GRANT THORNTON REPORT					SOUTHWEST ONE RESPONSE		
#	Description	Issue & Risk	Recommendation	Priority	Action	Target Date	Status
1	Active Directory – Timely Removal of Access	Avon and Somerset Police 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	This process is as agreed with the clients and if it is requested to be changed we will change it	N/A	Closed
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.	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.	Medium	Our strategy is for access management via TAM. Majority of lockouts occur via TAM. This item refers only to the use of the stores team at the Police due to their use of the Tranman product. We will raise use of SAP GUI at the next Cross-Authority Change Board (XACB) in December with a proposal to disable direct GUI access in Q1, and develop portal access where need is identified	31/03/2014	Open
		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.	Privilege accounts should be given user names that are randomly generated.	Medium	Only 20 employees. Agreed with Auditors that not necessary	N/A	Closed

GRANT THORNTON REPORT					SOUTHWEST ONE RESPONSE		
#	Description	Issue & Risk	Recommendation	Priority	Action	Target Date	Status
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	Medium	Raise use of SAP GUI at the next Cross-Authority Change Board (XACB) with a proposal to disable direct GUI access in Q1. Same points as per limited use as item 2	31/03/2014	Open
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	SWOne have identified the IDs and passwords to be rectified, and change has been applied in Development. Same change will be made in Pre-Prod on the 17th November and will be monitored for any business impact. Same change planned for Production by the end of November (next scheduled SAP outage).	30/11/2013	Open
		There is no segregation between users who are capable of programming and users who have a batch administration or operations role.	1. Segregation should be maintained between programmers and those who administer				

GRANT THORNTON REPORT					SOUTHWEST ONE RESPONSE		
#	**Description**	**Issue & Risk**	**Recommendation**	**Priority**	**Action**	**Target Date**	**Status**
5	SAP Segregation of Duties	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.	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	**Low risk -** Grant Thornton has confirmed that this only applies to one user. Grant Thornton were happy with the secondary controls (separation of duties) that were already in place to mitigate this, but SWOne agreed to amend this person's access to ensure that they cannot move any transport they have created.		Closed
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	**Low Risk -** Grant Thornton has confirmed that this only applies to one user. Grant Thornton were happy with the secondary controls (separation of duties) that were already in place to mitigate this, but SWOne agreed to amend this person's access to ensure that they cannot move any transport they have created.		Closed
7	Segregation of Duties – SAP Transports	The user, 'LKING' 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	**Low Risk** Grant Thornton has confirmed that this only applies to one user. Grant Thornton were happy with the secondary controls (separation of duties) that were already in place to mitigate this, but SWOne agreed to amend this person's access to ensure that they cannot move any transport they have created.		Closed

GRANT THORNTON REPORT					SOUTHWEST ONE RESPONSE		
#	Description	Issue & Risk	Recommendation	Priority	Action	Target Date	Status
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	**Low risk** Grant Thornton has confirmed that this only applies to one user. Grant Thornton were happy with the secondary controls (separation of duties) that were already in place to mitigate this, but SWOne agreed to amend this person's access to ensure that they cannot move any transport they have created.		Closed
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	These accesses are limited to privileged internal users. Report of access produced. SWO will continue to review the number of privileged users on the system and where justified remove or reduce.		Closed

GRANT THORNTON REPORT					SOUTHWEST ONE RESPONSE		
#	Description	Issue & Risk	Recommendation	Priority	Action	Target Date	Status
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	SWO already have control processes around the use and deployment of these accounts. SUPPORT is the SAP dial-in account - which already has CIM approval for its use, and CIM approval is sought every time SAP requires this access (not open access). DDIC account now benefits from the firefighter account process and CSMADM will be converted to a non-dialogue account.		Closed
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.	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	These accesses are limited to privileged internal users. Report of access produced. SWO will continue to review the number of privileged users on the system and where justified remove or		Closed

GRANT THORNTON REPORT					SOUTHWEST ONE RESPONSE		
#	Description	Issue & Risk	Recommendation	Priority	Action	Target Date	Status
		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.	custom programs and data.		reduce.		
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	These accesses are limited to privileged internal users. Report of access produced. SWO will continue to review the number of privileged users on the system and where justified remove or reduce.		Closed
13	SAP Access to Sensitive Tables SM30/SM31	The organisation has 22 users with access to sensitive table data editing transactions SM30 and SM31. A review of the organisations that these individuals work for identified a mixture of IBM, Somerset County Council, Taunton Deane Borough Council, Avon & Somerset Police and EPIUSE. All have been seconded to SW One, with the exception of IBM and the EPIUSE user. Access in all cases was authorised by SW One. Access to these transactions under certain conditions can allow customised data tables to be edited directly, potentially resulting in unauthorised entries or database integrity problems.	Ensure that customisable tables are adequately protected by preventing users from using the SM30 or SM31 transaction code. Where this is not possible due to business requirements customisable tables should be protected via authorisation groups and users restricted in their access those authorisation groups. At a very minimum, no user with access to SM30 and SM31 should have a wild card entry (*) in the DICBERCLS field of the S_TABU_DIS authorisation object. In all cases where users (both IT and end user) have access to SM30 and SM31, management should consider logging the use of these transactions and should review them periodically.	High	These accesses are limited to privileged internal users. Report of access produced. SWO will continue to review the number of privileged users on the system and where justified remove or reduce.		Closed