IT Audit Findings

Leeds City Council

Year ended : 31 March 2022

Issued : 25 October 2022 & 01 December 2022

Chris Houghton
IT Audit Senior Manager
T: +44 20 77282276
E: chris.houghton@uk.gt.com

Maha Sivakumar
IT Audit Manager
T: +44 20 7184 4338
E: maha.sivakumar@uk.gt.com

Veeren Sujan
IT Audit Associate
T: +44 20 7383 5100
E: veeren.h.sujan@uk.gt.com

Section 1: Executive summary and scope of work completed

01. Executive summary and scope of work completed

02. Summary of IT audit findings

03. Detail 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 2022, 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.

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: Summary of IT audit findings

01. Executive summary and scope of work completed

02. Summary of IT audit findings

03. Detail of IT audit findings

04. Review of IT audit findings raised in prior year

The following IT general control weaknesses were identified:

- User accounts identified with inappropriate access rights in FMS
- User accounts identified with inappropriate access rights in SAP
- Inadequate controls over privileged user accounts in SAP, FMS, and Capita Academy applications and databases
- Insufficient evidence of Implementation of Cyber Security Controls

Assessment		Number
Significant Deficiency	🔴	2
Deficiency	🟡	1
Improvement Opportunity	🟢	1

Section 3: Details of IT audit findings

01. Executive summary and scope of work completed

02. Summary of IT audit findings

03. **Detail of IT audit findings**

04. Review of IT audit findings raised in prior year

IT general controls findings

	Assessment	Issue and risk	Recommendations
1.	●	**User accounts identified with inappropriate access rights in FMS** 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. We noted that 14 finance users could set up user accounts and then assign additional financial responsibilities to these or other user accounts. **Risk** A combination of administration and financial privileges creates a risk that system-enforced internal controls can be bypassed. This could lead to - unauthorised changes being made to system parameters - creation of unauthorised accounts, - unauthorised updates to other account privileges	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. 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. 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. **Management response** 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 unauthorized user accounts.

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 findings

	Assessment	Issue and risk	Risk
2.	🔴	**User accounts identified with inappropriate access rights in SAP** We identified 24 user accounts with inappropriate privileged access. We noted the following: • 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 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. We performed further procedures to determine whether there had been changes to tables during the audit period and we noted that there were no significant table changes made during the period. The list of the users referred to has been provided.	Access to maintain all standard or customised SAP tables creates a risk that unauthorised table maintenance functions can be performed and result in data integrity issues. DEBUG access presents several risks when combined with other t-codes for example: -Change or Delete entries in tables through changing variable values from SHOW to EDIT including tables that are typically protected by SCC4 or do not have a view; Including change log table CDHDR. -Change or delete data through inserting break-point statements into program code and bypassing authority checks -Execute transactions user is not authorized to execute through inserting break-point statements into program code and bypassing authority checks. **Recommendations** 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. If incompatible business functions are granted to users due to organisational size constraints, management should ensure that there are review procedures in place to monitor activities. Debug access should not be permanently granted in the production environment. We recommend that the user accounts should be reviewed and debugging access removed.

Cont.

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 findings

	Assessment	Issue and risk	Risk
2.		*Cont.*	**Management response** We have reviewed the findings and access and have removed all DEBUG access in the LIVE system, with the exception of system users. 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. 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. **Grant Thornton update as of December 2022** 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.

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. 🟠

Inadequate controls over privileged user accounts in SAP, FMS, and Capita Academy applications and databases

Academy application

- 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.

FMS and SAP Oracle databases

- 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.

Capita Academy Ingres database

- 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.

Risks

- 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.
- Shared usage of privileged generic accounts reduces accountability for actions performed through these accounts. Unauthorised activities performed through shared privileged accounts may not be traceable to an individual.

Recommendations

- 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.
- Management should also control the usage of shared generic accounts by implementing a password vaulting solution that has the capability to change the password after use or logging and monitoring of the activities performed via these generic accounts.

Management response

Academy & Academy Ingres database

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.

SAP Oracle database

Access to the SAP Oracle Database and these users is controlled by the DBA team. They will give consideration to the following :

- 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.

FMS

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.

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
4.	🟢	**Insufficient evidence of Implementation of Cyber Security Controls**	

Issue and risk

Insufficient evidence of Implementation of Cyber Security Controls

We noted the following deficiencies:

- 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.

