IT Audit Findings
Shropshire Council

Year ended 31 March 2024

Issued 15 July 2024

Chris Houghton
IT Audit Senior Manager
T: +44 (0)20 7728 2276
E: Chris.Houghton@uk.gt.com

Azwan Bin Jamaluddin
IT Audit Assistant Manager, Audit
T: +44 (0)20 7865 2266
E: Azwan.Bin.Jamaluddin@uk.gt.com

Harveen Purewal
IT Audit Associate, Audit Support Centre
T: +44 (0)20 7865 2324
E: Harveen.Purewal@uk.gt.com

Contents

Section 1: Executive Summary

01. Executive Summary

02. Scope and Summary of Work Completed

03. Summary of IT Audit Findings

04. Detail of IT Audit Findings

To support the financial statement audit of Shropshire Council and Pension Fund for year ended 31 March 2024, Grant Thornton has completed a design and implementation review of 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 Shropshire Council and Pension Fund 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 of IT Audit Findings

04. Detail of IT Audit Findings

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

- Altair
- Unit 4
- Active Directory

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

- Evaluated the design and implementation for security management, change management controls and scheduled job monitoring controls
- Performed an assessment of the processes and controls used as part of transitioning Shropshire Council and Pension Fund's Altair system during the audit period.
- Performed an assessment of the cyber security environment during the audit period.
- 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 of IT audit findings

01. Executive Summary

02. Scope and Summary of Work Completed

03. Summary of IT Audit Findings

04. Detail of IT Audit Findings

Summary 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.

			ITGC control area rating			
IT system	**Level of assessment performed**	**Overall ITGC rating**	Security management	Technology acquisition, development and maintenance	Technology infrastructure	**Related significant risks / other risks**
Altair	Detailed ITGC assessment (design effectiveness only)	🟡	🟢	🟡	🟡	N/A
Unit 4	Detailed ITGC assessment (design effectiveness only)	🟢	🟢	🟢	🟢	N/A
Active Directory	Detailed ITGC assessment (design effectiveness only)	🟡	🟡	⚫	⚫	N/A

We also performed specific procedures in relation to the significant changes during the audit period, specifically the new system implementation. We observed the following results:

IT system	Event	Result	Related significant risks / other risks
Altair	**New system 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

Section 4: Detail of IT Audit Findings

01. Executive Summary

02. Scope and Summary of Work Completed

03. Summary of IT Audit Findings

04. Detail of IT Audit Findings

IT General Controls Assessment Findings

	Assessment	Issue and risk	Recommendations
1.	●	**Information on the privileged accounts within the Active Directory were not provided** We were not provided with the accounts under the Active Directory group “AD Admins “. Hence, we could not provide assurance on privilege access and its appropriateness **Risk** Users with administrative privileges at application level have the ability to bypass system-enforced internal control mechanisms and may compromise the integrity of financial data.	The Council should undertake a review of all user accounts on the Active Directory to identify all privileged accounts. For each account identified the Council should confirm the • 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. Where possible, privileged accounts should be removed, and individuals should have their own uniquely identifiable user accounts created to ensure accountability for actions performed. Alternately, the Council 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. **Management response** The AD admins screen shot evidence requested was unfortunately not supplied for this audit due to security team workload pressure. We do regularly review Privileged access accounts including Active directory/ Entra, O365 and infrastructure accounts that are applicable to the service offered to the Pensions team. We have previously responded to evidence this area in the council’s GT Financial Management audit and can provide evidence but on this occasion, we have failed to do so.

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.	🟢	**Lack of Change Management Controls for Batch Scheduling in Altair** The IT audit uncovered a deficiency in change management controls related to batch scheduling configurations. Specifically, there is a lack of formalised procedures for documenting, reviewing, and approving changes made to batch scheduling parameters and job schedules. **Risk** 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.	Establish a formalised change management process for batch scheduling configurations, including documentation of proposed changes, impact assessment, approval workflows, and implementation controls. Implement segregation of duties to ensure that only authorised personnel can make and approve changes to batch scheduling parameters. **Management response** It has been confirmed that the only batch job managed by the Pension Fund are the scheduled monthly reports. A process will be implemented to manage any change to these. It will involve the change and sign off by Senior Systems Officers.

