



IT Audit Findings

Leeds City Council

Year ended : 31 March 2023

Issued Date : 14 November 2023

Chris Houghton

Senior Manager, IT Audit

T: +442077282276

E: chris.houghton@uk.gt.com

Arpita Seth

Technology External Audit Assistant Manager

D +44 (0)20 7728 2331

E: Arpita.Seth@uk.gt.com

Karun Wadhera

Technology Audit OTM

T: +442071844417

E: Karun.Wadhera@uk.gt.com

Vikramsinh P Thorat

Senior OTM IT Audit

E: Vikramsinh.p.thorat@uk.gt.com



Contents

Section	Page
1. Executive summary	3
2. Scope and summary of work completed	4
3. Details of IT audit findings	5
4. Review of IT audit findings raised in prior year	12

Section 1: Executive summary

01. Executive summary

02. Scope and summary of work completed

03. Summary & Details of IT audit findings

04. Review of IT audit findings raised in prior year

To support the financial statement audit of Leeds City Council for year ended 31 March 2023, Grant Thornton has completed roll forward testing, followed up on prior year's findings and re-tested privileged access controls for the in-scope applications FMS, Capita (Academy) and SAP. Grant Thornton has also completed a design and implementation review of the IT General Controls (ITGC) for the Civica CX application identified as relevant to the audit.

This report sets out the summary of findings, scope of the work, the detailed findings and recommendations for control improvements.

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

Section 2: Scope and summary of work completed

01. Executive summary

02. **Scope and summary of work completed**

03. Summary & Details of IT audit findings

04. Review of IT audit findings raised in prior year

The objective of this IT audit was to complete a design and implementation review of Leeds City Council ITGC to support the financial statement audit. The following applications were in scope for this audit:

- Capita Academy
- FMS
- SAP
- Civica CX
- Active Directory

We completed the following tasks as part of this ITGC review:

- IT General Controls Testing: Design, implementation assessment over controls for security management; technology acquisition development and maintenance; and technology infrastructure.
- Performed high level walkthroughs, inspected supporting documentation and analysis of configurable controls in the above areas.
- Documented the test results and provided evidence of the findings to the IT team for remediation actions where necessary.

Section 3: Summary & Details of IT audit findings

01. Executive summary and scope of work completed



















02. Scope and summary of work completed

03. Summary & Details of IT audit findings

04. Review of IT audit findings raised in prior year

Section 3: Overview of IT audit findings





This section provides an overview of results from our assessment of the relevant Information Technology (IT) systems and controls operating over them which was performed as part of obtaining an understanding of the information systems relevant to financial reporting. This includes an overall IT General Control (ITGC) rating per IT system and details of the ratings assigned to individual control areas. For further detail of the IT audit scope and findings please see separate 'IT Audit Findings' report.]

IT system	Level of assessment performed	Overall ITGC rating	ITGC control area rating			Related significant risks / other risks
			Security management	Technology acquisition, development and maintenance	Technology infrastructure	
SAP	Detailed Roll forward ITGC assessment (design effectiveness)					N/A
Capita Academy	Detailed Roll forward ITGC assessment (design effectiveness)					N/A
FMS	Detailed Roll forward ITGC assessment (design effectiveness)					N/A
Civica CX	Detailed ITGC assessment (design effectiveness)					N/A
Active Directory	Detailed ITGC assessment (design effectiveness)			Not In Scope	Not in Scope	N/A


We also performed specific procedures in relation to the Cyber security performed during the audit period. We observed the following results:

IT system	Result	Related significant risks / risk / observations
Cyber Security	No Deficiencies Identified	n/a

Assessment

-  Significant deficiencies identified in IT controls relevant to the audit of financial statements
-  Non-significant deficiencies identified in IT controls relevant to the audit of financial statements / significant deficiencies identified but with sufficient mitigation of relevant risk
-  IT controls relevant to the audit of financial statements judged to be effective at the level of testing in scope
-  Not in scope for testing


