Wiltshire Council

Where everybody matters

Audit Committee
19 September 2012
Update on KPMG IT recommendations made in June 2012

Priority rating for recommendations		
1 ***Priority one***: issues that are fundamental and material to your system of internal control. We believe that these issues might mean that you do not meet a system objective or reduce (mitigate) a risk.	2 ***Priority two***: issues that have an important effect on internal controls but do not need immediate action. You may still meet a system objective in full or in part or reduce (mitigate) a risk adequately but the weakness remains in the system.	3 ***Priority three***: issues that would, if corrected, improve the internal control in general but are not vital to the overall system. These are generally issues of best practice that we feel would benefit you if you introduced them.

The recommendations listed below have been extracted from KPMG's interim audit report.
The numbering of the recommendations has been amended to remove the non IT points.
The updates have been discussed with KPMG and we have included their comments in the status section of each recommendation.

No	Risk	Issue and recommendation	Management response and current status
1	1	**Protection of the production environment from direct changes - *SAP*** The underlying SQL database that holds all SAP data can be accessed using generic user accounts by up to 237 Logica staff. This is considered to be a high volume of users. There is also a lack of compensating monitoring controls in place to ensure that direct database access is appropriate. Direct changes to data via the SAP Graphical User Interface (GUI) is restricted by technical controls to lock the live production environment and enforce changes to be actioned through non-production environments. However, no monitoring is carried out to ensure that these controls are operating effectively and that the production environment and the production client has remained locked from direct changes. There is a risk that unathorised changes are made to the data in the live system which remain undetected. **Recommendation** Restrict access to the underlying database to a minimal number of users, particularly where write/amend/delete access is granted. Such access should be appropriately logged and monitored. The Council should also consider enabling the tracking of changes to the data held within SAP database tables (table logging). Where possible, periodic review of table logs should be implemented to reduce the risk of unauthorised changes.	A mitigating control has been discussed with KPMG, which management will discuss with the Logica service delivery team. This control is whether Logica have a current ISAE3402 report which will provide assurance to KPMG of Logica's control environment. Responsible officer: Stuart Honeyball Date: 30 June 2012 Update Logica have previously provided copies of certificates and evidence to KPMG via Mark Wallington to show that the physical controls on the data centre are at IL3 level so I am assuming there are no outstanding issues on that aspect. Regarding the protection of the databases -Logica provides full support to Wiltshire in against contractually agreed and measured business hours, including 24x7 support for priority 1 calls. Logica has implemented BMC monitoring tools which is configured to automatically alert their on-call teams when certain system thresholds are breached. This mailbox is monitored 24x7 so if anything goes wrong with the system they are notified in advance and the Logica team reacts to them immediately. In order to provide the service to Wilts, Logica need full access to these production servers. If they did not have this access and did not have any Wilshire contacts at that particular time it could seriously hinder the progress of resolving P1 issues and in turn cause significant implications to the running of the business. This is a service that was defined as part of the tender and for which we pay Logica to implement, to ensure full business service availability. This is important as they are measured (and potentially financially penalised) against a contractually bound set of SLA's regarding performance and fault resolution targets, which cannot be reasonably met if they do not have appropriate access to our systems. This would clearly includes Database monitoring/maintenance as a component activity. To provide context to the seemingly high number of users with *potential* access to our database: Logica operates this support service from a number of control centres across the globe, using a 'follow the sun' support model. This means that shift duties are passed from office to office to ensure full continuity of service, as per the contract specifications. This approach requires that suitably trained resources are available in each of those locations during their operating hours, therefore analysis of the number of Logica analysts who *could* have access to our database should be made with reference to the contractually agreed and approved support model above. In addition, Logica has an internal monitoring tool to monitor who has logged on the PRD systems (at application level) at a particular time and date. This is being already being validated and checked monthly by Council staff. The international standard ISAE3402 is a recently introduced standard (June 2011) and as such compliance with this standard has never formed part of our hosting and support contact with Logica, which was let and signed in 2008. We believe that the existing controls which Logica hold and have demonstrated (ISO27000 and ISO9001, independently verified by Det Norske Veritas [DNV]) do already cover controls regarding management of access to client systems, and significant parallels can be drawn between these standards and the *relevant* parts of ISAE3402 in this context. **Action required**: Wiltshire Council is satisfied that Logica holds certification to evident its control environment is appropriate to the Council's requirement. **Status:** This is in process of being discussed between Logica and KPMG to resolve outstanding queries.