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 UAT testing completed for Altair changes** We noted that for the sample change obtained, testing was not conducted before promoting the change into the live environment. Additionally, no approval was given prior to implementation. However, we noted that post implementation approvals were given to confirm the change implemented had met that change request. **Risk** Failure to adequately perform change management testing prior to releasing the change into the production environment could lead to a loss of data integrity, processing integrity and/or system down-time.	Management should ensure that change management procedures are recommunicated to staff so that testing is performed and approved prior to introducing a change into the live environment. **Management response** When a system release is being deployed by Heywood's there will be Systems Team Leader sign off on the test plan following the testing undertaken in the TEST environment to the release being deployed into the LIVE environment. Please note that dates to the TEST and LIVE environment are agreed before testing is undertaken.

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

Cyber Security Assessment Findings

	Assessment	Issue and risk	Recommendations
1.	🟠	**Lack of a cyber security policies and procedures** During our review, we observed the following deficiencies in the Council's cyber environment: • We identified that the Council does not adhere or implement a cyber security framework in place to govern its IT environment • We identified that the following cyber security related policies in place (Asset Management, Back Ups, Risk Management and Business Continuity) did not consider cyber security related issues. Additionally, the Asset Management, Risk Management and Back Up policy had not been reviewed during the audit period. • We identified that the Council's security configuration standards and configurations for IT components are not documented. • We identified that data retention and monitoring policies are not in place. However, we acknowledge that they are under development with the goal of being implemented in the next financial year. • We identified that the IT organisational chart does not reflect those responsible for oversight and management of cybersecurity and its relevant controls. **Risk** Cybersecurity operational processes and control requirements may not be communicated to or understood by those within the organisation responsible for observing and/or implementing them	The Council should implement a cyber security framework that is followed to design, implement, and monitor cybersecurity controls. The Council should maintain documentation that details the cyber security policies governing the IT environment. These policies should be reviewed periodically to reflect and take into consideration the current cyber security landscape. **Management response** a) Policy and communication: The council is in the process of creating a cyber strategy. SC does review its IG policies with cyber security in mind as part of the overall risk to the organisation but to simplify policy, cyber threats are not specifically given their own mention, but applicable controls are included. This has been a conscious decision to create policies that are applicable to many risks rather than create specific section or policies related to specific risks. The backup policy is mentioned and that does have cyber elements such as a requirement for backups to be immutable but does not mention cyber although this is specifically a cyber threat requirement. The council also forcibly mandates completion of its cyber training withholding access to council systems for those not completing it. The council has also recently issued a request to system owners to review their supply chain arrangements in light of Central Government and NCSC advice. b) Cyber Framework: We agree that this would be beneficial and there is an existing internal audit recommendation. This will be considered as resourcing and priority allow. c) Cyber policy documentation: The council is in the process of creating a cyber strategy and policy changes may arise from the strategy.

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

Cyber Security Assessment Findings

	Assessment	Issue and risk	Recommendations (cont.)
1.	●	**Lack of a cyber security policies and procedures**	I would also add that the council has incorporated cyber and other risks into a supplier procurement document. We require new externally facing systems to provide evidence of vulnerability testing or we conduct 3rd party testing to provide assurance of data protection. We undertake external 3rd party assessment of our security controls multiple times a year. We have a 24x7 SOC monitoring and driving cyber response activity. The risk team are undertaking a major exercise to ensure business areas have reviewed their DR and BC plans specifically in relation to cyber. Directors require regular official updates on the council's cyber readiness via the IGLOO process. We recently undertook a real-world exercise to test ICT and directors' response to a potential cyber incident and a further Cyber response exercise is planned based around a loss of key material systems. Overall SC focuses a great deal of attention to attempting to manage the cyber threat.

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

	Control Name and Description	Reason/Justification
1.	Administrative access to the Altair database.	No controls relating to privileged access to the database were identified in the Service Now SOC 2 type II report.
2.	Batch management within Altair.	No evidence was available to verify that batch jobs had not failed during the audit period. Therefore, we were able to test this 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

Review of findings raised in prior year

Assessment	Issue previously communicated	Update on actions taken to address the issue
✓	**Lack of review of information security/audit logs in the Active Directory**	This finding has been remediated.
X	**Insufficient evidence of Implementation of Cyber Security Controls**	This finding has not been remediated. Please refer to Cyber Security Assessment Findings - finding 1 in this report for more details on the prior year finding.

Assessment

✓	Action completed
X	Not yet addressed

‘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.