Leeds City Council

IT Audit Findings

November 2016

IT Audit Findings – Risk Ratings Key

Within the following section a listing is provided of IT audit findings from the current year IT audit. For each finding a risk rating has been assigned, please see below for an explanation of each rating assigned.

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.

IT Audit Findings

Below are details of the individual points identified during the current years IT audit. Each has an associated risk and recommendation for resolution or reduction in risk and impact.

System Configuration (SAP Payroll)	
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.
Risk	**Medium** – Where applications 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 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	Service Managers will work with ICT to investigate the options available around strengthening of password configuration for SAP and seek to apply where possible within the next 3 months. It should be noted that the council's password policy states that the recommended password structures should be implemented 'where possible' i.e. taking into account the functional capabilities of each system.

IT Audit Findings (cont.)

System Password Parameters (SQL Database / UNIX Servers)	
Observation	The passwords used within the infrastructure underlying the SAP and FMS application 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. It is noted that these issues were not identified during the May 2016 internal audit over the FMS application as these components of system operation were not in scope.
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's password policy is currently undergoing a review, which is scheduled to be completed in spring 2017. Once the revised password policy is finalised, the options for password structure for system passwords will be reviewed. It should be noted that the existing policy states that the recommended password structures should be implemented 'where possible' i.e. taking into account the functional capabilities of each system, and also that CESG guidance is changing, and forcing frequent password changes is now seen as increasing risk.

IT Audit Findings (cont.)

Change Management – Approval to Implement Changes (SAP Payroll / FMS)	
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. In addition we note that the May 2016 internal audit over the FMS application did not identify this issue due to test procedures focusing on procedural design and not providing coverage of its operation.
Risk	**Medium** – Where changes are not approved or are approved at an inappropriate level 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.
Recommendation	Changes should not be implemented into the live application environment without appropriate approval. Evidence of approval being granted prior to changes being deployed should be consistently retained to ensure this critical procedural step occurs and ensure accountability in the event of a change having an adverse effect on the application or database operation.

IT Audit Findings (cont.)

Change Management – Approval to Implement Changes (SAP Payroll / FMS) Cont.	
Management Response	SAP The SAP Development Team have been reminded of processes to ensure all appropriate authorised documentation is completed prior to making any changes. However, this is not always feasible where urgent fixes are required ‘in the moment’ for example to fix a payroll processing problem. Such instances would be recorded as emergency changes, with appropriate retrospective confirmation. Changes would only be made to the live system with prior authorisation from senior managers. FMS This change was approved by a junior member of staff to ensure that the correction could be implemented promptly, as more senior officers were unavailable. The decision to implement the change in this instance was based on an assessment of risk, which took into account the complexity of the change, and the fact that it had been agreed by the client team for FMS. The change management procedure is to be amended to take account of a slightly revised process for the approval of urgent changes.

IT Audit Findings (cont.)

User Access – Privileged Users (SAP Payroll)	
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.
Risk	**Low** – Where application privileged access has been granted or retained inappropriately the risk is increased that inappropriate or unauthorised use of administrator privileges may occur, including the modification of financial data or system configuration. It was noted that the restriction on use of these accounts 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.
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	A review of user account maintenance processes will be undertaken and improvements made and applied within the next 3 months.

IT Audit Findings (cont.)

System Password Parameters (SAP Payroll / FMS)	
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. It is noted that the inconsistency between policy and system configuration was not identified during the May 2016 internal audit over the FMS application.
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's password policy, including distinguishing between standard, privileged and systems users, is currently subject to a review which is due to be completed in spring 2017. It should be noted that the policy states that the recommended password structures should be implemented 'where possible' i.e. taking into account the functional capabilities of each system. Once the password policy is finalised, the options for password structure for those users identified as privileged users in SAP and FMS will be reviewed.

IT Audit Findings (cont.)

User Access – Users Access Reviews (SAP Payroll)	
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.
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 consider expanding the scope of the current SAP application licence review to include periodic review of user access assignments and confirmation of the ongoing requirement for access held, specifically those account holding privileged or administrator access.
Management Response	A review of SAP user account maintenance processes will be undertaken and improvements made and applied within the next 3 months.