Risks

Not being able to evidence the existence and operation of cyber-security controls makes it difficult for the business to confirm that they are adequately protected against the threat of a potential cyber incident. In particular:

- Cybersecurity risk is the probability of exposure, loss of critical assets and sensitive information, or reputational harm because of a cyber-attach or breach within an organisation's network.
- Lack of policies or outdated policies can leave organisations at risk by failing to comply with new laws and regulations. They may not address new systems or technology which can result in inconsistent practices across the organisation.
- Lack of cybersecurity training prevents staff from being aware of cyber threats / risks which is key to being able to identify and respond to threats appropriately during day-to-day activities to minimise impact.

Recommendations

In the absence of appropriate evidence, it has been assumed that cyber-security controls are not in place; therefore, it is recommended that Management (wherever applicable):

- Implement and review all key policy and process documents on an annual basis. Reviews should be undertaken by a member of staff with appropriate knowledge and approved by management. The review/update should be formally documented within each document in a change and revisions reference table.
- Cybersecurity training should be given to make staff aware of the threats and risks they are exposed to when using technology and teach them the appropriate way to use IT to minimise risk exposure and work in line with the relevant processes and rules. Training should cover common attacks and threats and the appropriate response.

Management response

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.

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.

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 previously communicated	Update on actions taken to address the issue
X ●	**1. User accounts identified with inappropriate access rights in SAP** We identified 18 user accounts with inappropriate DEBUG access via S_DEVELOP authorisation object. Although the users were validated by the business as appropriate, they have DEBUG access which is not recommended as it can bypass most controls in SAP and is very difficult to perform a risk exposure check. Additionally, we also noted that there were 4 custom roles (ZLCC_HR_PROJECT_ ZLCC_HR_PROJECT_TEAM_BACKUP, ZSAP_ESS_AUTHORISATIONS and ZSAP_ESS_AUTHORISATIONS_ORIG) that were assigned with DEBUG access in production.	This finding has **not been remediated.** **Management comments as of 2021 –** The Council is reviewing this finding and will take appropriate remedial action once the technical implications have been fully assessed. **Update as of 2022 –** The Council has scheduled to review the roles for the end of mid year patching. **GT Comments as of 2022 –** We inquired with Lead Engineer on 17/08/2022 and confirmed that there have been no changes or remediations which have taken place during the audit period in concern. **Management comments as of 2022** Action on the previous year's findings was not taken during 2021/22 due to those findings being received towards the end of 2021/22. Debug access has now been removed from all users in LIVE. A review of Custom roles is to be undertaken to ensure that DEBUG access has been removed if relevant (whilst these appear to be custom roles they may be copies of Standard SAP roles, this will form part of the review)
✓ ●	**2. Segregation of duty conflicts within SAP** We noted that DEVACCESS table was active in production with 1 user-id [BOWLIM] assigned with developer access key in production. The user could potentially change the source code in production. Additionally, we also noted that , the user has developer keys in production with access to ABAP Editor/ABAP Function Modules/ABAP Workbench(SE38/SE37/SE80) allowing these users to make changes to source code in production. We also identified 4 user accounts with conflicting access combinations that can be used to make changes to customised objects in development environment and transport the changes from QA to production environment.	This finding has **been remediated.** **Management comments as of 2021 –** The Council is reviewing this finding and will take appropriate remedial action once the technical implications have been fully assessed. **Update as of 2022 –** There is a process in place where a monthly report is being run to check DEVACESS Table in SE16 and this is compared to User Details in RSUSR200. **GT Comments as of 2022 –** We inspected the DEVACCESS check table report for the month of July 2022 and noted the respective valid through and last logon dates to SAP. To corroborate the valid through and last logon dates provided, we cross checked these details with the USR02 report generated for the audit period under consideration and confirmed that the users have not logged into the system during the audit period and the valid through dates were set prior to the financial audit period.

Assessment

✓ Action completed
X Not yet addressed

Section 4: Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
X ●	**3. Inadequate control over generic accounts within FMS database and Capita (Academy) application** While the system was configured to record failed logins, the following generic accounts were not monitored for suspicious activity: • Two generic FMS database administrator user accounts “SYS” and “SYSTEM” are used by Oracle database administrators for performing day to day database administration activities. • One of the generic Capita(Academy) administrator user account – “Database Admin” which is used by David Hughes, Principal DBA Officer for managing users within the application and database. Additionally, no password reset controls were configured on these user accounts to enforce the periodic change of passwords.	This finding has **not been remediated.** **Management comments as of 2021 –** FMS – These generic user IDs and passwords are encrypted into scripts for some automatic processes, and there would be risk involved in rewriting these scripts for periodic password changes. The passwords are held in a Database vault. Academy - This is an admin account for the Database administrator. Although the account has a generic name, only the Principal DBA Officer has access, therefore the account is personal to him. This account is not for managing users, this account is only to access and maintain the backend build of the system and tables. **Update as of 2022 –** FMS **–** Activities performed using the generic user ID "Database Admin" is still not monitored. Further, we also understood that there is no password reset controls configured on these user accounts to enforce the periodic change of passwords. Additionally, in relation to Academy, we noted that the 'AISDBA' login does get reset periodically and is a manual process that happens quarterly. Academy – activities performed by the administrator user account “Database Admin” are not monitored. **GT Comments as of 2022 –** We inquired with Lead Engineer, IT Engineer and Senior Financial Manager on 03/08/2022 and confirmed that there have been no changes or remediations which have taken place during the audit period in concern. **Management comments as of 2022** FMS – Please see 2021/22 item 3 for comments regarding monitoring. These IDs are encrypted into scripts for some automatic processes, and thus periodic password changes would involve risk. Academy - We are 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.

