programme of managerial checks on the work of the security administrators.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End March 2008

Objective 2.1.2				
d) Users who have left are not promptly removed or deactivated from the SAP system.	H	Tighten the procedures surrounding leavers, to ensure that they are promptly removed or deactivated on the system.	Agreed. Responsible Officer: Eamonn McGirr Completion Date: September 2007	This audit action is complete.
e) Users who accessed the SAP applications via the SAP portal were not subjected to the same access security measures as those whose access was via SAP login.	H	Tighten the portal access system, to ensure that portal users are subject to the same degree of password control as login users.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End June 2008
f) It was not possible to reliably identify users who had not used the system for more than a year, as many current portal users appear to fall into this category.	H	Prepare a list of current portal users, and use it in conjunction with a list of users who appear not have used the system for more than a year to identify instances of true non-use. Delete or deactivate the true non-users.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End February 2008
g) There are forty SAP users who have the role of SAP ALL or SAP NEW assigned. These roles allow access to all SAP functions, including the deletion of records and alterations to module configurations.	H	Restrict the use of SAP ALL and SAP NEW roles to essential users only. Develop subsidiary roles for users such as the SAP support team, who require more powerful access than that available to ordinary users.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End July 2008

Objective 2.1.3				
h) It was not possible to fully ascertain which users had access to maintain the software configuration parameters.	H	Confirm which users have access to maintain each of the software configuration parameter files. Restrict this access to one or two trusted users only.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	This audit action is complete.
i) The SAP password parameters do not require a password length of eight characters, as specified in the Council's Information Security Policy.	M	Revise the password parameters to require a password length of eight characters.	Agreed. Responsible Officer: Eamonn McGirr Completion date: September 2007	Incomplete. Revised completion date: End December 2008
j) Not all the software configuration parameters conform to current best practice. (A list of these parameters, with current and recommended settings, is available from Internal Audit).	M	Carefully consider the current settings of these parameters, and revise them to reflect them to reflect best practice, where appropriate.	Agreed. Responsible Officer: Vic Falcus Completion date: September 2007	Incomplete. Revised completion date: End June 2008

Objective 2.1.4				
k) SAP system log information is not used to identify and investigate security events.	H	Use SAP log information as a basis for the identification of security exposures. Use analysis by program to manage the large volumes of data involved	Agreed. Responsible Officer: Eamonn McGirr Completion date: October 2007	Incomplete. Revised completion date: End June 2008
l) SAP security events are not reviewed.	M	Use the information in the SAP logs to form the basis of a regular review of security events.	Agreed. Responsible Officer: Eamonn McGirr Completion date: October 2007	Incomplete. Revised completion date: End June 2008
m) There is no mechanism to ensure that senior management are made aware of significant SAP security events.	M	Ensure that security items of significance, arising from the regular review of security events, are notified to senior management for consideration of further action.	Agreed. Responsible Officer: Eamonn McGirr Completion date: October 2007	Incomplete. Revised completion date: End June 2008

8. Work Programme, supplied by ICT

Evaluation of Findings	H/M/L	Recommendation	Client Response	SAP security team - latest status comments/planned task	Complete Y/N	Based on current resource levels
Objective 2.1.1						
a) There is no policy or procedures to provide guidance to SAP support staff in the implementation and maintenance of SAP security.	H	Revise, finalise and agree the SAP security policy that currently exists only in draft form. Develop and adopt security procedures based on the policy for the guidance and protection of SAP support staff	Agreed. Completion date Sept 2007	The SAP security team already have processes in place and the policy now needs to reflect these actual processes. These current processes include - 1) Transport process - to process system changes through from the development stage to the live environment. 2) Request for change procedure - to ensure all requests to further develop SAP user roles are documented including business justification. 3) New SAP users process - ensuring all new users receive training and their change managers do not request system access for them until this has taken place. 4) Access for external consultants - 3rd party access form is signed by external consultants and a standard form is sent out requesting details of the access required, for authorisation by the SCC member of staff requesting the access on their behalf. 5) Leavers Procedure - monthly process to report on all leavers who are SAP users, and automatically change validity date of their id to prevent any further access. 6) Dormant users procedure - report to change man	This is addressed in terms of the existence of security procedures, and we are currently in the process of updating the policy so they are reflected in a single document.	Complete by February 08
b) The necessary policies and procedures are not available to all staff.	M	Publish the agreed policy and procedures to all staff, so that they may be readily referred to, when required.	Agreed. Completion date Sept 2007	To follow on from a)	Not Complete	Complete by March 2008