No	Risk	Issue and recommendation	Management response and current status
2	2	**Standard SAP super user accounts** Standard SAP super user accounts are not appropriately controlled in all instances of SAP. Such accounts are generic and possess the powerful SAP_ALL profile, allowing access to all system functionality. Accounts should be maintained in a locked state with complex passwords and used only where necessary. In such a case, use of the account should be appropriately requested, approved, monitored and documented. It was noted that the greatest risk lies in the unlocked account (DDIC) in the production client. This was stated to be necessary in order for system jobs to execute. **Recommendation** SAP standard user accounts should be locked in all clients and passwords made non-trivial. Dependencies on SAP standard user accounts should be removed where possible and replaced by system or communication type accounts that cannot be accessed by end-users	The status of the userID DDIC in the Production system will be amended from Dialog to System. This will remove the possibility of anyone logging on to a SAPGUI session via this userID. All other standard userID's will be reviewed and the passwords, lock statuses and user types corrected as necessary. Responsible officer: Stuart Honeyball Date: 30 June 2012 <u>Update</u> The Council confirm the recommended changes have been made. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented as described then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
3	2	**Access to sensitive SAP transactions** A number of users were noted to possess access to sensitive SAP transactions that were not required according to their job role and requirements. It was noted that user access to the above transactions is in some circumstances validated by business requirements. **Recommendation** Access to sensitive SAP transactions should be reviewed to ensure that access is restricted to only those users that require the functionality according to their job role and requirements. Where business reasons exists for access to such transactions, this should be appropriately documented, approved and monitored. Enforce segregation of duties for IT and business users with any known exceptions subject to further documentation and appropriate approval.	Many of these transactions cover standard transactional activities which are used in a number of areas of the business. SAP Support Team will review those users with these types of access and make necessary amendments. We will also seek to develop additional documentation to ensure that we can effectively manage the review and recording of changes to these transactions, where they are not already covered by our existing critical transaction monitoring processes. A review of the transaction codes considered critical will also be undertaken to ensure appropriate coverage. Responsible officer: Stuart Honeyball Date: 30 June 2012 Update The Council confirms the recommended changes have been made. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented as described then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
4	3	**Resolution of problems directly in the SAP production environment** A small number of instances were identified during the financial year where testing for problem resolution was carried out directly in the live production environment. It was stated that taking action in the production environment only occurred where alternative actions had already been carried out. Despite this, there is a risk that the production environment may be negatively impacted by performing un-tested problem resolution activities. **Recommendation** Resolution of problems directly in the production environment should be avoided wherever possible. Such activities should be carried out in a non-production environment that appropriately mirrors the production environment to validate testing performed. This will ensure that there is no risk to the integrity of the production environment whilst performing problem resolution activities.	There are specific changes in SAP that can only be made in the production environment. This is not a matter of choice but the way that SAP is configured. In the last year there have been 7 specific occasions when changes have needed to be made in the production environment. Three of these are related to adding a product category for a council service called 'Help to live at home' where the data has to be created directly in the production environment. An evidence trail is in place for each of these instances including screen shots which has been evidenced and approved by the SWAP audit including time of opening and closing; reason for opening, who has opened who has actioned the changes and that it has been closed. Each of these steps is monitored by a third (neutral) person who sits outside the process of opening and closing or taking any action in the live environment. The auditor's recommendations are noted and understood, and it is our standard operating process to diagnose, test and fix faults in the Development (DEV) Quality Assurance (QAS) environments