IT general controls assessment findings

Assessment	Issue and risk	Recommendations
1.	<p data-bbox="203 297 240 339"></p> <p data-bbox="337 297 1073 318">User accounts identified with inappropriate access rights in FMS</p> <p data-bbox="337 332 1100 444">Administrative access to FMS has been granted to users who have financial responsibilities. The combination of financial responsibilities with the ability to administer end-user security is considered a segregation of duties conflict.</p> <p data-bbox="337 458 1100 682">We noted that 13 Finance users with role ‘System Controller Status = 2’ could set up user accounts and then assign additional financial responsibilities to these or other user accounts. Some Finance users provide systems support and require this functionality; other users who perform financial reporting, create a segregation of duties conflict. We did not perform additional procedures to verify if the users had access to and used this functionality The list of users referred has been provided.</p> <p data-bbox="337 736 389 758">Risk</p> <p data-bbox="337 772 1100 885">Depending on the functionality of a system and the nature of the administration access rights, a combination of administration and financial privileges creates a risk that system-enforced internal controls can be bypassed. This could lead to</p> <ul data-bbox="337 899 955 1003" style="list-style-type: none"> - unauthorised changes being made to system parameters - creation of unauthorised accounts, - unauthorised updates to other account privileges 	<p data-bbox="1131 297 1995 432">Access should be based on the principle of least privilege and commensurate with job responsibilities. Management should define segregation of duty policies and processes and ensure that there is an understanding or roles, privileges assigned to those roles and where incompatible duties exist. It may be helpful to create matrices to provide an overview of the privileges assigned to roles.</p> <p data-bbox="1131 446 1995 525">We would recommend that the “System Controller Status = 2” role is removed from the finance users and assigned to the system administrators who manage the application or assigned to users whose activities are logged and monitored.</p> <p data-bbox="1131 539 1995 652">Management should adopt a risk-based approach to reassess the segregation of duty matrices on a periodic basis. This should consider whether the matrices continue to be appropriate or required updating to reflect changes within the business.</p> <p data-bbox="1131 666 1995 891">If incompatible business functions access rights are granted to users due to organisational size constraints or other business needs, management should review their current detective controls on a regular basis to identify and monitor activities. These may include reviewing system reports of detailed transactions; selecting transactions for review of supporting documents; overseeing periodic counts of physical inventory, equipment or other assets and comparing them with accounting records; and reviewing reconciliations of account balances or performing them independently.</p> <p data-bbox="1131 905 1995 961">We are aware that there is a project to implement a dual authorisation which has gone live since the conclusion of our audit.</p> <p data-bbox="1131 1011 1394 1036"><i>Continue to next page..</i></p>




Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


IT general controls assessment findings

	Assessment	Issue and risk	Recommendations
1.		User accounts identified with inappropriate access rights in FMS	<p>Management response</p> <p>Officers have reconsidered Grant Thornton's finding and remain satisfied that the specific system controller functionality within FMS does not give rise to additional risk when combined with financial functionality. In FMS, the system controller access referred to does not permit users to bypass system enforced dual authorization controls. However, transferring the system controller function away from knowledgeable Finance staff would increase the risk of inappropriate access being given to users.</p> <p>Following the previous year's audit report the Council noted that there was a potential weakness in the creation of new users, as new user accounts could be created by one single system controller – a risk which was unrelated to whether the system controller function was performed by Finance or by other staff. However, during 2023 the Council has improved the functionality in FMS so that one individual system controller can no longer create and activate a new user account.</p> <p>The Council periodically risk-assesses all functionality in FMS. This highlights those areas of functionality within the system which represent the highest risk, and it is in the light of this work that the Council is satisfied with its current arrangements. FMS provides a full audit trail of system administrator activity, and detection controls are in place.</p>




Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


IT general controls assessment findings

Assessment	Issue and risk	Recommendations
2. 	<p>Inadequate controls over privileged user accounts in FMS, and Capita Academy databases</p> <p><u>FMS Oracle databases</u></p> <p>We noted that activities performed by system administrators via generic user accounts SYS and SYSTEM were logged. However, the activities were not reviewed on a periodic basis. We were informed that the DBA team of the Council have agreed that individual accounts will be set up for their use when resources allow.</p> <p><u>Capita Academy database</u></p> <p>We noted that activities performed by system administrators via generic user IDs 'aisdba' were logged. However, these activities were not reviewed on a periodic basis. We were informed that management is in the process to implement a new module within Academy that monitors the system users including generic accounts.</p> <p>Risks</p> <p>Without logging and monitoring of administrator activities, in particular generic accounts, it might not be possible to detect unauthorised activities that are performed via these accounts.</p>	<p>Management should consider developing a logging and monitoring strategy for critical administrative activities. Resources should be allocated to monitor only those activities that are critical. These logs should be reviewed by an independent person on a periodic basis or as and when alerted.</p> <p>Management response</p> <p><u>FMS</u></p> <p>As noted, individual accounts will be set up for use by individual staff. However, this will not remove the requirement for generic IDs to run scripted processes, although the use of the generic IDs will be limited to this. The functionality for auditing of 'sys operations' is switched on for the FMS database, ensuring that there is an audit trail of the activities carried out by these IDs.</p> <p><u>Academy</u></p> <p>As noted, the Council is in the process of implementing new modules which will help to address this point.</p>

Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

SAP controls assessment findings

	Assessment	Issue and risk	Recommendations
3.		<p>Users with inappropriate access to directly create and modify SAP roles in production</p> <p>From our review, we identified four (4) Dialog user accounts who have access to directly create and modify roles respectively in the production environment using the PFCG transaction. The List of users referred has been provided.</p> <p>We performed further audit procedures to determine whether the roles are created or changed in production are based on a formal request and approval. We noted that these roles are created or changed in Development and QA and then moved to production via transports, other roles are changed directly in production as and when required by business and there is no formal request and approval process followed by Council.</p> <p>Risks</p> <p>Access to create and modify roles directly into production creates a risk that inappropriate access within the application or underlying data may be granted without following formal user management procedures.</p>	<p>Management should adopt a consistent process for managing roles within production and consider the following :</p> <ul style="list-style-type: none"> • Newly created roles or changes to existing roles should be implemented as transports in all circumstances. Creation of new roles and changes to existing roles should be initially performed in development, tested in quality and imported into production via transport requests. • If there are any exceptions to the process, users with the ability to directly implement new roles or perform role modifications should be assigned with Firefighter access with a set validity period based on formal approvals. • Roles should be created or modified within each development system and transported to the target systems from development. The ability to create or modify roles should be restricted. <p>Management response</p> <p>In practice the procedure in place is not to amend roles directly in the 'live' environment, and the standard process is that changes are implemented through the 'development' environment and QA. The current permissions will be removed and will only be given on request in case of firefighting, with all such requests being logged.</p>

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


SAP controls assessment findings

	Assessment	Issue and risk	Recommendations
4.	●	<p>Inappropriate segregation of duties conflict within SAP as users have ability to configure and delete audit logs in production</p> <p>We performed a comparison of all users with the ability to configure audit logs within production via SM19 with those with the ability to re-organise or delete them in production using SM18. We identified four (4) users with both access rights. The List of users referred has been provided.</p> <p>To perform our further additional procedures, we were informed that the SM21 logs are retained for only previous 12 days and then deleted. Therefore, we were unable to perform further testing.</p> <p>Risks</p> <p>Users with access to SM19 and SM18 have the ability to configure and delete audit logs on SAP. Hence, inappropriate and anomalous activity may not be detected and resolved in a timely manner.</p>	<p>Management should segregate a user's ability to configure (SM19) and delete (SM18) user security event logs within production.</p> <p>If for operational reasons access cannot be fully segregated, alternative options to mitigate the risk could include usage of Firefighter accounts with a set validity period based on formal approvals.</p> <p>Management response</p> <p>This function is carried out by the Council's third-party support contractor. Officers will discuss with the contractor whether this access is needed and whether there are any practical barriers to it being segregated by user as recommended.</p>

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

Section 4: Review of findings raised in prior year

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
<p>X</p> 	<p>User accounts identified with inappropriate access rights in FMS</p> <p>Administrative access to FMS has been granted to users who have financial responsibilities. The combination of financial responsibilities with the ability to administer end-user security is considered a segregation of duties conflict.</p> <p>We noted that 14 finance users could set up user accounts and then assign additional financial responsibilities to these or other user accounts.</p>	<p>The finding has not been remediated.</p> <p>Management response as of 2022</p> <p>The role of setting up new users in FMS is undertaken by staff within the Corporate Financial Integrity team to help ensure that the access permissions given are appropriate. The Council has assessed that the risk involved in setting up new user accounts is inherent to that function and is not significantly affected by other roles which users performing the function may have. The Council has various controls in place to detect unauthorised user accounts. Going forward, system improvements which were already under development will ensure that passwords for user accounts, including newly assigned accounts, can only be generated by genuine users logged in to the Council's systems with a council network ID matching the details of the FMS ID. This will minimise the risk of unauthorised user accounts.</p> <p>GT Comments as of 2023 – We inquired with Lead Engineer, IT Engineer and Principal IT Officer and confirmed that there have been no changes or remediations which have taken place during the audit period in concern. However, We are aware that there is a project currently underway to implement a dual authorisation project which has gone live since the conclusion of our audit.</p> <p>Please refer to Finding 1 above in the section “IT general controls findings”.</p>

