Taunton Deane Borough Council

Corporate Governance Committee – 10 March 2014

SAP Access Audit Report

Report of the Strategic Finance Officer
(This matter is the responsibility of Executive Councillor *Mrs Vivienne Stock-Williams*)

1. Summary

SCC (and our) external auditors, Grant Thornton, have recently completed an audit report in relation to SAP access by ICT staff for Somerset County Council.

The report identified a number of actions required to resolve some areas of concern relating to SAP system access.

This report provides a copy of the Grant Thornton report and a progress update against the identified actions. All of the actions are scheduled to be completed by 31st March 2014.

2. Background

2.1 On 1st April 2009 Taunton Deane Borough Council along with Somerset County Council, Avon and Somerset Police and Southwest One Ltd implemented a new combined back office and finance system, SAP (Systems, Applications, Products)

2.2 As part of the audit of Somerset County Council's 2012/13 accounts their external auditor, Grant Thornton (who is also our external auditor) completed a "Review of South West One (SWO) AP IT Controls" audit. Whilst this was part of Somerset CC's accounting audit, as SAP is a shared system the audit was effectively on behalf of all partners. This audit focused specifically on access to the SAP system and was not a general audit of the system or the ICT service.

2.3 Taunton Deane Borough Council along with the other partners have recently had a chance to discuss the report with SCC and Grant Thornton

2.4 An updated report and comments on the various issues are appended to this report.

2.5 It is important to note that the findings from this audit were factored into Grant Thornton's unqualified opinion of the 2012/13 accounts.

3. SAP Access – Overview of Audit Findings

3.1 The Grant Thornton report has highlighted some areas of concern relating to access to SAP.

3.2 The main issues of the Grant Thornton report are;

- There are users of SAP that can access all company and partner records
- Some users can access personally identifiable data

3.3 All large computer systems have a user based security and access management system in place to ensure users of the system can only access the parts of the system and data that are relevant to their job role. The ICT team responsible for supporting the entire system, and for developing and implementing changes to that system need privileged access to the system in order to perform that role.

3.4 The SAP system allows control of these so-called Superuser permissions such that different members of the ICT team have different subsets of the whole permission set. No individual member of the ICT team has all Superuser permissions, and so most support activities require the input from more than one member of the ICT team to complete.

3.5 To provide additional mitigation of the risk that these privileged permissions potentially create, non-technical controls are in place in addition to the technical controls provided by the permission subsets. These non-technical controls are known as Secondary Controls, and take the form of documented processes and written approvals to perform certain changes to the system. For example, the process of moving an updated program from the test system to the live system requires the sign off of testing activities and the documented approval of the SAP Support Manager before the update can go ahead.

3.6 One of the report findings was that allocation of the subset of Superuser privileges appeared to be excessive. Further analysis identified that some reduction in permissions allocated to certain individuals within the ICT team would be possible without preventing them performing their job role. Implementation of these changes is underway and will be complete by the end of March 2014. In the meantime as discussed above, the Secondary Controls regime is in place to provide assurance that only authorised activities are undertaken by members of the ICT team. The effectiveness and enforcement of the Secondary Controls is subject to a quarterly audit undertaken by external IBM assessors, and to our knowledge this audit has not reported any defects.

3.7 The Grant Thornton report did confirm that even thought they found a weakness in controls they found no evidence of actual inappropriate access or changes to data.

4. Action Plan and Way Forward

4.1 We have worked with the other partners and Grant Thornton to finalise the report, attached as Appendix A.

4.2 We have also worked with SWOne to develop an action plan to address the findings. Appendix B shows this action plan – with the specific findings raised by Grant Thornton, the response from SWOne and also our comments on the issue with a RAG status.

4.3 Three of the twelve issues have an Amber status as work is still in progress. This work is due to be completed by the end of March 2014 and is being monitored by the Retained ICT Lead. The remainder are closed and have a Green status, demonstrating that significant work that has been completed since the original report was released.

4.4 Grant Thornton will review this plan and progress as part of their future work currently being planned.

5. Finance Comments

5.1 There are no specific financial implications resulting from this report, although, as stated above, SAP is the Authority's finance system..