of SAP before effecting the same in Production. It is by exception that any changes are made in the production environment and only when these cannot be done in DEV and QAS. Responsible officer: Stuart Honeyball Date: 30 June 2012 <u>Update</u> The Council's standard approach to applying problem fixes is through the development and test systems for testing before release into production. Only in exceptional circumstances are fixes applied directly to live, and then such releases are tightly managed. The system is backed up enabling a restoration to previous state if necessary. Wiltshire Council considers this matter is CLOSED. Wiltshire Council consider that the evidence and monitoring in place is satisfactory and that this matter is closed. SWAP are carrying out a further check on this at the request of Michael Hudson and if this is satisfactory we would request that KPMG agree that the monitoring is sufficient and agree the matter is closed. **Status:** Pending confirmation as to how it is ensured that any instances of unlocking the production environment for direct changes are detected, KPMG agree in principle that if the actions detailed above are implemented as described then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
5	1	**Powerful User Accounts - *Northgate*** There are a number of generic powerful user accounts in use for the Northgate system. Although an audit log is produced of all action carried out using these accounts, they are not reviewed and are overwritten every 4 weeks. This may result in the inability to attribute actions to an individual user or unauthorised persons gaining access to the system data. **Recommendation** The use of generic powerful user accounts, where more than one member of staff has access, should be kept to a minimum. Where they are required, regular monitoring of who has access to them should be carried out and a random sample of audit logs reviewed by a senior independent manager.	Access details for the powerful user accounts within the Northgate system are restricted to the Revenues and Benefits system team members. These team members have user accounts with the same level of access as these powerful users in order to minimise the circumstances when these accounts need to be used. The recommendation that the use of these accounts is monitored is accepted and procedures will be put in place for the Systems Manager and Head of Revenues and Benefits to do so on a four weekly basis. Responsible officer: Sally Kimber/Ian Brown Date: 1 July 2012 Update A documented process has been put in place and is now live. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
6	2	**Removal of user access - *Northgate*** The appropriate line manager is required to complete a leavers form for all leavers which is either emailed or sent in hard copy to the System Administrator, who will then revoke the user's access to Northgate. However, it was noted that very few leavers forms are received by the System Administrator If the System Administrator is not notified of all leavers in a timely fashion there is a risk that unauthorised persons may have access to the system data. **Recommendation** Remind all line managers of the requirement to promptly notify the System Administrator of all leavers.	Recommendation is accepted and in addition, the current users of the system will be checked on a regular basis to the Wiltshire Council directory to ensure that if any leavers have been missed, the relevant line manager can be contacted. Responsible officer: Sally Kimber Date: 30 June 2012 Update A documented process has been put in place and is now live. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
7	3	**Password Configuration Settings - Northgate** Password complexities within Northgate are managed on a profile basis. Each user is assigned to one of 8 individually configured profiles. Of the 8 profiles identified, 7 were noted to have an adequate level of complexity. The password parameters for the remaining profile, "FIRST_DEFAULT, do not comply with the Council password policy. **Recommendation** Amend the password parameters for the "FIRST_DEFAULT" profile in line with the Council's password policy.	Wiltshire Council has approached Northgate for advice regarding this recommendation as although it is accepted, management need to establish if there are any other implications that should be taken into account as this profile is used by the generic user accounts which are used to run specific jobs/processes. Responsible officer: Sally Kimber Date: 30 June 2012 Update Advice from Northgate is that this is not something that can be easily changed. The Council will continue to pursue this issue with the vendor to further assess the risk and apply risk management. Council view of status = IN PROGRESS **Status:** KPMG understand that this issue is difficult to address and is dependent on the vendor. As a result of the fact that the priority is only low and graded a '3', KPMG will review the impact on the audit approach of non compliance but anticipate that this can be accepted and no further work will be required.

