Grant Thornton
An instinct for growth™

Leeds City Council

Information Technology Audit Report

Year Ended 31st March 2020

CONFIDENTIAL

Grant Thornton
An instinct for growth™

Contents

1. EXECUTIVE SUMMARY

1.1 Introduction

To support its opinion on the financial statements of Leeds City Council, Grant Thornton has completed the design effectiveness of the IT General Controls (ITGC) within the IT environment, as they affect the financial statements for year-ended 31st March 2020.

The IT audit at Leeds City Council was a limited scope review. This report sets out the summary of observations, scope of the work, the detailed observations and recommendations for control improvements. This included completing a SAP technical review, which covered the controls relating to Leeds City Council's SAP Basis components.

The matters raised in this report came to our attention as a result of the limited scope ITGC and SAP design review and are matters that we believe needed to be brought to your attention. Therefore, our comments cannot be expected to include all possible control improvements that a more wide-ranging engagement might identify.

We would like to take this opportunity to thank all the staff at Leeds City Council for their assistance in completing this IT Audit.

1.2 Summary of Observations

- **Security & Access Controls:** Control weaknesses were noted in the Security and Access of Leeds City Council's SAP Payroll system. These weaknesses include:
  - End users granted inappropriate access to run programs from command line on SAP Payroll
  - Default / built-in accounts unlocked within SAP Payroll
  - Inadequate audit logging on SAP Payroll
  - Change management segregation of duties conflicts on SAP Payroll

- **IT General Controls:** Control weaknesses were noted in Leeds City Council's general IT controls related to other applications. These weaknesses include:
  - Inappropriate finance team access granted to IT support staff members on FMS
  - Inadequate information assurance policy

2. SCOPE & SUMMARY OF WORK COMPLETED

The primary objective was to complete an ITGC design review of Leeds City Council's FMS, Capita Academy, SAP Payroll and, to a limited extent, Windows Active Directory to support the Financial Statements audit. The SAP security and authorisation review was performed by manually extracting user access listings while onsite and performing walkthroughs of the FMS, Academy, Active Directory and SAP controls.

We completed the following tasks, as part of this IT Audit:

- IT General Controls (Design Effectiveness on FMS, Academy, SAP Payroll and Active Directory);
- Completed security and authorisation review of Leeds City Council's SAP system;
- Performed high level limited testing of configurable controls in the above areas within SAP; and
- Documented the test results and provided evidence of the observations to application support teams for remediation actions where necessary.

3. CLASSIFICATION OF RECOMMENDATIONS

The observations contained herein and the detailed recommendations supporting the individual points are broadly classified into two classifications. The assessment for each observation is a reflection of the effect the findings have upon internal control and the Financial Statements.

Assessment	Key to assessment of internal control deficiencies
●	Significant Deficiency - risk of significant misstatement
●	Deficiency - risk of inconsequential misstatement

4. DETAILED OBSERVATIONS AND RECOMMENDATIONS

The detailed observations and recommendations are grouped into following categories:

- **SAP Basis (technical) Review Observations** – Section 4.1 provides a technical review covering access and security controls within Leeds City Council's SAP Payroll system.
- **IT General Controls Observations** – Section 4.2 provides details of the ITGC observations related to the FMS and Academy systems and the Leeds City Council's Active Directory.

4.1 SAP Basis (Technical) Review Observations

As a general comment, please note that the number of users shown below only includes valid and unlocked dialogue users, unless otherwise specified.

No	Observation and Risk	Recommendation & Management Response	Assessment
1	**End users granted inappropriate access to run programs from command line on SAP Payroll** During our audit, we observed that there were 12 users from the BSC Pensions and FIM/NIP Teams with access to run programs from command line via the SAP transaction SA38. Per discussion with the SAP Lead Application Officer, we understood that a report was created for the BSC Pensions team, which they were currently testing through this transaction at the time of the audit, with a view to have this moved onto their normal profile once development was complete. We were informed that following our audit the process was completed and access revoked subsequent to our audit and that the access was also revoked from the FIM/NIP team. Additionally, the Lead Application Officer informed us that a monthly reporting process would be introduced with the objective of identifying inappropriate access to sensitive SAP transactions. Inappropriate access to sensitive transactions and authorisation objects within SAP increases the risk of	No further action recommended by management as the finding / inappropriate access was revoked subsequent to our audit. **Management Response:** *This issue was addressed during the course of the audit, and monthly checks are now underway.*	Deficiency 

No	Observation and Risk	Recommendation & Management Response	Assessment
	account misuse and processing of unauthorised transactions. Considering that account level activity is not logged and reviewed, there risk exists that any misuse will also go undetected by management.		
2	**Default / built-in accounts unlocked within SAP Payroll** During our audit, we observed that two default / built in user accounts (DDIC and or SAP*) were unlocked on SAP Payroll system. We however also observed that at the time of the audit both accounts had their passwords changed from the commonly known default values and neither accounts were set to accessible user types (User Type System). SAP standard accounts such these are often assigned the highest system privileges and are a target for unauthorised access attempts. The standard accounts do not need to be active in the system and increase the risk of unauthorised access if not locked down. Further the DDIC/SAP* accounts are often associated with background processes which will fail if the account is system locked when the number of failed login attempts parameter is exceeded.	We recommend that management should consider locking these accounts and, where possible, removing processes that run on the via the DDIC / SAP* accounts. **Management Response:** *Officers are investigating what obstacles there are to locking the DDIC and SAP* roles, and whether these can be removed.*	Deficiency ●