6. Legal Comments

6.1 There are no specific legal implications resulting from this report.
.

7. Links to Corporate Aims

7.1 There are no Corporate Aim implications of this report.

8. Environmental and Community Safety Implications

8.1 There are no environmental and community safety implications of this report.

9. Equalities Impact

9.1 There are no equality impacts of this report.

10. Risk Management

10.1 The Grant Thornton report highlighted some areas of risk with regard to the ICT access to SAP. However, these risks are being mitigated by the secondary controls that are in place.

11. Partnership Implications

11.1 SAP is a shared platform between all the partners of Southwest One. Any changes to this platform need to be agreed by all partners.

12. Recommendations

12.1 That the Corporate Governance Committee notes the Grant Thornton report and the actions being taken to address the concerns raised.

Appendices:

Appendix A: Grant Thornton “Review of South West One (SWO) SAP IT Controls”
Appendix B: Action Plan Update
Appendix C: Glossary of Terms

Contact:

Maggie Hammond
01823 358698
m.hammond@tauntondeane.gov.uk

Fiona Kirkham
01823 356522
f.kirkham@tauntondeane.gov.uk

Grant Thornton

Review of South West One (SWO) SAP IT Controls

Contents

Appendices

Introduction

1. As part of our 2012/13 interim audit we have completed a high level review of the IT controls operated by IBM over SWO and the system provided under SAP. Somerset County Council shares use of the SWO system with Avon and Somerset Police and Taunton Deane Borough Council. Since inception of the contract IBM has provided the service under a single 'software as a service licence' (SAAS). SAAS is not uncommon as it enables costs to be shared across a number of clients.

2. SAP maintains separation of accounting between the entities in two ways:

1. It can act as a single system (known as a SAP client) which separates accounts by trial balance codes (known as company codes). This method is suitable for large companies who have several subsidiaries that have their own legal status. This method allows for consolidation of accounts at group level. At a technical level, it uses a shared database schema that stores a shared set of configuration parameters and a shared set of users. Each table in the database contains data from each of the trial balance codes. Access to data is restricted through the SAP security model and requires detailed access permissions to be created to ensure adequate restrictions. From the perspective of administration, this method represents the easiest method to manage as there is only a single system to manage. It is likely to be the lowest cost model because of this. In our view, however, it is the least secure method to manage legal entities that have no relation to each other.

2. The second method is a single system with multiple clients i.e. a client for each legal entity. In this case, each SAP client has its own database schema, configuration parameters and users. This method can use multiple trial balance codes to separate accounts if an organisation wishes, but, unlike the first method, the data in each client can be physically and logically separated from the data in another client. Because the data lies in a different database schema it does not use a shared set of users, it has its own users. In this model the security model only has to restrict access to specific functions and data since all users in the database belong to the entity itself.

3. The contract that SCC entered into uses the first option above and we have therefore sought evidence as to how effective access controls are being operated.

Findings

4. We have set out in Appendix 1 our detailed findings and recommendations for improving controls but there are two key issues that are set out below that require the Council's urgent response.

5. Our review included two basic tests for access to unsecured custom programs and table access (SA38 and SM30/31). These are sensitive SAP transactions that are difficult to implement with users because they give considerable access across the system and should be restricted from end users as well as ICT support staff that are not required to access those parts of the application. We found what we consider to be an excessive number of users from each of the legal entities with access to these transactions given the level of support needed for an SAP application that is not required to be supported 24/7.

6. We identified 26 users who had access to the custom program SA38. SWO, because of confidentiality, have not given us the names of these users. As we are unable to identify these individuals we only have SWO's assurance that these are genuine seconded employees. We have therefore been unable to form a view as to the appropriateness of this level of access or who is gaining access. However, this appears to be an excessive number of users.

7. It should be noted that while we have identified this potential weakness in control we have no evidence of actual, inappropriate access or changes to data. However, our review was not intended to go into this level of detail and further testing would be required to establish if inappropriate access had been made.

Recommendation

8. We have set out in Appendix 1 our recommendations for improving controls.

Appendix 1: Internal control deficiencies; Summary of findings and Recommendations.