No	Risk	Issue and recommendation	Management response and current status
8	3	**Review of user access - Northgate** No reviews of the appropriateness of user access has been performed since July 2011 and no documentary evidence has been retained for any reviews previously carried out. Without a regular review of system users there is a risk that unauthorised users may have access to the system data. **Recommendation** Undertake a review of all users on a regular (e.g. six monthly) basis to ensure that the level of access remains appropriate and all accounts for users who have left have been removed.	Recommendation accepted. Responsible officer: Sally Kimber Date: 31 July 2012 Update A documented process has been put in place and is now live. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
9	2	**Powerful user accounts - *Civica*** Powerful "system Administrator" access to Civica WebPay is controlled via assignment to the administrators user group. However, the System Administrator advised that, due to limitation in the system, it was not possible to generate a list of all users assigned to the administrators user group. "System Administrator" access within Civica Workstation is controlled via assignment of level 20 access. Of the 11 live accounts assigned with level 20 access, two ("system Administrator (001)" and "system Administrator (ww)") were identified for which the System Administrator was not aware of their purpose or who may have access to them. Of the two Civica databases one is hosted by the supplier and one by the Council. Council staff only have direct database access to Workstation. Access to the database is obtained via one of five SQL Database accounts. Of these two were disabled at the time of the audit. Of the remaining three accounts one is used by the application and cannot be used by an individual. Access to the remaining two accounts is restricted to a small number of ICT staff. No review of access is performed and passwords are not subject to periodic change. Without proper controls over such powerful user accounts there is a risk that unauthorised changes to the system data could be made and remain undetected. **Recommendation** The purpose of the two level 20 user accounts in WebPay which the System Administrator is unaware of should be investigated and, if appropriate, deleted. For the two SQL Database accounts , to which ICT staff have access, a log should be maintained showing who had access to the accounts and the date	At application level, the 001 account is used by automated system jobs and is not assigned to a real user. Will review the requirement and usage of the 001 account and other admin level accounts. There are two separate Civica databases: The WebPay database is hosted by the supplier. Wiltshire council staff have no direct access to this. The local 'workstation' database is stored on Wiltshire systems. Access is controlled by ICT. The 'ICON' account is used in the setup of the application. We will investigate the options around recording who has used the generic accounts on specific dates. Any issues etc are investigated and dealt with on an exceptions basis as all transactions are logged and traceable. Responsible officer: Neil Salisbury Date: December 2012 Update Action plan agreed, due date remains valid. Council view of status = IN PROGRESS **Status:** KPMG agree in principle that if the actions detailed above are implemented as described then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
10	2	**Removal of user access - *Civica*** Leavers cannot be clearly identified on the Civica WebPay system as a result of limited information within the system and the fact that the Syntax for the userID does not allow for the full user name. The Civica Workstation system does not permit the disablement or deletion of user accounts. Passwords are reset when the system administrator is notified that a user has left, however, there is no mechanism whereby this can be verified. The system administrator also confirmed that regular reviews of users are not carried out to ascertain if all system users are current and the level of access appropriate for their role. By not removing user accounts for users who have left, there is a risk that access to Council data could be gained by unauthorised persons. **Recommendation** Due to the system limitation it is more vital that regular reviews of users are carried out to identify where users have left or have changed roles and no longer require their current level of access.	We will undertake annual reviews of user accounts starting December 2012. Responsible officer: Neil Salisbury Date: 1 December 2012 Update A documented process has been put in place and is now live. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
11	2	**Monitoring of powerful user access by third parties - *Civica*** Access by external persons to the WebPay system is gained using the generic Administrator account. This is enabled only as and when requested. The availability of this account is managed exclusively by the System Administrator. Although a call is logged within the Civica support desk a call is not logged with the Council support desk. This is in contravention of the Council's policy. Third party access to the Workstation system is obtained through the use of the Civica_comino domain level user account. In order to access this account Civica are required to contact IT who issue a unique code, generated by a VPN secureID token which will enable Civica to connect to the Council network. The System Administrator confirmed that no monitoring is performed of actions undertaken by external users on either of the above accounts. **Recommendation** A call should be logged with the IT help desk to record when Civica have been granted access to the WebPay system. The System Administrator should carry out a periodic check of any changes made to the Workstation system using the Civica_Comino Domain account.	WebPay is hosted by Civica. They therefore have full access to the system environment. They are contractually obliged to provide a working system. However, they have no 'user' access to the application unless granted by Wiltshire. This is rare and is usually in response to a support call. We will look to get ODBC access (read only) to the hosted database to enable direct enquiries on user activity. We will ensure that a call is logged with Wiltshire's IT Service Desk when 'user' access is granted to Civica support personnel. The Civica_comino domain account is a Windows account. It carries no application access. Therefore, no direct changes can be made to the application using this account. – In order to gain access to the application as a 'user', this would have to be enabled by the system administrator. Responsible officer: Neil Salisbury Date: No further actions proposed. Update The process has been agreed and therefore this issue is considered closed. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented as described then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Issue and recommendation	Management response and current status
12	3	**Changes to system configuration - *Civica*** The System Administrator advised that configuration changes for Civica workstation such as changes to the processing rules are generally actioned by the system administration team and are. These changes are not logged within the service desk and are not subject to independent approval or progression via the ICT change control process. Changes are done in the test environment prior to being actioned in the live environment. Changes are performed by System Administrators using level 20 access. As these changes are not logged there is a risk that unauthorised changes could be made to the system configuration and impact on the accuracy or the system data. **Recommendation** All configuration changes should be logged with the service desk.	Wiltshire Council considered this a minor risk. Major system changes (new interfaces / upgrades etc) are formally tested and recorded. However, it is neither practical nor preferable to log ALL changes with the service desk and little if anything would be achieved by such procedures. Responsible officer: Neil Salisbury Date: No actions proposed. Update Council view of status = Wiltshire accept this issue and resulting risk. **Status:** KPMG have an assigned a low level priority to this issue and graded it a '3'. As a result KPMG acknowledge that Wiltshire Council accept the risk and will review the impact on the audit approach of non compliance but anticipate that this can be accepted and no further work will be required.