Assessment

- ✓ Action completed
- X 2 Not yet addressed

Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
✓	User accounts identified with inappropriate access rights in SAP	The finding has been Remediated.
●	<p>We identified 24 user accounts with inappropriate privileged access. We noted the following:</p> <ul style="list-style-type: none"> • 7 out of 24 business users had access to DEBUG - ABAP Debugger in production. • 7 out of the 24 business users had access to SM30 and SM31 - Call ViewTable Maintenance • 13 out of 24 business users had access to Batch admin: SM36 - Schedule Background Job, SM37 - Monitor Batch Job • 11 out of 24 business users had access to Batch scheduling: SM36 - Schedule Background Job, SM37 - Monitor Batch Job <p>As mentioned above, we identified 7 user accounts with inappropriate DEBUG access via S_DEVELOP authorisation object and assigned access to maintain all SAP standard or customised tables via SM30 or SM31. Although the users were validated by the business as appropriate, they have DEBUG access which is not recommended as it can by-pass most controls in SAP and is very difficult to perform a risk exposure check.</p>	<p>Management response as of 2022</p> <p>We have reviewed the findings and access and have removed all DEBUG access in the LIVE system, with the exception of system users.</p> <p>The users specified do not have direct access to SM30 & SM31 and are unable to update all tables as specified. They do have access to maintain one specific table which has been created to allow for a bespoke programme to be used to Automate the submission of RTI Returns to and from HRMC.</p> <p>We believe that the criteria used to gain the original audit sample data from SAP was incorrect which resulted in incorrect returns for SM36 and SM37. The reports have been re-run with the correct criteria, and this has highlighted an issue for which corrective action has been taken.</p> <p>GT Comments as of 2023</p> <p>We received additional evidence following the issue of the draft report and noted that the inappropriate users' permissions were removed and only users from SAP BASIS and Support team have access in-line with the user's job roles and responsibilities.</p>

Assessment

- ✓ Action completed
- ✗ Not yet addressed

Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
X	<p>Inadequate controls over privileged user accounts in SAP, FMS, and Capita Academy applications and databases</p> <p>Academy application</p> <ul style="list-style-type: none"> We noted that activities performed by system administrators via generic user accounts (academy -Academy Remote Supp and aisdba -Database Admin) were logged. However, these were not reviewed on a periodic basis. Even though the password to access "aisdba -Database Admin" was shared, this was not securely stored in a password vault. <p>FMS and SAP Oracle databases</p> <ul style="list-style-type: none"> We noted that activities performed by system administrators via generic user accounts SYS and SYSTEM were logged. However, these were not reviewed on a periodic basis. <p>Capita Academy Ingres database</p> <ul style="list-style-type: none"> Activities of generic user IDs (academy, aisdba, and ingres) were logged from an application level. However, we noted that the activities performed by these three accounts were not logged from the database level. 	<p>This finding has been partially remediated.</p> <p>Management response as of 2022</p> <p>Academy & Academy Ingres database</p> <p>The Council is in the process of purchasing audit logging which sits inside the system. We believe this will allow us to log what each user is undertaking.</p> <p>SAP Oracle database</p> <p>Access to the SAP Oracle Database and these users is controlled by the DBA team. They will give consideration to the following :</p> <ul style="list-style-type: none"> Creating an account for each named DBA with appropriate role privileges. Creating account(s) for the scripts which may use SYS to logon to the database. Reviewing scripts and processes to identify other uses of SYS and SYSTEM accounts. Changing the SYS password and creating processes to change this after use and/or periodically. Appointing an independent body and reviewing the requirements for reporting on the above. <p>FMS</p> <p>Consideration will be given as to whether a resource exists which is both independent and has sufficient technical knowledge to be able to meaningfully review activity logs.</p> <p>GT Comments as of 2023 – We inquired with Lead Engineer, IT Engineer and Principal IT Officer and confirmed that there have been changes or remediations taken place during the audit period in concern, however some of the remains same for the current year. Please refer to Finding 2 above in the section "IT general controls findings".</p>

Assessment
 ✓ Action completed
 X Not yet addressed

Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
✓	<p>Insufficient evidence of Implementation of Cyber Security Controls</p>	<p>This finding has been remediated.</p>
●	<p>We noted the following deficiencies:</p> <ul style="list-style-type: none"> • Lack of maintaining baseline security configuration standards and configurations for IT components (for example, networking equipment, cybersecurity equipment, servers, and workstations, mobile devices). • No formal documented data classification and retention policy, controls, and monitoring processes were available. • No evidence related to cybersecurity trainings provided to employees which were conducted during the audit period under consideration 	<p>Management response as of 2022</p> <p>Staff resource has now been identified to review the relevant policies. These will be updated with a document control table and relevant review dates applied.</p> <p>Under the Council's Information Management and Governance Strategy, mandatory Information Governance training is undertaken by all staff at least every two years, and the Council is satisfied that this frequency is appropriate. The latest tranche of training is being undertaken during autumn 2022.</p> <p>sits inside the system. We believe this will allow us to log what each user is undertaking.</p> <p>GT Comments as of 2023 – We inquired with Lead Engineer, IT Engineer and Principal IT Officer and confirmed that there have been changes or remediations which have taken place during the audit period in concern. GT obtained and tested additional evidences for Cybersecurity workpapers and found no deficiencies.</p>

Assessment

- ✓ Action completed
- X Not yet addressed



© 2023 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.