



IT Audit Findings

Leeds City Council

Year ended : 31 March 2024

Issued Date : 12 November 2024

Chris Houghton

Senior Manager, IT Audit

T: +44 20 7728 2276

E: chris.houghton@uk.gt.com

Arpita Seth

Technology External Audit Assistant Manager

D +44 20 7728 2331

E: Arpita.Seth@uk.gt.com

Sahil Chaudhary

Audit Associate

T: +44 20 7184 4613

E: Sahil.Chaudhary@uk.gt.com

Priyanka Goyal

Junior OTM IT Audit

E: Priyanka.Goyal@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 2024, Grant Thornton has completed a Design and Implementation review of the IT General Controls (ITGC) for the in-scope applications FMS, Capita(Academy) and SAP identified as relevant to the audit. Grant Thornton also performed the roll forward testing, followed up on prior year's findings and re-tested privileged access controls for the in-scope application, Civica CX, 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:

- SAP
- FMS
- Capita Academy
- 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.
- Completed a detailed technical security and authorisation review of Leeds City Council SAP system as relevant to the financial statements audit, and
- 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 ITGC assessment (design effectiveness)					N/A
FMS	Detailed ITGC assessment (design effectiveness)					N/A
Capita Academy	Detailed ITGC assessment (design effectiveness)					N/A
Civica CX	Detailed roll forward 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


SAP controls assessment findings

Assessment	Issue and risk	Recommendations
1.	 <p data-bbox="312 291 1120 401">The passwords for standard SAP IDs are not secured appropriately Our audit procedures identified that the password for standard SAP IDs are not secured. We inspected the report RSUSR003 and noted that for the production client, the password could be easily found.</p> <p data-bbox="312 454 379 474">Risks Bypass of system-enforced internal control mechanisms through inappropriate use of SAP standard accounts increases the risk of making unauthorized changes to system and client.</p>	<p data-bbox="1135 291 1976 372">We recommend that password for all SAP standard accounts should be changed from the system default settings and are not trivial for all clients on the production instance</p> <p data-bbox="1156 425 1417 445">Management response Password changes will be requested for these standard IDs.</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 database, and Capita Academy application and Database</p> <p><u>FMS Oracle databases</u></p> <p>We noted that activities performed by system administrators via generic user accounts were logged. However, the activities were not reviewed on a periodic basis. The finding was identified in prior year and remains the same for current year.</p> <p>Additionally, we also noted that the password for the account is shared among the system administrators.</p> <p>The list of accounts referred to has been provided.</p> <p><u>Capita Academy application</u></p> <p>For a generic Capita support account within Academy, we noted that account is used by Capita, the third-party vendor for supporting the Capita (Academy) system as needed. We were informed that Capita will log a call with the Council and access the system. However, we were unable to obtain the evidence demonstrating the call request and approval by the Council.</p> <p>Additionally, we also noted that activities performed via generic user IDs were logged. However, these activities were not reviewed on a periodic basis.</p> <p>The details of account referred to has been provided.</p> <p><u>Capita Academy database</u></p> <p>We noted that the account is restricted to database administrators and activities performed by database administrators via generic user IDs 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>Management should undertake a review of all user accounts on the Capita and FMS application and database to identify all generic privileged accounts. For each account identified management should confirm the</p> <ul style="list-style-type: none"> - requirement for the account to be active and be assigned privileged access - which users have access - controls in place to safeguard the account from misuse. <p>Where possible, generic privileged accounts should be removed, and individuals should have their own uniquely identifiable user accounts created to ensure accountability for actions performed. Alternately, management should implement suitable controls to limit access and monitor the usage of these accounts (i.e. through increased use of password vault tools / logging and periodic monitoring of the activities performed). Where monitoring is undertaken this should be formally documented and recorded.</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>Setting up individual accounts for use by individual staff would not remove the requirement for generic IDs to run scripted processes, although the use of the generic IDs could be limited to such processes. 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 the generic IDs, however the audit trail output is highly technical and could not be reviewed and understood by individuals from outside of the specialist team. The service will investigate setting up individual IDs.</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

Continue to next page..