No	Risk	Issue and recommendation	Management response and current status
13	3	**Access to migrate changes to the Civica production environment** Access to migrate data to the test the live environments is performed via a generic SQL Database owner level account (ICON). The System Administrator confirmed that access to this account is restricted to a limited number of ICT personnel. However, the account password is not subject to periodic changed and the account is not monitored to validate or monitor any actions performed. The account password is stored within a central spreadsheet held by the security team. **Recommendation** Undertake a regular independent review of actions carried out using the ICON accounts.	Any issues are investigated on an exceptions basis. The 'ICON' account is used for ALL ODBC connections by the application. Therefore to attempt to conduct a full review of all actions carried out by this account would be unworkable and would achieve little. Responsible officer: Neil Salisbury Date: No further actions proposed. Update Council view of status = Wiltshire accept this issue and resulting risk. **Status:** KPMG have an assigned a low level priority to this issue and graded it a '3'. As a result KPMG acknowledge that Wiltshire Council accept the risk and will review the impact on the audit approach of non compliance but anticipate that this can be accepted and no further work will be required.

No	Risk	Issue and recommendation	Management response and current status
14	3	**Monitoring of scheduled jobs - *Civica*** All jobs are monitored on screen but there are no formal established procedures for conducting daily checks or reporting and resolving any errors caused through the overnight processing. No records of the actions taken to correct errors are maintained. **Recommendation** Introduce a formal process for daily checks on all scheduled jobs, and for reporting and resolution of any errors.	Scheduled jobs are monitored on an exceptions basis. We will implement a log of 'exceptions' to include comments, resolutions etc. Responsible officer: Neil Salisbury Date: 1 December 2012 Update Wiltshire accepts risk but will implement a log of exceptions to include comments and resolutions. Due date remains valid. Council view of status = Wiltshire accept this issue and resulting risk. **Status:** KPMG have an assigned a low level priority to this issue and graded it a '3'. As a result KPMG acknowledge that Wiltshire Council accept the risk and will review the impact on the audit approach of non compliance but anticipate that this can be accepted and no further work will be required.

No	Risk	Issue and recommendation	Management response and current status
15	3	**Change Control - *Civica*** All changes to the Civica WebPay are carried out by Civica. Civica will notify the Council of proposed changes and, if the Council does not raise any objections, will action the changes during system downtime. No assurances are received by the Council as to the level of testing carried out prior to the change actioned. For Workstation the System Administrator confirmed that no changes had been made during the financial year. It was noted that there is no documented change control process in place and no documentation is retained of changes made. Without a proper process in place there is a risk that unauthorised or untested changes could be made to the system which may compromise system performance and data. **Recommendation** Document the process for review, development, testing and approval of all system changes to the workstation. When changes are made documentation should be retained to provide evidence that the proper process had been followed.	For WebPay (hosted), Civica are contractually obliged to provide an up to date system. Therefore they apply software patches etc directly. Version / functionality upgrades etc are controlled by Wiltshire and are tested and logged etc. A basic process for upgrades etc will be documented. Responsible officer: Neil Salisbury Date: 1 December 2012 Update A documented process has been put in place and is now live. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented as described then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

Prior year recommendations

- The recommendations listed below have been extracted from KPMG's interim audit report.
- The numbering of the recommendations has been amended to remove the non IT points.
- The updates have been discussed with KPMG and we have included their comments in the status section of each recommendation.