	Issue and risk	Recommendation	Priority
1	**Active Directory – Timely Removal of Access** The Council has a Changes/Leavers form for line manager to complete to notify IT of leavers. However, the form is not always completed and reliance is placed on HR department notifying IT of changes or leavers. HR only process these changes on a monthly basis which means that active accounts could remain dormant for up to 4 weeks before being disabled. There is a risk that leaver's accounts could be used by current members of staff to gain unauthorised access to sensitive information or be able to manipulate data that will not be attributable to their accounts.	Implement a robust process to ensure leavers have all their IT rights revoked in a timely manner and that any changes in status are notified to IT immediately.	Medium

	Issue and risk	Recommendation	Priority
2	**SAP - Intruder Lockout Controls/Monitoring** Where users are authenticated by SAP controls rather than Tivoli Access Manager (TAM), users are not locked out if they fail to provide the correct password after a given number of attempts. This increases the chances that the account will be compromised over a period of time and the greater the chance that unsuccessful attempts will go undetected. A reasonable number is a maximum of 6 attempts, after which the account should be locked and user initiated lockouts should be investigated by security personnel. Furthermore, management do not investigate login failures on high risk or privileged user accounts. The SAP system resets the counter on a daily basis and therefore the most effective review frequency is daily. This setting is hard coded and cannot be extended for a longer period. Some privileged accounts have user names that may identify them as privileged. To avoid this some councils use randomly generated user names for all user accounts.	Review account lockout settings over the SAP GUI and ensure that user accounts are locked out where the number of failed attempts to gain entry has been reached (maximum of 6 failed attempts). Furthermore, management should ensure that invalid attempts and account lockouts are regularly reviewed using report RSUSR006. Privilege accounts should be given user names that are randomly generated.	Medium
3	**SAP Password Controls** We noted the following SAP password controls issues: 1. Not currently enforcing 'strong' passwords by the use of a special character and/or numeric character; 2. No minimum password length; and 3. No password expiration period. The lack of strong/complex passwords facilitates password	Password controls should be improved by the implementation and enforcement of: 1. Increased password complexity by enforcing a special character and/or numerical character in the password string. 2. Password dictionary controls to prevent the use of common words as passwords; 3. A minimum password length; and	Medium

	Issue and risk	Recommendation	Priority
	guessing and may potentially allow the system to be compromised by unauthorised users. Where passwords do not expire, there is a risk that they will become vulnerable to being disclosed over time and can therefore provide access to the system and data	4. A forced password change interval to expire after a reasonable amount of time. It is recommended that passwords are changed between 60 and 90 days.	
4	**SAP Default Passwords** The SAP default accounts use powerful profiles that give full access to the productive or installation reference system. Default passwords were still assigned to default accounts: Continued use of the default passwords significantly reduces the effectiveness of password controls and increase the risk of unauthorised access.	Default or trivial passwords for SAP should be changed immediately and regularly thereafter.	Medium
5	**SAP Segregation of Duties** There is no segregation between users who are capable of programming and users who have a batch administration or operations role. The lack of segregation between programming, operations and management prevents adequate controls being exercised which could lead to unauthorised changes being made to the system. Without management segregation the risk of unauthorised changes remaining undetected is increased.	1. Segregation should be maintained between programmers and those who administer programs that are run as batch processes. Programmers should not have access to change batch programs in production nor select which programs are run. 2. Where there are difficulties in separating the functions, mitigating controls should be considered that periodically review changes made to the batch programs and ensure that changes are authorised.	Medium

	Issue and risk	Recommendation	Priority
6	**SAP Segregation of Duties – Programming/Security** There is inadequate separation of responsibilities for programming from security or other operational functions. The failure to maintain separation between programming responsibilities and system security can potentially allow system security parameters to be compromised and unauthorised data changes to be go undetected.	Programmers should be restricted from having any operational access in the production environment which is best achieved by removing their user record. Temporary production access may be appropriate for certain change projects, however it is recommended that such access is removed after a defined period of time or closure of the project.	Medium
7	**Segregation of Duties – SAP Transports** One user has the ability to transport changes made in the development environment directly to the production environment via STMS transport tools. A user can therefore make a change in the development system and pass it through to production system without anyone else being involved. A segregation of duties is essential to avoid this potential weakness.	Programmers should: • be restricted from accessing SAP transport utilities. This should be achieved by removing all user records for programmers. • not have any privileged access to the operating system on the SAP server or have the ability to remotely call the SAP transport program 'tp'.	High

