IT Audit Findings

Coventry City Council

Year ended : 31 March 2024

Issued Date : 11 September 2024

Nerys Bint
IT Audit Partner
T: +44 (0)20 7728 2868
E: nerys.bint@uk.gt.com

Arpita Seth
Technology External Audit Assistant Manager
T: +442073835100
E: Arpita.seth@uk.gt.com

Shrabanti Halder
Junior OTM
E: shrabanti.halder@uk.gt.com

Contents

Section 1: Executive summary

To support the financial statement audit of Coventry City Council for year ended 31 March 2024, Grant Thornton has completed a design and implementation review of the IT General Controls (ITGC) for applications 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 Coventry City Council for their assistance in completing this IT Audit.

Section 2: Scope and summary of work completed

The objective of this IT audit was to complete a design and implementation controls review over Coventry's IT environment to support the financial statement audit. The following applications were in scope for this audit:

- ResourceLink
- CareDirector
- Business World Unit 4
- Capita
- ContrOCC

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

- Evaluated the design and implementation for security management, change management and job scheduling controls where relevant.
- 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.
- Performed a cyber security assessment and inspected supporting documentation.

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	
ResourceLink	Design and Implementation					N/A
CareDirector	Design and Implementation					N/A
Capita	Design and Implementation					N/A
Business World Unit 4	Design and Implementation					N/A
ContrOCC	Design and Implementation					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

Continue to next page..

Section 4: Details of IT audit findings

IT general controls assessment findings

	Assessment	Issue and risk	Recommendations
1.	●	**Absence of formal upgrade management process and data validation procedures** Through our audit procedures, we identified that an upgrade performed in Oct 2021 led to technical issues with file formats and duplication of files in CareDirector. We noted that no manual reconciliations were performed between CM2000 and CareDirector for the period October 2021 to January 2022. Instead, the Council made payments based upon their average invoice amount prior to the change. We understand that the completion of payment reconciliations was targeted to be finished by the end of 2024. At present, seven out of nine reconciliations have been completed with a further two remaining for Caremark and Consummate. **Risks** Failure to adequately perform change management processes prior to releasing the change into the production environment could lead to a loss of data integrity, processing integrity and/or system down-time.	For future upgrades, the Council should - implement a formal upgrade management / system implementation procedures encompassing planning, testing, and implementation phases. - ensure rigorous testing is completed to identify and address potential issues, followed by validation procedures to verify the integrity of data. **Management response** The upgrade was completed during the 2021-2022 audit period, and all issues were resolved before the 2023-2024 audit period. Care Director upgrades follow a structured process involving planning, testing, and implementation, subject to approval by our Adult Social Care Management Team (ASCMT). Rigorous testing is conducted to identify and address potential issues, followed by validation procedures to verify data integrity. CM2000 has been decommissioned, and providers are now paid based on actual hours every eight weeks, with reconciliations requested every four weeks to facilitate easy payment reconciliation. We maintain a spreadsheet to evidence reconciliations between CM2000 and CareDirector. Payment reconciliations have been completed and signed off by Internal Audit, except for one which is still in progress. The decision to write off the Consummate reconciliation was made following recommendations from Internal Audit and financial operations.

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.	●	**Insufficient control over nested accounts within ContrOCC, CareDirector and Business World database** During our review, we identified that there were a number of nested accounts identified within ContrOCC, CareDirector and Business World database. These accounts provide continuous privileged access for third-party consultants to the system. While these consultants provide system support services to the Council, we regard the total number of users to be excessive: • CareDirector – 28 • Business World – 27 • ContrOCC – 26 The details of the users are provided in Appendix 1. **Risks** 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.	The Council should undertake a review of all user accounts on ContrOCC, CareDirector and Business World database to confirm - requirements for the account to be active and assigned privileged access - which users have access - controls in place to safeguard the account from misuse. While these accounts may be necessary for ongoing support services, the Council should re-evaluate whether all third-party accounts need to be active. It is recommended that the Council undertakes a review of these accounts to confirm the ongoing need. **Management response** The engagement of a third-party database administration team is crucial for the effective management of our multiple databases. The third-party team, with its extensive expertise and large workforce, ensures rapid response to any issues and provides the council with the necessary resilience and access to specialised knowledge. We acknowledge the concern regarding the number of third-party users with access to our financial databases. To address this, we have already implemented a quarterly review process to ensure that access is granted only to those individuals actively working with our portfolio of databases. This measure is designed to minimise the risk of unauthorised and inappropriate changes to the database. We are committed to strengthening our control mechanisms and will continue to work closely with the third-party provider to ensure that access is appropriately managed and monitored. **Advanced/CareWorks** Maintaining this number of named accounts is essential for delivering responsive system support. These accounts are not permanently open; access is granted for specific time periods upon request by our Digital Services Team. If Advanced operatives require access to our database, they will request this quoting a support ticket we have raised for a specific issue. We then raise a ticket with internal ICT to activate their account for a set period, which never includes weekends. We provided evidence of this process to GT in July 2024.