c) It was not possible to check whether the work of the SAP security administrators adhered to documented procedures.	M	Once the policy and procedures have been published, institute a programme of managerial checks on the work of the security administrators.	Agreed. Completion date Sept 2007	The SAP security team are part of the SAP development services teams and as such their work is monitored as for any other team member. All security team members understand and follow the processes highlighted in 2.1.1a)	Already addressed but consideration and review of the value of a more formal approach to the managerial checks is planned.	Complete by March 2008
Objective 2.1.2						
d) Users who have left are not promptly removed or deactivated from the SAP system.	H	Tighten the procedures surrounding leavers, to ensure that they are promptly removed or deactivated on the system.	Agreed. Completion date: Sept 2007	A new security program has been written to automatically assign a validity date to a user id linked to a leaver position to restrict access to the system by that user id. This program is incorporated in a documented leavers procedure. Internal Audit have reviewed and checked the effectiveness of this procedure and their response to date has been to accept the process.	Complete Audit may consider the need to review the frequency with which the process is undertaken, which is currently on a monthly basis.	Complete
e) Users who accessed the SAP applications via the SAP portal were not subjected to the same access security measures as those whose access was via SAP login.	H	Tighten the portal access system, to ensure that portal users are subject to the same degree of password control as login users.	Agreed. Completion date: Sept 2007	A new version of the portal is currently being built. This is expected to be completed by end of December 2007. At this point technical testing of the new version will commence and part of this testing will check the feasibility of aligning the password control to the existing password control we have for network user ids(single sign on). Technical testing is planned to take place during the first quarter of 2008.	Awaiting build of new portal EB7 to be completed, expect to progress during second quarter of 2008	Complete by June 2008, subject to the success of EB7

f) It was not possible to reliably identify users who had not used the system for more than a year, as many current portal users appear to fall into this category.	H	Prepare a list of current portal users, and use it in conjunction with a list of users who appear not have used the system for more than a year to identify instances of true non-use. Delete or deactivate the true non-users.	Agreed. Completion date: Sept 2007	2 reports have been produced:- 1) "not used" those users who have never logged onto the system. 2)"Last logon date" those users who have a logon date of more than 6 months or more old. Now in the process of contacting Directorate Change Managers to make recommendations i.e.delete the user or keep as they should be using the system	Completed reports. Completion of actual deactivation dependant on feedback from change managers. These reports now form the dormant users process.	February 2008 subject to feedback from change managers.
g) There are forty SAP users who have the role of SAP ALL or SAP NEW assigned. These roles allow access to all SAP functions, including the deletion of records and alterations to module configurations.	H	Restrict the use of SAP ALL and SAP NEW roles to essential users only. Develop subsidiary roles for users such as the SAP support team, who require more powerful access than that available to ordinary users.	Agreed. Completion date: Sept 2007	1)Original figure of 40 SAP users is now reduced to 31, as system users can not be included in this audit. These are required by the system itself in order for it to function correctly. Of the remaining 31 users, only 2 of these are situated in the user community, in the HRSSC payroll control team, the rest are used by the SAP development team members themselves. Work has focussed on the user community usage as this was considered to be a higher risk. 2)The HRSSC Payroll control team have been using our newly developed Payroll Control role since July 07 in the live environment, and have requested they retain access to SAPALL/SAPNEW as a contingency until after the year end payroll processes have been completed in May 2008. 3)All other users of SAPALL/SAPNEW are experienced system developers whose job is to develop and configure the SAP system itself. We have produced a report detailing all parts of the SAP system accessed by this group of people over the last 2 years, and we are now due to start work on a n	Priority new user community role now in use. Research into new system developer role completed.	Remaining lower priority roles to be completed by July 2008.