IT general controls assessment findings

Assessment	Issue and risk	Recommendations
2.	 <p>Inadequate controls over privileged user accounts in FMS database, and Capita Academy application and Database</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>The use of generic or shared accounts with high-level privileges increases the risk of unauthorised or inappropriate changes to the application or database. Where unauthorised activities are performed, they will not be traceable to an individual.</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
3.	<p data-bbox="161 305 1038 361">● Lack of formal Batch management approval within FMS application</p> <p data-bbox="298 382 1038 504">For a selected Batch change sample, we noted that there was no formal approval obtained to ensure that the Batch change had been formally approved by an appropriate person from the Finance team before promoting the change into the live environment.</p> <p data-bbox="298 565 1038 806">Risks Without adequate change management controls, unauthorised or undocumented changes to batch scheduling configurations can lead to disruptions in critical business processes, data loss, and security vulnerabilities. Furthermore, the absence of a structured change management process increases the likelihood of configuration errors and inconsistencies.</p>	<p data-bbox="1052 305 1962 386">We would recommend that the Council establish a formalised change management process for batch scheduling configurations, including documentation of proposed changes, impact assessment, approval workflows, and implementation controls.</p> <p data-bbox="1052 401 1962 482">The Council should implement a segregation of duties control to ensure that only authorised personnel can make and approve changes to batch scheduling parameters.</p> <p data-bbox="1052 575 1962 714">Management response The batch change sampled in the audit had been discussed and approved by the Finance team during a meeting, but this had not been formally recorded. New batch scheduling approvals for FMS now follow the same change management process as the authorisation of all other FMS changes.</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	
4.	●	<p data-bbox="300 285 1129 321">Insufficient Evidence of Implementation of Cyber Security Controls</p> <p data-bbox="300 335 1129 421">Our audit procedures identified that there is no formal Cyber Security framework established presently. We were informed that Council is working to establish the ISMS framework as best practice.</p> <p data-bbox="300 449 1129 535">We noted that the Cyber Security policies were last updated in 2020 and 2021, we were informed that Council is working to update the policies by end of 2024.</p> <p data-bbox="300 549 1129 656">Given the increasing risk from cyber-attacks over recent months, the council should ensure they are current with cyber security monitoring and prevention practices. This should include penetration testing and central government IT certification.</p>	<p data-bbox="1149 285 1993 321">Management response</p> <p data-bbox="1149 321 1993 399">As noted, the Council is working towards establishing a formal framework. However, it should be noted that extensive arrangements are already in place :</p> <ul data-bbox="1149 399 1993 913" style="list-style-type: none"> <li data-bbox="1149 399 1993 599">• In June 2024 LCC signed up to the Cyber Assessment Framework (CAF) for Local Government based on the NCSC's Cyber Assessment Framework. We are working towards implementing the CAF's 4 objectives and 14 principles around managing security risk, protection against cyber-attacks, detecting cyber security events, and minimising the impact of cyber security incidents. This work is being headed up by the recently appointed Head of Security & Technical Architecture. <li data-bbox="1149 599 1993 656">• A comprehensive review and replacement of cyber security related policies is underway. <li data-bbox="1149 656 1993 714">• There are many technical controls in place to monitor for and prevent cyber security incidents and a dedicated IT Security Team of SMEs. <li data-bbox="1149 714 1993 771">• The council utilises a vulnerability management tool to scan for vulnerabilities across our IT estate several times a week. <li data-bbox="1149 771 1993 913">• An annual penetration takes place for the annual IT Health Check required to obtain compliance to connect to the government's Public Services Network. The current compliance certificate expires in January 2025. Other penetration tests take place throughout the year on an ad hoc basis to test specific applications or systems

