KPMG

Leeds City Council

IT Audit Findings

September 2017

IT Audit Findings

Below are details of the individual points identified during the current years IT audit, in addition a summary of these and the status of prior year points will be included within the ISA260 report. Each point has an associated risk and recommendation for resolution or reduction in risk and impact. Each finding has also been assigned a risk rating, please see Appendix 1 for an explanation of ratings applied.

User Administration (FMS)	
Observation	User administration procedures relating to new access requests and monitoring changes to individuals jobs / roles could be strengthened, specifically: - 1 of the 40 users sampled for review was granted access to the application without having an request form completed per the access request procedure; and - Whilst a report of staff members changing roles exists there is no regular, proactive review of those individuals to ensure their access remains appropriate for job role. Management were able to provide retrospective approval for the new access request noted above.
Risk	**Low** - User Administration is one of the basic building blocks for a well controlled IT environment. Based on our experience, weaknesses that exist in user administration procedures are a common root cause for financial and transactional error, fraud and / or data leakage. Maintaining and consistently applying a robust set of control procedures therefore is crucial to minimising the risk of these occurring. It is noted that the risk is reduced in this instance through bi-annual reviews of FMS user access, as these reviews would identify any access not required for a user's current job role.
Recommendation	Management should consider periodically reviewing user administration process operation to ensure that a consistent level of control is being applied. Consideration should be given for review over key procedures i.e. mover access review. This would enable the identification of opportunities to enhance and develop those processes to reduce the opportunity for exceptions or control operator error to occur and not be identified in a timely manner.
Management Response	Schools systems controllers have been reminded of the need to ensure that the user access request form is received before new FMS users are set up. The main process for reviewing FMS user access rights is the six monthly review of all users' access, which should identify any changes required as a result of changes in role. Whilst it is possible to also identify and review access rights more quickly when users change to a different role, it is felt to be more important to target limited staff resources at ensuring FMS accounts for leavers are identified and closed promptly. The additional checks on staff moving post will be carried out as resources allow.

IT Audit Findings (cont.)

Privileged Access (SQL Database)	
Observation	Administration of the databases underlying both the SAP Payroll and FMS applications is undertaken via the Oracle Enterprise Cloud Manager tool. This tool has been configured to use generic Oracle Database super user accounts which are therefore shared amongst the database administrator team. Whilst use of these accounts is required for some activities (i.e. upgrades and applying patches) more day to day operational activity could be undertaken through accounts assigned to specific, named individuals with a level of delegated privilege.
Risk	**Low** – Where shared accounts are used the risk is created that activity can occur without ensuring individual user accountability. Where these shared accounts are regularly used and especially where these accounts have super user access assigned the risk is increased of inappropriate or unauthorised use of privileges to modify key financial data and / or system configuration. It is noted that for both applications the likelihood of negative impact is considered to be decreased as all individuals with access to the accounts are limited to the Leeds City Council Database Administrator team with details stored within the Technical Services Portal.
Recommendation	Management should, where possible, create additional user accounts to either ensure individual accountability for the use of high levels of privilege or to allow assignment of lower levels of privilege to individuals as required by their job role. Consideration should being given to performing a periodic review of usage logs for the shared super user accounts to confirm that all activity can be linked to an approved change or incident ticket, and to identify and investigate any potential misuse.
Management Response	Options will be explored for establishing an audit trail to identify which users have logged in using the standard Oracle super user accounts.

IT Audit Findings - Prior Year Update

Below are updates for each of the individual points identified during prior year IT audits that remain open. Each has an associated risk and recommendation for resolution or reduction in risk and impact. Each finding has been assigned a risk rating, please see Appendix 1 for an explanation of ratings applied.

System Configuration (SAP Payroll)	
Prior Year Observation	The SAP Payroll application is not consistently configured in a manner aligned to the Leeds City Council Password Policy or good practice. Configuration where misalignment has been identified includes enforcement of password complexity and overarching system security options that prevent misuse of a built in superuser account. Limited remedial activity has now occurred in response to the audit observations to align configuration within the SAP application to good practice.
Current Year Observation	**Part Resolved** – It is noted that the overarching system security options are now aligned with good practice. However it is noted that passwords, specifically in relation to complexity continue to not be aligned to both good practice and Leeds City Council Password Policy. Whilst a new password policy is being developed by the Council this has not been implemented during the audit period.
Risk	**Low** – Where applications are not aligned to good practice or internal standards, the risk is increased that inappropriate or unauthorised access may be gained. Passwords are a key component of the information security environment required to protect systems and the data held therein. It was noted the SAP application does require passwords to be in place, of a suitable length and changed periodically therefore the risk is reduced. Also that for all instances of privileged or administrator access confirmation was provided by management that staff were sufficiently knowledgeable and experienced to manually select strong, complex passwords.
Recommendation	Management should review and amend the password configuration within the systems to ensure alignment to both the internal policy and also to good practice. Where this is not possible a risk assessment should be undertaken to review, mitigate, monitor and if required accept the resulting risk.
Management Response	The council is in the process of introducing a new password policy, which has different requirements from the previous policy which the 2015/16 finding refers to. Work is underway to assess how the new policy can be best implemented for SAP passwords.