Objective 2.1.3						
h) It was not possible to fully ascertain which users had access to maintain the software configuration parameters.	H	Confirm which users have access to maintain each of the software configuration parameter files. Restrict this access to one or two trusted users only.	Agreed. Completion date: Sept 2007	The SAP production system is protected or locked so that no development/configuration can be made directly to the production system. Any development /configuration has to go through the Dev/QA/Prod transport system. This is standard SAP practice.	Complete	Complete
i) The SAP password parameters do not require a password length of eight characters, as specified in the Council's Information Security Policy.	M	Revise the password parameters to require a password length of eight characters.	Agreed. Completion date: Sept 2007	1)Review has been completed that show that system limitations with current version of R3 etc prevent us complying fully with policy, so the security policy will require amendment to match the current system capabilities. 2)Investigation into improvements within current constraints in the current R3 system has shown that we can increase minimum password length from 3 to 7. This change is currently under test and will require a rollout plan to enable a successful change in the live environment. 3)The implementation of the new version of R3 is expected to start during 2008. In the meantime new CRM and SCH SAP systems will be checked for compliance after their build is complete. 4) The plans to ensure individual SAP module password parameters comply with the policy, may be superseded by the plans being developed to work towards a single sign on, a staged approach which will synchronise the new version of the portal (EB7) with the new version of SAP R3.	Review complete. This objective can not be realised currently because of system constraints.	01/12/2008. To be available in the new version of R3.

j) Not all the software configuration parameters conform to current best practice. (A list of these parameters, with current and recommended settings, is available from Internal Audit)	M	Carefully consider the current settings of these parameters, and revise them to reflect them to reflect best practice, where appropriate.	Agreed. Completion date: Sept 2007	The SAP development teams have not seen any adverse system effects to date, as a result of these current parameter settings. Question on the priority currently assigned to this - more appropriate that this is low? Investigation into the set of parameters has been completed and they are listed in an attachment to this report. The internal SAP basis team, in conjunction with the external basis suppliers, are currently planning to change these parameters in the SAP development environments, monitor and test their effect, and then consider the value of changing them.	Investigation complete. Change Testing in development schedule needs to be confirmed with the Basis team.	Target Jun 08, but need to agree date with the Basis team.
Objective 2.1.4						
k) SAP system log information is not used to identify and investigate security events.	H	Use SAP log information as a basis for the identification of security exposures. Use analysis by program to manage the large volumes of data involved	Agreed. Completion date: Oct 2007	The SAP security team are able to monitor the usage of individual users, and groups of users utilising program RSUSR200, which shows last logon date and time , and date of password change. There is also a program which can be used to highlight where a user has had more than 3 logon attempts.	Work completed on initial phase. This objective is ongoing as we continue to improve on monitoring the usage of SAP.	Initial phase complete. Phase 2 June 08
l) SAP security events are not reviewed.	M	Use the information in the SAP logs to form the basis of a regular review of security events.	Agreed. Completion date: Oct 2007	Adhoc monitoring now takes place for users who have SAPALL/SAPNEW access. Frequency now needs to be reviewed and agreed with Audit.	Complete but require agreement from Audit on frequency.	Initial phase complete. Phase 2 June 08

m) There is no mechanism to ensure that senior management are made aware of significant SAP security events.	M	Ensure that security items of significance, arising from the regular review of security events, are notified to senior management for consideration of further action.	Agreed. Completion date: Oct 2007	Any security breaches resulting from the above monitoring can be escalated to Audit, ICT information security team, and Senior management asap by the SAP security team. So far, there has been no reason to do this.The SAP security team can immediately lock the users id(s) pending further investigation.	Plan in place. Now requires formal documentation and inclusion in the SAP security policy	Initial phase complete. Phase 2 June 08

Definitions of Overall Audit Opinion on System Adequacy and Control

Level	System Adequacy	Control Application
Substantial Assurance	A robust framework of controls ensures that objectives are likely to be achieved.	Controls are applied continuously, or with minor lapses.
Adequate Assurance	A sufficient framework of key controls for objectives to be achieved, but the control framework could be stronger.	Controls are applied, but with some lapses which may put some system objectives at risk.
Limited Assurance	There is a risk of objectives not being achieved due to the absence of key internal controls.	There is a significant breakdown in the application of controls.