No	Observation and Risk	Recommendation & Management Response	Assessment
3	**Inadequate audit logging on SAP Payroll** During our audit, we observed that audit logging within the SAP system, specifically automatic recording of SAP transaction (function) usage, was set to the default value / not enabled. This is configured through the following parameter: • rsau/enable = 0 Without adequate audit logging and subsequent monitoring of logs retained, the risk is significantly increased that unauthorised activities, including but not limited to, inappropriate changes to users, the system and data therein will not be identified in a timely manner.	We recommend that management should consider updating the SAP audit logging configuration in line with the Council's application and data security objectives, and may consider the following parameter value: • rsau/enable = 1 As part of enabling audit logging we would recommend that management review the users and transactions covered to ensure appropriate focus on high risk SAP transactions (functions), users with elevated levels of access and / or those users with most exposure to segregation of duty threats (i.e. combinations of IT and business responsibilities / access). A process should also be implemented for independent, periodic monitoring of logs produced. **Management Response:**	Deficiency

No	Observation and Risk	Recommendation & Management Response	Assessment
		Officers are discussing with the council's SAP technical support provider, and seeking to make changes to these parameters.	
4	**Change management segregation of duties conflict on SAP Payroll** During our audit, we observed Segregation of Duties conflicts due to access assigned within the SAP Development, Quality Assurance (QA) and Production / (live) environments. Specifically, 1 SAP user (BOWLIM) possessed a development key and change transportation permissions (via STMS) in both the QA and Production environments. This would allow a user to create a change in the development environment and transport it into QA and then into the live environments. Additionally, the same user had access to open the system for direct change (via SCC4) and make changes to the system coding (via SE38). This would allow the user to open the SAP system for direct change and make those changes. Where change management segregation of duties is not maintained the risk is created that individual user are able to develop and implement changes without independent	No further action recommended as the finding/inappropriate access was revoked subsequent to our audit. **Management Response:** *This issue was addressed during the course of the audit.*	Deficiency

No	Observation and Risk	Recommendation & Management Response	Assessment
	approval and / or review. We were informed that following our audit this access combination had been removed from the relevant user.		

4.2 IT General Controls Review Observations

No.	Observation and Risk	Recommendation & Management Response	Assessment
5	**Inappropriate finance team access granted to IT support staff members on FMS** During our audit, we observed that 4 members of IT Application support team with Level 1 (Administrator) access to FMS also had access / ability to post journals on the FMS system. This creates a segregation of duties conflict as these users are also undertake FMS user administration (including, but not limited to, changing assigned access levels and creating new users) and this access combined with journal posting abilities creates risk of circumvention of system controls. Specifically, inappropriate access to finance functions by members of IT with level 1 privileged access on FMS may	We recommend that management review and remove access to finance functions within FMS e.g. posting and approving of journals for members of IT with Level 1 access. Where this is not possible due to operational requirements or technical limitations, we recommend that management should implement monitoring to periodically review activity by these users (i.e. journals posted) to ensure it is appropriate.	Deficiency ●

No.	Observation and Risk	Recommendation & Management Response	Assessment
	grant them the opportunity to process unauthorised transactions without management detection.	This should be formally documented and completed by an individual independent of the IT application support team. **Management Response:** *The council already had in place a system to check on a quarterly basis for the more significant risk of payment or order activity by IT support staff. Following the audit this has been extended to cover lower risk activity such as journals by these staff.*	
6	**Inadequate Information Security Assurance Policy** During our audit, we noted that an Information Security Assurance Policy is documented. However, this policy did not address the below key areas of information security standards noted within the document as requiring detailed specification: • Governance; • Employee security • Training and awareness; • Network and access control; and	We recommend that management develop additional documentation in the following key areas of information security in support of the existing Information Security Assurance policy: • Governance; • Employee security • Training and awareness; • Network and access control; and	Deficiency

No.	Observation and Risk	Recommendation & Management Response	Assessment
	• Physical security. Without adequate information security policies and procedures, the risk is increased that the actions carried out by council staff will not support the organisation's security objectives, and this in turn may result in confidentiality, integrity or availability issues.	• Physical security. **Management Response:** *Those documents listed above which are not already in place are scheduled to be covered as part of an ongoing review programme for policies within DIS.*	

Grant Thornton
An instinct for growth™

5. FOLLOW UP OF PRIOR YEAR FINDINGS

No.	Summary issue and risk previously communicated	Follow up commentary	Status
	Generic user accounts on Academy During our review, we noted that there were generic user accounts on Academy, below are the details: **Academy** • tr2, tr3, tr4, tr5, tr6 • train1, train3, train4, train5, train6 Generic ids are well known in the public domain, so they tend to be one of the areas that external hackers will probe first, when attempting access. Failure to take precautions against the use of generic ids may leave the Council exposed to unauthorised access through these accounts. This is particularly important if the default accounts in question have sensitive access rights.	Generic user accounts were not identified on Academy as part of the 2019/20 IT audit.	Closed