IT Audit Findings - Prior Year Update (cont.)

System Password Parameters (SQL Database / UNIX Servers)	
Prior Year Observation	The passwords used within the infrastructure underlying the SAP payroll and FMS applications are not configured in a manner aligned to the Leeds City Council Password Policy or good practice. The components effected includes: • Oracle Databases; • UNIX Servers hosting the Applications / Databases; and • Technical Services Portal (used to store Admin shared passwords for the above). Aspects of password configuration where the expected standards are not enforced include minimum length, complexity, history, rotation and account lockout.
Current Year Observation	**Open** - No change to system configuration or policy was noted during the 2017 IT Audit. Whilst a new password policy is being developed by the Council this has not been implemented during the audit period.
Risk	**Medium** – Where passwords are consistently not aligned to good practice or internal standards, the risk is increased that inappropriate or unauthorised access may be gained to applications, servers and databases. Passwords are a key component of the information security environment required to protect systems and the data held therein. It was noted that for all instances of privileged or administrator access confirmation was provided by management that staff were sufficiently knowledgeable and experienced to manually select strong passwords and change them regularly.
Recommendation	Management should review and amend the password configuration within the systems to ensure alignment to both the internal Council policy and also to good practice. Where this is not possible a risk assessment should be undertaken to review, mitigate, monitor and if required accept the resulting risk.
Management Response	The council is in the process of introducing a new password policy which has different requirements from the previous policy, which the 2015/16 finding refers to. Work is underway to assess how the new policy can be best implemented for the infrastructure passwords referred to above.

IT Audit Findings - Prior Year Update (cont.)

Change Management – Approval to Implement Changes (SAP Payroll / FMS)	
Prior Year Observation	Change management procedures relating to approval of changes prior to implementation have not been consistently followed within the SAP Payroll and FMS applications, specifically: • Evidence of appropriate approval for changes to be deployed on the SAP Payroll application was not provided for 7 of the 40 changes sampled. It was noted this included 4 instances of appropriate approval not being granted and 3 instances where changes had been developed directly within the live environment. • Evidence of appropriate approval for changes to be deployed into the FMS live application environment could not be provided for 1 of the 8 changes sampled. It was noted this was due to the approval being granted by an individual more junior than required per policy guidelines. For both applications all changes have been granted retrospective approval by an appropriate member of staff.
Current Year Observation	**Part Resolved** – In relation to SAP Payroll, all 40 changes sampled for inspection were noted to have been appropriately documented, approved and developed within the appropriate application environment. In relation to FMS, 1 of the 6 changes sampled for inspection was noted to not have evidence retained of its testing, segregation between its implementer and developer and of approval being granted prior to its implementation in the live system. Management provided retrospective confirmation this change was appropriate and noted that this was primarily a documentation retention issue.
Risk	**Low** – Where the change management process is not appropriately evidenced the risk is increased that changes may be deployed into the live environment without completing the full change management procedure and could then have an negative impact on system availability and the related business operations.

IT Audit Findings - Prior Year Update (cont.)

Change Management – Approval to Implement Changes (SAP Payroll / FMS) Cont.	
Recommendation	Changes should not be implemented into the live application environment without completing the full change management procedure and with each stage of the procedure being appropriately evidenced. Management should consider periodically reviewing the change management procedure operation to ensure that controls are consistently being applied across all changes.
Management Response	Procedures for documenting changes to FMS were improved during 2016/17. This should ensure that documentation of testing is always retained even for very minor changes such as this one.

IT Audit Findings – Prior Year Update (cont.)

User Access – Privileged Users (SAP Payroll)	
Prior Year Observation	There are 2 generic, user accounts assigned privileged / administrator access within the SAP Payroll application which management confirmed did not currently require the level of privilege assigned. In 1 instance it was noted that the account had previously been required for internal IT operational use but that this function has been outsourced to a third party within the 6 months prior to the audit without a corresponding update to the accounts assigned access.
Current Year Observation	**Open** – It was noted that both of these accounts were still active and had retained this level of elevated access. From discussion with management it was understood that amending these accounts requires a lengthy review and testing process to avoid any impact on the system operation and that changes were planned. In addition it was noted that a number of users had transactional level access privileges assigned which were not required for their job roles, specifically: - Two users were assigned the ability to make changes to the application at the table level should the system be open. - All active users were noted to have the ability to assign roles to other user accounts, however it was observed that this was no an option accessible via the standard user interface. Additional testing confirmed that this privilege had not been misused by individuals whose job role does not include role assignment / user maintenance. In both instances management confirmed this had occurred due to this access being part of legacy profiles assigned to users. These points were identified this year due to additional in-depth audit testing of user access being undertaken based on the prior year audit finding.
Risk	**Medium** – Where application privileged access has been granted or retained inappropriately the risk is increased that inappropriate or unauthorised use of privileges may occur, including the modification of financial data or system configuration. It was noted that the restriction on use of the accounts assigned administrator level access to a small number of system administrators within the SAP support teams limited the potential for negative impact to the system operation and data held therein. Similarly based on the additional testing undertaken it was possible to gain assurance that the transactional level privileges had not been abused.