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.	●	**Lack of formal change management procedures for changes to job schedules within Capita** During our review, we identified that there is no formal process followed to make changes to batch job configurations. All the changes are discussed verbally via team meetings as and when required. We understand that the Council does not document, review, or approve changes made to batch scheduling parameters and job schedules. **Risks** Without adequate change management controls, unauthorized 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.	The Council should establish a formalized change management process for batch scheduling configurations, including documentation of proposed changes, impact assessment, approval workflows and implementation controls. **Management response** The council will explore the implementation of a more structured process for significant modifications to batch jobs. However, accommodating minor changes such as date parameters daily may not be feasible within this formal framework.

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.	●	**Lack of security events monitoring for Capita, ResourceLink, ContrOCC, Business World and Active Directory (AD)** During our review, we understand that security event logs for AD are sent to Azure Sentinel and monitored by the SOC cyber team 24*7. Post discussion with Council and review of evidence, GT IT Audit noted that the Council reviews and monitors security logs daily for anomalies such as external login attempts etc. However, GT IT Audit noted that there is no monitoring performed on the activities performed by privileged users within Capita, ResourceLink, ContrOCC, Business World and AD. **Risks** Without enabling security event logging and then proactively monitoring them increases the risk that anomalous security activity such as failed login attempts, may not be identified and / or addressed in a timely manner. Additionally, unauthorised system configuration and data changes made using privileged accounts will not be detected by management.	It is recommended that the Council proactively reviews the security event logs for privileged users to detect any suspicious activities such as - repeated invalid/ unauthorised login attempts to access systems, data or applications - privileged user activities - privileged generic accounts - changes to system configurations, tables and standing data These reviews should be performed by one or more knowledgeable individuals, who are independent of the day-to-day use or administration of these systems and formally evidenced. Any issues identified within these logs should be investigated and mitigating controls implemented to reduce the risk of reoccurrence. **Management response** The presence of privileged users on key financial systems is essential for the maintenance, continuous improvement, and timely troubleshooting of any issues that may arise. These users play a critical role in ensuring the systems operate efficiently and effectively. However, we acknowledge that there is room for improvement in the monitoring and reviewing of activities performed by these privileged users. To address this, the council will undertake a comprehensive review of the logging and reporting capabilities available within these systems. This review will aim to enhance our ability to detect and mitigate the risks associated with unauthorised activities. We are committed to implementing robust monitoring mechanisms to ensure the security and integrity of our financial systems. The council will develop and enforce policies and procedures to regularly review and monitor privileged user activities, thereby strengthening our overall IT governance framework.