8	**SAP Direct Access to Production** Programmers have direct access to the final working version of the system rather than making sure that changes are made in development and only transferred to production following suitable change controls, testing and authorisation. Direct access to programming editing tools in the production environment represents a high risk to the organisation as it allows unauthorised changes to be made to data and programs.	Ensure that all development keys are removed from the production environment to ensure that direct changes are not applied without an approved transport.	High
9	**SAP Excessive Privileges – RZ10** The RZ10 transaction allows many system security and operational parameters to be switched off or changed. It should be used only where there is approval from management under a change control process. At present it is not appropriately restricted and12 dialogue users have access. Inappropriate use of the RZ10 transaction can expose the SAP system to security breaches and other operational problems.	Ensure that access to the RZ10 transaction code is restricted to the system administrator and the EMERGENCY or fire-fighter user ID. No end users or other IT staff should have access to this transaction.	High
10	**SAP Excessive Privileges - SAP All Privilege** The review noted the SAP_ALL profile had been allocated to the following users: SUPPORT CSMADM DDIC	The SAP_ALL profile should be reserved for use within an emergency or fire-fighter type ID that can be locked when not in use. SAP ALL access should be time limited and its use monitored.	High

	The SAP_ALL authorisation profile contains virtually full system rights and should not be used with any dialogue type accounts within the production environment. The profile provides access to all IT functions as well as business transactions which with misuse can cause operational instability and financial misstatements. Restricting the use of SAP_ALL to an emergency or fire-fighter type account can limit the use of such accounts through limiting their period of validity. It also enables monitoring of when the account has been used by referring to the SAP change document log contained in the report RSUSR002.		
11	**SAP Excessive Privileges – SA38** It was noted that 26 users had access to the SA38 privilege. The use of the transaction code SA38 in the production environment should be highly restricted since it provides access to run custom programs that have not been secured with authorisation objects or authorisation groups, thereby allowing the user to access functionality and data not associated with their normal SAP role. It should be noted that in many SAP implementations, custom programs may be inherited from legacy SAP installations and new custom programs may not have been programmed using authority checks. Access to SA38 provides full access to any program that does not contain an authority check and can therefore circumvent the standard SAP authorisation model.	The use of SA38 should be restricted to system administrators and personnel who have been given permission to access all custom programs and data.	High

12	**SAP Excessive Privileges – SCC4** Access to the client administration transaction code SCC4 has not been restricted. 8 accounts were identified with this privilege. The client administration function provided by SCC4 allows the SAP client to be opened for changes which if done in an inappropriate or unauthorised manner can have significant consequences for the integrity of the data within the system.	Client administration function should be restricted to the system administrator and the emergency user or fire-fighter ID. Management should regularly review the SCC4 change log to ascertain if the SAP client has been opened with proper authorisation.	High