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

Controls For Which Assurance Could Not Be Provided

Change Management [FMS]	<p>For in-house developed applications, code change requests are raised through a formal change management process, reviewed, and approved before any development work starts.</p> <p>In-house developed code changes are subject to all or a combination of unit, system integration, regression, and user acceptance testing, before being signed off by business users confirming that requirements of the change request have been met.</p> <p>Changes which have been tested and signed off by business users are evaluated and approved by personnel independent of the development and testing process, as to when they can be deployed into production.</p>	<p>Insufficient evidence was provided for the Grant Thornton IT Audit Team to assess the controls over the changes within the FMS applications.</p> <p>Due to system limitation, we were unable to obtain the change logs from FMS systems to verify last change date made within audit period. Therefore, we were unable to test the control.</p>
Change Management [FMS]	<p>Developers do not have continuous access to the production environment and cannot implement their own changes into the production environment.</p>	<p>Insufficient evidence was provided for the Grant Thornton IT Audit Team to assess the controls over the list of developers and Implementers within the FMS applications.</p> <p>Due to system limitation, we were unable to obtain the system generated list of developers and Implementers from FMS systems to verify the segregation of duties maintained within audit period. Therefore, we were unable to test the control.</p>
Change Management [Capita]	<p>Developers do not have continuous access to the production environment and cannot implement their own changes into the production environment.</p>	<p>Insufficient evidence was provided for the Grant Thornton IT Audit Team to assess the controls over the list of developers and Implementers within the Capita application.</p> <p>Due to unavailability of SOC report, we were unable to test the control.</p>
Batch Monitoring [FMS]	<p>Operations personnel manually monitor the status of batch jobs to identify exceptions or events that need their intervention, allowing them to address the issues in a timely manner.</p>	<p>Insufficient evidence was provided for the Grant Thornton IT Audit Team to assess the controls over monitoring scheduled job failures within the FMS application.</p> <p>Due to system limitation, we were unable to obtain the system generated list of developers and Implementers from FMS systems to verify the segregation of duties maintained within audit period. Therefore, we were unable to test the control.</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

Controls For Which Assurance Could Not Be Provided

Batch Monitoring
[FMS]



Operations personnel manually monitor the status of batch jobs to identify exceptions or events that need their intervention, allowing them to address the issues in a timely manner.

Insufficient evidence was provided for the Grant Thornton IT Audit Team to assess the controls over monitoring scheduled job failures within the FMS application.
Due to system limitation, we were unable to obtain the Batch error sample within audit period to test the control.

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>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 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>The finding has been remediated.</p> <p>Management response as of 2023</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> <p>GT Comments as of 2024 – Per enquiry, we confirmed that the 13 users with role 'System Controller Status = 2' does not perform any administrative tasks. All the administrative tasks such as creating new users, deleting the users etc are carried out by privileged users with role 'System Controller Status = 1'. Therefore, the finding has been remediated from prior year.</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
X	<p>Inadequate controls over privileged user accounts in FMS, and Capita Academy databases</p>	<p>The finding has been Remediated.</p>
●	<p><u>FMS Oracle databases</u></p> <p>We noted that activities performed by the system administrators via generic user accounts were logged. However, the activities were not reviewed on a periodic basis. We were informed that the DBA team within the Council have agreed that individual user accounts will be set up when resources allow.</p> <p><u>Capita Academy database</u></p> <p>We noted that activities performed by system administrators via generic user IDs 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 will monitor all the system users including generic accounts.</p>	<p>Management response as of 2022</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> <p>GT Comments as of 2024</p> <p><u>FMS Oracle databases</u></p> <p>We confirmed that there have been no changes or remediations which have taken place during the audit period in concern. Please refer to Finding 3 above in the section "IT general controls findings".</p> <p><u>Capita Academy database</u></p> <p>We confirmed that there have been improvement in the overall control as we can see that the access is restricted to administrators, however we noted that there is no monitoring performed by council for the generic account. Therefore, we rated the finding as a Control Improvement for the current year. Please refer to Finding 4 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>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> <ul style="list-style-type: none"> . 	<p>This finding has been remediated.</p> <p>Management response as of 2023 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> <p>GT Comments as of 2024 – The finding has been remediated for current year.</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>Inappropriate segregation of duties conflict within SAP as users have ability to configure and delete audit logs in production</p>	<p>This finding has been remediated.</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>Management response as of 2023</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> <p>GT Comments as of 2024 – The finding has been remediated for current year.</p>

Assessment

- ✓ Action completed
- X Not yet addressed



© 2024 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.