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

Review of other findings raised in prior year

Assessment	Issue and risk previously communicated [FY2023]	Update on actions taken to address the issue [FY2024]
✓	**Inadequate control over generic user accounts within Capita Ingres database** Through our audit procedures, we identified that the following generic accounts within the Capita database - aisdba - revtrain - autouser are used by members from the 'Revenue and Benefits' team. This is considered to be a segregation of duties conflict, as the team have both financial responsibilities along with the ability to perform administrative tasks in database.	This finding has been remediated. We inspected and verified that no finance members has privileged access to the application. Privileged access is only restricted to systems support team which is necessary for them to carry out their job role. The systems support team administer the Academy system, so need administration rights to maintain the system and resolve issues. Further, we noted that the systems team do not enter/amend any direct debit amounts or bank details and are only responsible to run the system jobs to create the direct debit files that go to the banks. Therefore, the finding has been remediated from the prior year. Further, we verified that REVTRAIN is a default logon that has never been used and AISDBA & autouser passwords have to be changed every 90 days and the passwords are only known to the systems team. Access to these privileged generic accounts is now appropriately restricted to authorized personnel from systems team to carry out financially critical business functions.
X	**Inadequate control over generic user accounts within CareDirector Database** During our review, we identified that there were a number of nested accounts within the 6 generic database accounts, providing access to 38 third party consultants. These consultants provide database support services to the Council.	This finding has not been remediated. We inspected and verified that there were a number of nested accounts within 6 generic database account, providing access to 46 third party consultants. These consultants provide database support services to the Council. Please refer to finding 2 above.

Assessment
✓ Action completed
X Not yet addressed

Review of other findings raised in prior year

Assessment	Issue and risk previously communicated [FY2023]	Update on actions taken to address the issue [FY2024]
✓	**Segregation of duties conflicts within Business World and Capita (Academy)** **Business World Unit 4:** In FY22, we noted that three finance users with administrative access still have their access enabled. Further, we also noted that seven finance team members who had access to amend the batch schedule in Business World still retained access. We understood that one account (User Carolyn Prince, Lead Accountant) was disabled since the user had left the council. In FY23, we identified that one Finance team member has access to amend the batch schedule in Business World Unit 4. The combination of financial responsibilities along with the ability to perform administrative task is considered as segregation of duties conflict. **Capita (Academy):** We identified an increase in the number of Finance members (FY23:7 members, FY22: 5 members) from the Revenue and Benefits team with administrative access to Capita. The combination of financial responsibilities along with the ability to perform administrative task is considered to be a segregation of duties conflict. Please refer to Appendix 2. We also noted that four member of the finance team still had access to amend the batch schedule in Capita (Academy).	This finding has been remediated. For Business World Unit 4, we noted that no user from finance has access to amend the batch job. For Capita, we inspected and verified that no finance member has privileged access to the application. Privileged access is only restricted to systems support team which is necessary for them to carry out their job role. The systems support team administer the Academy system, so need administration rights to maintain the system and resolve issues. Further, we noted that the systems team do not enter/amend any direct debit amounts or bank details and are only responsible to run the system jobs to create the direct debit files that go to the banks.

Assessment
✓ Action completed
X Not yet addressed

Review of other findings raised in prior year

Assessment	Issue and risk previously communicated [FY2023]	Update on actions taken to address the issue [FY2024]
X	**Lack of formal management approval for the upgrade to CareDirector** **CareDirector** Through our audit procedures, we identified that an upgrade performed in Oct 2021 led to technical issues with file formats and duplication of files in CareDirector. We noted that no manual reconciliations were performed between CM2000 and CareDirector for the period October 2021 to January 2022. Instead, the Council made payments based upon their average invoice amount prior to the change. We understand that payments will be reconciled in 2023. While the Council were aware of the implementation issues, it was unclear how these were considered in the decision to go live with the upgraded version. We were unable to obtain any formal sign off by management when the upgrade was promoted into the live environment. We understand that communication was only orally agreed with the Head of Service.	This finding has not been remediated. We were informed that seven out of nine reconciliations have been completed. The remaining two reconciliations for Caremark and Consummate are still in progress. Therefore, the finding remains same from prior year. Please refer to finding 1 above.
X	**Lack of security events monitoring for CareDirector, ResourceLink, Capita and AD** Information security event logs, which record the activities performed by privileged user accounts within CareDirector, ResourceLink, Capita and AD are captured but are not proactively monitored for any suspicious events.	This finding has been partially remediated. For CareDirector, we verified that activity logs for privileged users are now reviewed on an annual basis. For ResourceLink, Capita and AD, we determined that the finding remains from the prior year. Please refer to finding 4 above.

Assessment
✓ Action completed
X Not yet addressed