ACTION PLAN UPDATE **APPENDIX B**

#	Description	Issue & Risk	Recommendation	Priority	SWO Category	SWO Comments	SWO View of Risk	Status	TDBC RAG	TDBC Narrative
1	Active Directory – Timely Removal of Access	The Council have a Changes/Leavers form for the line manager to complete to notify IT of leavers. However, the form is not always completed and reliance is placed on HR department notifying IT of changes or leavers. HR only process these changes on a monthly basis which means that active accounts could remain dormant for up to 4 weeks before being disabled. There is a risk that leaver's accounts could be used by current members of staff to gain unauthorised access to sensitive information or be able to manipulate data that will not be attributable to their accounts.	Implement a robust process to ensure leavers have all their IT rights revoked in a timely manner and that any changes in status are notified to IT immediately.	Medium	Active Directory	Access to SAP is not controlled by same process as AD. The AD process is agreed with the client. No remedial action to be taken	Not applicable to SAP	Closed	🟩	Agreed
2	SAP - Intruder Lockout Controls/Monitoring	Where users are authenticated by SAP controls rather than Tivoli Access Manager (TAM), users are not locked out if they fail to provide the correct password after a given number of attempts. This increases the chances that the account will be compromised over a period of time and the greater the chance that unsuccessful attempts will go undetected. A reasonable number is a maximum of 6 attempts, after which the account should be locked and user initiated lockouts should be investigated by security personnel. Furthermore, management do not investigate login failures on high risk or privileged user accounts. The SAP system resets the counter on a daily basis and therefore the most effective review frequency is daily. This setting is hard coded and cannot be extended for a longer period. Some privileged accounts have user names that may identify them as privileged. To avoid this some organisations use randomly generated user names for all user accounts.	Review account lockout settings over the SAP GUI and ensure that user accounts are locked out where the number of failed attempts to gain entry has been reached (maximum of 6 failed attempts). Furthermore, management should ensure that invalid attempts and account lockouts are regularly reviewed using report RSUSR006. Privilege accounts should be given user names that are randomly generated.	Medium	Authentication	Normal access to SAP is via employee portal which goes through TAM and therefore DOES apply password policy. As a result of this recommendation, direct SAP GUI access is possible and this is being disabled through a technical change which has been developed and tested in preproduction. Implementation to production will be done during a regular maintenance window targeted for early feb, pending change approval. In response to this recommendation, SWO are implementing a process to review the priveledged account login failures using a TAM report quarterly as part of their existing BAU controls. Reset counter is set in TAM for normal access. SAP GUI access is being revoked per item 2. The only accounts which could be definitively identified as priveleged from the username alone, are the SAP standard accounts eg DDIC and SAP*. SWO reviewed this recommendation with GT who accepted that this was not applicable in this case as low risk.	Users going directly via SAP GUI rather than employee portal would not have password rules enforced. Risk of brute force attack if user ID's were known. This risk has increased following SCC's publication of the GT report. Any attack on the system is likely to target known admin id's.	Closed	🟩	The change to disable SAP GUI access has now been implemented. All user access to SAP is authenticated via TAM
3	SAP Password Controls	We noted the following SAP password controls issues: 1. Not currently enforcing 'strong' passwords by the use of a special character and/or numeric character; 2. No minimum password length; and 3. No password expiration period. The lack of strong/complex passwords facilitates password guessing and may potentially allow the system to be compromised by unauthorised users. Where passwords do not expire, there is a risk that they will become vulnerable to being disclosed over time and can therefore provide access to the system and data	Password controls should be improved by the implementation and enforcement of: 1. Increased password complexity by enforcing a special character and/or numerical character in the password string. 2. Password dictionary controls to prevent the use of common words as passwords; 3. A minimum password length; and 4. A forced password change interval to expire after a reasonable amount of time. It is recommended that passwords are changed between 60 and 90 days.	Medium	Authentication	This is set in TAM for normal access. SAP GUI access is being revoked per item 2.	As per SAP GUI access.	Closed	🟩	The change to disable SAP GUI access has now been implemented. All user access to SAP is authenticated via TAM