No	Risk	Recommendation	Current status
1	1	**Direct changes to live environment – SAP** Introduce immediate logging / alerting of when the SAP production environment needs to be unlocked for direct changes to be made and ensure an adequate audit trail is recorded and retained every time for independent review of appropriateness.	It is only in exceptional circumstances that changes are made to the SAP system in production without first applying to test. In all cases where this is necessary all steps are taken to take and/or verify backups have been taken of the system. Update Council view of status = COMPLETE **Status:** KPMG note that a related and more detailed issue and management response has already been made and addressed within the points raised for 2011-12 – refer to point #4 in Appendix 1 entitled 'Resolution of problems directly in the SAP production environment'
2	1	**Monitoring of powerful application user accounts - *SAP*** Continue to identify where powerful user access can be removed if it is not deemed absolutely necessary. Controls should be formally developed to ensure that logs of powerful user access for both Wiltshire Council staff and Logica are sufficient, complete, and reviewed by an appropriately skilled independent resource.	The number of users with the SAP_ALL and/or SAP_NEW roles has decreased to 8 users, one Wiltshire Council user and 7 Logica users (there were 8 but a further one has recently been deleted). Wiltshire Council considers this to be an acceptable level of risk, particularly with reference to the support arrangements/contract described above. The SAP support team will continue to maintain the log of powerful user access and Logica have been requested to do the same. A member of IT security (an independent resource) will now be checking the logs on an agreed basis. A member of IT Security Rod Taylor (who sits in another service directorate and separate to Information Services and the SAP team) has agreed to inspect the SM 19/20 logs and a process is being developed with a meeting to agree this on the 4th September. Update Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.
3	1	**Change management procedures - *SAP*** Review the access assigned to all users on at least an annual basis to ensure the ongoing appropriateness of user access and ensure formally recorded and appropriately signed-off documentation is retained to support performance of this review.	This process is monitored via manager returns when a leaver occurs requesting cessation of authorisation; a monthly report generated after the payroll is run showing all leavers; a weekly report is generated showing all staff who have changed role within the council and therefore may need their access rights reviewed. All the reports are checked by the SAP team, verified and the documentation retained. In addition the council is currently running a systems review on the starter to leaver process and the monitoring of access rights forms part of that review. Any findings from the review that will improve the process further. Will be implemented. Update Council view of status = Complete **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Recommendation	Current status
4	1	**Change management procedures** ***Civica Icon systems, revenues and benefits systems and Simdell*** Ensure Council policies around change management are adhered to with regards to recording / retention of documentation produced for each key stage in the change management process and also for the default disabling of network user accounts used by third party support providers for remote access.	**Civica –** Superseded by point #15 in Appendix 1 entitled 'Change Control' **Simdell** – To be followed up during 2012-13 year end audit due to Simdell being replaced in 2013 **Revenues and benefits** – Superseded by implementation of new Northgate system, control will need to reviewed during 2012-13 year end audit **Status –** See updates for each individual application noted above
5	1	**Use of shared accounts for application administration duties** ***Civica Icon systems, revenues and benefits systems and Simdell*** Review all current user accounts with system administrator privileges for appropriateness of ongoing use. Create separate assigned powerful user accounts between the system administrator and the third party support provider. Also, introduce a regular independent monitoring process over these powerful user accounts (especially those used by the third party support provider).	**Civica –** Superseded by point #9 in Appendix 1 entitled 'Powerful user accounts' and point #11 in Appendix 1 entitled 'Monitoring of powerful user access by third parties' **Simdell** – To be followed up during 2012-13 year end audit due to Simdell being replaced in 2013 **Revenues and Benefits** – Superseded by point #5 in Appendix 1 entitled 'Powerful User Accounts' **Status –** See updates for each individual application noted above
6	1	**Use of shared accounts for database administration duties** ***Revenues and benefits systems, Civica Icon Workstation*** See comment made against issue number four, and in particular for Northgate consider immediate review and reduction in the number of excess accounts, especially in the development stage of the new Northgate system in December.	**Civica –** Superseded by point #9 in Appendix 1 entitled 'Powerful user accounts' **Simdell** – To be followed up during 2012-13 year end audit due to Simdell being replaced in 2013 **Revenues and benefits** – Superseded by implementation of new Northgate system, control will need to reviewed during 2012-13 year end audit **Status –** See updates for each individual application noted above
7	1	**Domain / server administrator access - *Network*** Ensure continuance of the internal review and update procedures noted above, ideally to be completed as soon as possible and reduce the number of domain and server level administrator accounts to appropriate and acceptable levels.	Following the restructure of ICT in August/September 2011 IS can demonstrate a reduction in powerful accounts in use. The Council requires change control to be applied to changes to powerful accounts and an audit/assurance process is in place to monitor changes. Information Assurance receive email alerts when accounts are modified. Update Council view of status = Complete **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.

