KPMG

Leeds City Council

IT Audit Findings

July 2018

IT Audit Summary

The tables below provide a summary overview of findings from the current year and the updated status of prior year findings.

Current Year:

Low	Medium	High
2	0	0

Prior Year:

Status	Low	Medium	High	Total
Open	1	1	0	2
Part Implemented	2	1	0	3
Closed	3	0	0	3

KPMG

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.

Change Management (SAP Payroll)	
Observation	A number of users are assigned transactional level access on the SAP Payroll application that would allow them to independently develop and implement changes to the live application functionality or configuration without requiring another users approval. It was noted that during the audit period 8 changes had been developed and implemented on the live application by the same individual. Management were able to provide retrospective, independent confirmation that the changes made were in line with the relevant change request and approval which had been granted.
Risk	**Low** – Changes could be made to the live application without having followed the formally defined change procedure. Where changes do not consistently follow the change management process there is the risk that changes could be implemented that would negatively impact on system functionality and availability. This issue is raised as low risk due to the functionality being available within SAP for review of all changes made which confirmed only a small number of changes had been implemented and approved by the same individual and these all had supporting justification.
Recommendation	The ability to develop and implement changes should be assigned to different individuals, with system access updated to reflect this. Where this is not possible due to limitations on resource availability, proactive monitoring of user activity with periodic reviews should be undertaken to ensure that all changes made to the live application can be linked to an approved change request.

IT Audit Findings

Change Management (SAP Payroll)	
Management Response	Processes are in place so that implementation of changes is normally carried out independently from the developer of the change. However, these eight incidents occurred due to a number of factors, including work completed by different teams where changes had to be implemented in a particular order to allow for the configuration to work, and one incident due to an error in how changes were working, where our external support (Mandant Solutions Ltd) had supplied a fix and needed it testing and only the developer was available to move this through the system. This was monitored by the Managers. Steps are already in place to ensure that this should not happen, however, mentoring has been introduced to ensure that where incident like this which cannot be avoided that these are documented clearly. **Responsible:** Principal System Support Officer **Due date:** In place

IT Audit Findings (cont.)

User Administration (SAP Payroll)	
Observation	User administration procedures relating to new access requests and revoking leaver access could be strengthened, specifically: - 1 of the 25 users sampled for review was granted access to the application without having a request form completed as per the access request procedure; and - 3 users had retained access to the application after their stated leaving date. All users were confirmed to only hold self service access therefore did not have access to privileged system functionality. 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 all users identified by audit testing did not have privileged access therefore the risk created is low.
Recommendation	Management should consider periodically reviewing user administration process operation to ensure that a consistent level of control is being applied.
Management Response	Changes are being put into place so that all new user access to be granted is submitted via Remedy, which should ensure that no authorisation documentation should be misfiled. In addition we are introducing a monitoring system so that when access is removed from users as part of the monthly maintenance where a comparison is taken between the employee’s leaving date and the date they last accessed the systems, these will then be followed up at the time with the managers. **Responsible:** Principal System Support Officer **Due date:** In progress, partially implemented

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.

User Administration (FMS)	
Prior Year Observation	2017 Finding: 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 a 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.
Current Year Observation	**Part Resolved** - We noted that all FMS users sampled for review had followed the appropriate access request process. We noted that proactive reviews of those individuals who change role still do not occur to ensure their access remains appropriate.
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

IT Audit Findings – Prior Year Update

User Administration (FMS)	
Management Response	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. **Responsible:** Principal Finance Manager **Due date:** Ongoing

IT Audit Findings - Prior Year Update (cont.)

System Configuration (SAP Payroll)	
Prior Year Observation	2016 Finding: 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. 2017 Update: 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.
Current Year Observation	**Part Resolved** – It is noted that the overarching system security options continue to be 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 continues to be 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.

IT Audit Findings - Prior Year Update

System Configuration (SAP Payroll)	
Management Response	Management will consider how best to apply the new password policy to the SAP system. **Responsible:** Principal System Support Officer **Due date:** October 2018

IT Audit Findings - Prior Year Update (cont.)

System Password Parameters (Database / UNIX Servers)	
Prior Year Observation	2016 Finding: 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 affected 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. 2017 Update: 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.
Current Year Observation	**Open** - No change to system configuration or policy was noted during the 2018 IT Audit. Whilst a new password policy continues to be 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.

IT Audit Findings - Prior Year Update

System Password Parameters (Database / UNIX Servers)	
Management Response	The new password policy is now enforced at the OS level for all UNIX servers and for database accounts. **Responsible:** ICT Infrastructure Manager **Due date:** In place

IT Audit Findings – Prior Year Update (cont.)

User Access – Privileged Users (SAP Payroll)	
Prior Year Observation	2016 Finding: 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. 2017 Update: 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 not 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.
Current Year Observation	**Part Resolved** – It was noted that both of the generic accounts had this access removed and / or been made inaccessible to all users. The ability to make changes to the application at table level had also been removed where not required for a job role. However it was noted that all active users continued to have transactional level access privileges assigned which grant them the ability to assign roles to other user accounts. It was understood that this continues to be an option accessible via the standard user interface and additional testing confirmed that this privilege had not been misused by individuals whose job role does not include role assignment / user maintenance. Management confirmed this had occurred due to this access being part of legacy profiles assigned to users.

IT Audit Findings - Prior Year Update (cont.)

User Access – Privileged Users (SAP Payroll)	
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 based on the additional testing undertaken it was possible to gain assurance that the transactional level privileges had not been abused however a level of risk remains.
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	As last year whilst some users have the rights to assign roles within the pre-designed access rights they do not have access to the transaction to assign roles, processes are in place to ensure that these transactions are never assigned to users who do not have the right as part of their job to assign roles. **Responsible:** Principal System Support Officer **Due date:** In place

IT Audit Findings - Prior Year Update (cont.)

System Password Parameters (SAP Payroll / FMS)	
Prior Year Observation	2016 Finding: 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. 2017 Update: 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.
Current Year Observation	**Open** - No change to system configuration or policy was noted during the 2018 IT Audit. Whilst a new password policy continues to be 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.

IT Audit Findings - Prior Year Update

System Password Parameters (SAP Payroll / FMS)	
Management Response	FMS : A system development has been approved for FMS which will align all users' passwords to the level of complexity required in the new policy for privileged users. This will be implemented as soon as development resources allow. **Responsible:** Principal Finance Manager **Due date:** September 2018 SAP: Investigations are underway to see if it is possible to change the password to meet the new policy. **Responsible:** Principal System Support Officer **Due date:** October 2018

IT Audit Findings - Prior Year Update (cont.)

Privileged Access (Database)	
Prior Year Observation	2017 Finding: 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.
Current Year Observation	**Closed** – Individual user accounts have been added within the Oracle Enterprise Cloud Manager tool, generic super user accounts should now only be used in specific circumstances where required.
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.

IT Audit Findings - Prior Year Update (cont.)

Change Management – Approval to Implement Changes (SAP Payroll / FMS)	
Prior Year Observation	2016 Finding: 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. 2017 Update: 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.
Current Year Observation	**Closed** – All changes sampled on both the FMS and SAP Payroll applications had followed the change management process as specified.
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.)

User Access – Users Access Reviews (SAP Payroll)	
Prior Year Observation	2016 Finding: 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. 2017 Update: 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.
Current Year Observation	**Closed** – A user access review is currently being undertaken to review and verify all SAP Payroll user access, this is then planned to be repeated periodically in the future.
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.

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.