4	SAP Default Passwords	The SAP default accounts use powerful profiles that give full access to the productive or installation reference system. Default passwords were still assigned to default accounts: <removed for security purposes>. Continued use of the default passwords significantly reduces the effectiveness of password controls and increase the risk of unauthorised access.	Default or trivial passwords for SAP should be changed immediately and regularly thereafter.	Medium	Authentication	Following the recommendation, SWO have rectified the specified accounts in November 2013	Risk of system access via SAP standard account. However, these were already locked down.	Closed	🟩	Agreed
5	SAP Segregation of Duties	There is no segregation between users who are capable of programming and users who have a batch administration or operations role. The lack of segregation between programming, operations and management prevents adequate controls being exercised which could lead to unauthorised changes being made to the system. Without management segregation the risk of unauthorised changes remaining undetected is increased.	1. Segregation should be maintained between programmers and those who administer programs that are run as batch processes. Programmers should not have access to change batch programs in production nor select which programs are run. 2. Where there are difficulties in separating the functions, mitigating controls should be considered that periodically review changes made to the batch programs and ensure that changes are authorised.	Medium	Segregation of Duties	GT confirmed this applies to one user. Secondary controls were already in place. User cannot be amended without impacting service. Change control process is in place requiring management approval to implement changes. Separation of duties is also in place across the SAP team. SWO recognise that these are soft controls. A hard implementation would require additional resources.	Low risk as secondary controls are in place	Closed	🟩	TDBC agree that secondary controls in place provide sufficient mitigation of this risk
6	SAP Segregation of Duties – Programming/Security	There is inadequate separation of responsibilities for programming from security or other operational functions. The failure to maintain separation between programming responsibilities and system security can potentially allow system security parameters to be compromised and unauthorised data changes to be go undetected.	Programmers should be restricted from having any operational access in the production environment which is best achieved by removing their user record. Temporary production access may be appropriate for certain change projects, however it is recommended that such access is removed after a defined period of time or closure of the project.	Medium	Segregation of Duties	Change control process is in place requiring management approval to implement changes. Separation of duties is also in place across the SAP team. SWO recognise that these are soft controls. A hard implementation would require additional resources.	Low risk as secondary controls are in place	Closed	🟩	TDBC agree that secondary controls in place provide sufficient mitigation of this risk
7	Segregation of Duties – SAP Transports	One user has the ability to transport changes made in the development environment directly to the production environment via STMS transport tools. A user can therefore make a change in the development system and pass it through to production system without anyone else being involved. A segregation of duties is essential to avoid this potential weakness.	Programmers should: be restricted from accessing SAP transport utilities. This should be achieved by removing all user records for programmers. not have any privileged access to the operating system on the SAP server or have the ability to remotely call the SAP transport program 'tp'.	High	Segregation of Duties	Change control process is in place requiring management approval to implement changes. Separation of duties is also in place across the SAP team. SWO recognise that these are soft controls. A hard implementation would require additional resources.	Low risk as secondary controls are in place	Closed	🟩	TDBC agree that secondary controls in place provide sufficient mitigation of this risk
8	SAP Direct Access to Production	Programmers have direct access to the final working version of the system rather than making sure that changes are made in development and only transferred to production following suitable change controls, testing and authorisation. Direct access to programming editing tools in the production environment represents a high risk to the organisation as it allows unauthorised changes to be made to data and programs.	Ensure that all development keys are removed from the production environment to ensure that direct changes are not applied without an approved transport.	High	Segregation of Duties	This is not correct. Th one user who was the identified 'programmer' in finding 7 does not have a development key in production therefore cannot do developments directly in production.	N/A	Closed	🟩	Agreed
9	SAP Excessive Privileges – RZ10	The RZ10 transaction allows many system security and operational parameters to be switched off or changed. It should be used only where there is approval from management under a change control process. At present it is not appropriately restricted and 12 dialogue users have access. Inappropriate use of the RZ10 transaction can expose the SAP system to security breaches and other operational problems.	Ensure that access to the RZ10 transaction code is restricted to the system administrator and the EMERGENCY or fire-fighter user ID. No end users or other IT staff should have access to this transaction.	High	SAP Priveleges	GT have identified 26 ID's with RZ10 and SM38. Whilst these are all priveledged users in the SAP support team, it will be further restricted according to business need. Nobody outside the SAP techincal team has access to this transaction. Target number is 3 for RZ10 and 16 for SA38 by end March 2014.	SWO accept GT's view of risk.	In Progress	A	Progress to make the required changes is tracked at the fortnightly SAP Cross Authority Change Board meeting. In the meantime strong secondary controls migitate the level of risk