No	Risk	Recommendation	Current status
7	2	**User access reviews - *SAP*** Review the access assigned to all users on at least an annual basis to ensure the ongoing appropriateness of user access and ensure formally recorded and appropriately signed-off documentation is retained to support performance of this review.	**Status:** KPMG note that a relevant detailed issue and management response has already been addressed within point #3 in Appendix 2 entitled 'Change management procedures'
8	2	**User access reviews - *Network*** Ensure continuance of the overall network user access review process, with particular focus on the more powerful user accounts.	**Outstanding**. See Internal Audit Report March 2012, recommendation 4 **Status:** Noted by KPMG as still in process of being resolved.
9	2	**Removal of user access for staff leavers – *SAP, Network*** Review the current access removal process to identify where potential improvements could be made to revoke access in a timely manner for user accounts relating to staff leavers and changes in staff position/role.	A process has been documented and made live within SAP support team above and beyond the standard leavers process. This process was initiated in September 2011. Council view of status = COMPLETE **Status:** SAP leavers process tested by KPMG during 2011-12 testing as operating without notable findings
10	2	**Removal of user access for staff leavers** ***Civica Icon, revenues and benefits systems, Simdell*** For Simdell and the revenues and benefits systems, amend the leavers notification process to at least include a regular check (e.g. monthly) of a HR-sourced leavers listing against a full user account listing. For Civica Icon (Webpay), undertake a full review of all current user accounts to identify those that are no longer required and adequately rename the remainder to facilitate a more robust access removal process.	**Civica –** Superseded by point #10 in Appendix 1 entitled 'Removal of user access' **Simdell – Outstanding.** See Internal Audit report May 2012, recommendation 2 **Revenues and Benefits** – Superseded by point #6 in Appendix 1 entitled 'Removal of user access' **Status –** See updates for each individual application noted above

No	Risk	Recommendation	Current status
11	2	**Automated job schedule controls – *SAP*** Ensure that system access to control key jobs / interfaces is regularly checked and introduce a procedure to formally record when key jobs / interfaces are monitored for successful completion.	Documented processes are in place and have been reviewed and assured by the South West Audit Partnership. Council view of status = COMPLETE **Status:** KPMG agree in principle that if the actions detailed above are implemented appropriately then the issue can be deemed as addressed – further audit work is required before full conclusion can be made.
12	2	**Access assigned to new/existing users** ***Revenues and benefits systems, Civica Icon Workstation, Simdell*** For the revenues and benefits systems, this procedure should be considered during the systems development stage of the new revenues and benefits system. For Civica Icon Workstation, review current process around new user account creation and ensure approval documentation is retained for at least 12 months to maintain a full audit trail. For Simdell, retain the user access requests and approval communications for at least twelve months before disposal to ensure a full audit trail is maintained.	**Revenues and benefits** – Superseded by implementation of new Northgate system, control will need to reviewed during 2012-13 year end audit **Civica – Outstanding** **Simdell –** To be followed up during 2012-13 year end audit due to Simdell being replaced in 2013 **Status –** See updates for each individual application noted above