Assessment

✓ Action completed

X Not yet addressed

Section 4: Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
X ●	**4. Lack of review of information security/audit logs in FMS and Capita (Academy)** Information security event logs, which capture the monitoring of activities such as failed logins and use of privileged user accounts within Capita(Academy) and FMS are not reviewed.	This finding has **not been remediated.** **Management comments as of 2021 –** FMS – The possibility of reporting on failed logins will be considered. Academy – The system does not have the technical capability to provide a log showing when a user's access was created/amended or revoked. **Update as of 2022 –** FMS – there is a formal process in place to review activities/tasks performed by administrators in the FMS application. Capita – There is a manual process to record when an account is created and revoked. **GT Comments as of 2022 –** We inquired with Lead Engineer, IT Engineer and Principal IT Officer on 09/08/2022 and confirmed that there have been no changes or remediations which have taken place during the audit period in concern. **Management comments as of 2022** Academy - We are 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. After 3 failed attempts the accounts are locked and can only be unlocked by system admin.

Assessment

✓	Action completed
X	Not yet addressed

Section 4: Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
✓ ●	**5. Weak password configuration settings for FMS and Capita (Academy).** The password policy document does not stipulate password complexity and age to be configured on Leeds City Council's IT applications In addition, the following password parameters were not in line with the Council's password policy. **FMS** Passwords History --'Not Configured' in FMS and 20 passwords' as per policy Capita(Academy) -Minimum length- 8 characters' as per Capita(Academy) and 12 characters' as per policy -Password History -10 as per Capita(Academy) and 20 as per policy -Invalid logon attempts- 3 as per Capita(Academy) and 10 as per policy.	This finding has **been remediated.** **Management comments as of 2021 –** Password policy – Section 13 of the Council's password protocol sets out minimum complexity requirements for subsidiary systems where use of SSO (Single Sign On) isn't possible. FMS – The password history in FMS is configured to look at the last 20 passwords. Academy – Academy uses SSO (Single Sign On). Where this is not technically possible for a specific user, the strong password configuration is enforced in line with section 13 of the corporate Password Protocol. **Update as of 2022 –** Remediated. Capita Academy is authenticated via the Active directory (SSO). Hence, the password settings configured in the Active Directory are applicable. **GT Comments as of 2022 –** We inquired with Lead Engineer and IT Engineer 03/08/2022 and confirmed that the following finding has now been remediated during the audit period in concern. We obtained supporting evidence to verify the password configurations.
X ●	**6. Lack of formal User Management and Batch Monitoring policies and procedures** While security management and batch monitoring procedures are in place, formal user access management and batch monitoring policies are not established to ensure a consistent process is followed across different applications, database and operating systems.	This finding has **not been remediated.** **Management comments as of 2021 –** None. **Update as of 2022 –** Formal user access management and batch monitoring policies are not established to ensure a consistent process is followed across different applications, database and operating systems at Leeds City Council. **GT Comments as of 2022 –** We inquired with Senior Financial Manager on 03/08/2022 and confirmed that there have been no changes or remediations which have taken place during the audit period in concern. **Management comments as of 2022** Officers in IDS will look into the potential benefits of establishing corporate policies in these areas.

Assessment

✓ Action completed

X Not yet addressed

Controls for which assurance could not be provided

Control Area	Control Name and Description	Reason / Justification
Security Management	• Administrative privileges or super-user rights granted to system administrator are restricted to those that require access and are authorized	**Capita Academy application** • We were unable to ascertain the list of users who were granted access to the passwords of the generic user ID “academy -Academy Remote Supp” in the Capita Academy application which was stored in a password vault: **Capita Academy Ingres database** • Evidence to show that the password to access the generic user ID “Academy” was securely stored in a password vault not shared. **Management comments** Capita has been unable to provided this information due to its system capabilities.

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