10	SAP Excessive Privileges - SAP All Privilege	The review noted the SAP_ALL profile had been allocated to the following users: SUPPORT CSMADM DDIC The SAP_ALL authorisation profile contains virtually full system rights and should not be used with any dialogue type accounts within the production environment. The profile provides access to all IT functions as well as business transactions which with misuse can cause operational instability and financial misstatements. Restricting the use of SAP_ALL to an emergency or fire-fighter type account can limit the use of such accounts through limiting their period of validity. It also enables monitoring of when the account has been used by referring to the SAP change document log contained in the report RSUSR002.	The SAP_ALL profile should be reserved for use within an emergency or fire-fighter type ID that can be locked when not in use. SAP ALL access should be time limited and its use monitored.	High	SAP Priveleges	**All of GT's recommendations were already in place at the time of audit.** SAP all is reserved for those 3 accounts + firefighter. Support and Firefighter ID's are locked when not in use, DDIC and CSMADM cannot be locked and are required by the system. Support and Firefighter access is time limited by management approval at the point they are needed and its use monitored through shared priviledge ID audits. As a result of the report, SWO have also removed dialogue access for CSMADM.	Appropriate care has been taken of these accounts.	Closed	🟩	Agreed
11	SAP Excessive Privileges – SA38	It was noted that 26 users had access to the SA38 privilege. The use of the transaction code SA38 in the production environment should be highly restricted since it provides access to run custom programs that have not been secured with authorisation objects or authorisation groups, thereby allowing the user to access functionality and data not associated with their normal SAP role. This could expose the organisations data to users who do not work directly for the organisation. It should be noted that in many SAP implementations, custom programs may be inherited from legacy SAP installations and new custom programs may not have been programmed using authority checks. Access to SA38 provides full access to any program that does not contain an authority check and can therefore circumvent the standard SAP authorisation model.	The use of SA38 should be restricted to system administrators and personnel who have been given permission to access all custom programs and data.	High	SAP Priveleges	As per item 9.	An SA38 user can run programs in the system. In theory therefore, writing and running a malicious program. Ie Read and Write	In Progress	A	Progress to make the required changes is tracked at the fortnightly SAP Cross Authority Change Board meeting. In the meantime strong secondary controls migitate the level of risk
12	SAP Excessive Privileges – SCC4	Access to the client administration transaction code SCC4 has not been restricted. 8 accounts were identified with this privilege. The client administration function provided by SCC4 allows the SAP client to be opened for changes which if done in an inappropriate or unauthorised manner can have significant consequences for the integrity of the data within the system.	Client administration function should be restricted to the system administrator and the emergency user or fire-fighter ID. Management should regularly review the SCC4 change log to ascertain if the SAP client has been opened with proper authorisation.	High	SAP Priveleges	These are all priveledged users in the SAP support team, it will be further restricted according to business need. Nobody outside the SAP technical team has access to this transaction. Target number is 3 for SCC4 by end Q1.	SWO agree with GT's risk assessment. Read and Write available depending on the other transactions available to the user	In Progress	A	Progress to make the required changes is tracked at the fortnightly SAP Cross Authority Change Board meeting. In the meantime strong secondary controls migitate the level of risk

Appendix C – Glossary of Terms

Term	Description
AD	Active Directory – the user directory, permissions and security system used by Microsoft Windows servers
BAU	Business As Usual – processes and activities which form part of the day to day running of the service
CSMADM	SAP User ID used to access support activities within the system
DDIC	SAP User ID used to access support activities within the system
DICBERCLS	Database field where specific details of access limitations are held
Employee Portal	The web browser based screen which all non-ICT users use to access the SAP system
EPIUSE	SAP tool used to clone data between live, test & development systems
GUI	Graphical User Interface – the SAP ‘screen’ that connects directly to the SAP system
IT	The Information Technology support team – this report
RSUSR002	SAP report on users, user roles and authorisations
RZ10	SAP program used to manage access profiles within the system
S_TABU_DIS	SAP authorisation profile that enables limiting of access to data
SA38	SAP program used to run other programs
SAP_ALL	Permissions group with full permissions on SAP system
SCC4	SAP program used to manage changes to the SAP client system
SM30	SAP program used to display and update background table data
SM31	SAP program used to display and update background table data
SM38	SAP program to display transaction queues and activity logs
STMS	SAP Transport Management System – the mechanism by which changes are moved from the development -> test -> live environments
SUPPORT	SAP User ID used to access support programs within the system
TAM	Tivoli Access Manager – an authentication and authorisation system used to manage user access into SAP