IT Audit Findings – Prior Year Update (cont.)

User Access – Privileged Users (SAP Payroll) Cont.	
Recommendation	Periodic reviews should be undertaken over all accounts with privileged access assigned. Privileged access should be removed from all user accounts where it is not required for current tasks or an individuals job role.
Management Response	The two generic IDs are needed to enable batch jobs to be run. A technical solution has now been found to change the account type of these IDs, so that they cannot be logged in to by users. The access rights of the two users who had the ability to make changes at the table level have been amended. The inclusion within the self service user role of the ability to assign roles to other user accounts has been removed. This function did not appear on the menus available to these users, who would thus have been unaware that they had such rights. Even if they had been aware of it, users would have required a very high level of technical knowledge of the SAP system in order to misuse this function, given that it did not appear on their menus.

IT Audit Findings - Prior Year Update (cont.)

System Password Parameters (SAP Payroll / FMS)	
Prior Year Observation	The passwords assigned to privileged accounts within the SAP Payroll and FMS applications and supporting infrastructure are not configured in a manner aligned to the Leeds City Council Password Policy. The components effected includes: • Applications; • Oracle Databases; • UNIX Servers hosting the Applications / Databases; and • Technical Services Portal (used to store Admin shared passwords for the above). Internal standards specify increased requirements for the passwords associated with privileged accounts within the applications and infrastructure, however this has not been implemented and therefore is not automatically enforced.
Current Year Observation	**Open** - No change to system configuration or policy was noted during the 2017 IT Audit. Whilst a new password policy is being developed by the Council this has not been implemented during the audit period.
Risk	**Low** – Where passwords are consistently not aligned to internal standards, the risk is increased that the information security environment may not be enforced consistently across the IT estate. This could lead to inconsistent application configuration allowing inappropriate or unauthorised access to be gained to applications, servers and databases. It was noted that the underlying policy mandated configuration for non-privileged users is aligned to good practice for both privileged and non-privileged users. This finding therefore refers primarily to inconsistencies between policy and privileged access system configuration.
Recommendation	Management should review and amend either the internal standards or password configuration within the systems to ensure consistent alignment and clearly defined security standards.
Management Response	The council is in the process of introducing a new password policy which has different requirements from the previous policy, which the 2015/16 finding refers to. Work is underway to assess how the new policy can be best implemented for the account passwords referred to above.

IT Audit Findings - Prior Year Update (cont.)

User Access – Users Access Reviews (SAP Payroll)	
Prior Year Observation	The SAP Payroll application user access review is focused on the continued requirement for application user licences and does not consider the level of access assigned to individual users. This review would therefore not identify individuals who had changed duties within their job role and inappropriately retained elevated or privileged SAP Payroll access.
Current Year Observation	**Open** – Pilot user access reviews have occurred as part of creating a process for reviewing and verifying SAP Payroll user access, however development is still ongoing and the majority of users have not had their assigned access reviewed during the audit period.
Risk	**Low** – While user access reviews are considered a compensatory control to ensure a well controlled and restricted user population they do undertake an essential function to ensure all access, including privileged or administrator access continues to be required and is appropriately approved.
Recommendation	Management should continue to develop the process to effectively review user access within the SAP Payroll application. Once completed this should be applied as a priority to those teams and departments within the Council which are considered the highest risk based on factors including level of SAP access, risk of breaching segregation of duty and level of staff turnover / movement between roles.
Management Response	Monthly checks are undertaken to ensure that those users who no longer require SAP access are identified. Managers will consider the options to determine a practical approach to reviewing the access rights of ongoing users within SAP.

Appendix 1 - IT Audit Findings – Risk Ratings Key

High priority:	Medium priority:	Low priority:
A significant weakness in the system or process which is putting you at serious risk of not achieving your strategic aims and objectives. In particular: significant adverse impact on reputation; non-compliance with key statutory requirements; or substantially raising the likelihood that any of the strategic risks will occur. Any recommendations in this category would require immediate attention.	A potentially significant or medium level weakness in the system or process which could put you at risk of not achieving your strategic aims and objectives. In particular, having the potential for adverse impact on the reputation of the business or for raising the likelihood of strategic risks occurring.	Recommendations which could improve the efficiency and/or effectiveness of the system or process but which are not vital to achieving strategic aims and objectives. These are generally issues of good practice that the auditors consider would achieve better outcomes.