Grant Thornton

IT Audit Findings

Dorset Council and Pension Fund

Year ended 31 March 2024

Issued 12 September 2024

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

Alex Korolchuk
Engagement Manager, IT Audit
T: +44 (0)20 7184 4459
E: Alex.Korolchuk@uk.gt.com

Thato Khumalo
Assistant Manager, IT Audit
T: +44 (0)20 7728 2249
E: Thato.Khumalo@uk.gt.com

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

Kamal Abdulahi
Associate, IT Audit
T: +44 (0)20 7383 5100
E: Kamal.Abdulahi@uk.gt.com

Muhammad Haseeb
Associate**,** IT Audit
T: +44 (0)20 7383 5100
E: Muhammad.Haseeb@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 Dorset Council and Pension Fund ("Dorset") 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 Dorset 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, implementation and operating effectiveness controls review over Dorset's IT environment to support the financial statement audit. The following applications were in scope for this audit:

- SAP
- Capita
- UPM
- Active Directory

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

- Evaluated the design, Implementation and operating effectiveness for security management and change management controls and cybersecurity
- 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 Dorset's 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 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.

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 only)	🔴	🔴	🟢	🟡	**n/a**
Capita	Detailed ITGC assessment (design effectiveness only)	🟡	🟡	🟢	⚫	**n/a**
UPM	Detailed ITGC assessment (design effectiveness only)	🟡	🟡	🟢	⚫	**n/a**
Active Directory	Detailed ITGC assessment (design effectiveness only)	🟢	🟢	⚫	⚫	**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

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
1.	🔴	**Users with inappropriate access to ABAP debugger in production** ABAP debugger is used for performing debugging functions such as inserting a code to correct any errors in the source code. Users are therefore able to execute unauthorised transactions through these amendments to code. We noted that there were 26 active Dialog(A) accounts and 1 Service (S) assigned with access to ABAP Debugger in production granted via S_DEVELOP authorisation object. Refer to ***Appendix 1*** for the list of users. We further observed that 20 users had made program attributes changes, accounting header documents changes and master data changes during the audit period. The 7 others have access to ABAP debugger in production but have not made any changes during the period. **Risks** Unauthorised access to ABAP debugger increases the risk of: • unauthorised change or deletion of table entries including tables that are typically protected by SCC4, • the ability to perform debugging functions by inserting break-point statements into program code • the ability to bypass authority checks and execute transactions	It is recommended that management remove ABAP debugger access permanently from production. It is best practise to use Firefighter accounts with an approved business case and set validity period. **Management response** As discussed, our understanding was that the ability to debug and amend code was not possible simply with the S_DEVELOP authorisation and that access to the object types was also required to carry out any debugging. In finding that the object type was embedded within another role, which then did give the ability to debug, we have since removed access from that role. In which case, debug access can now only be gained through being granted access to the debug role, which can only be gained through a request to the Security Officer and authorised by the ICT Operations Manager. We also capture this approval in the monthly audit reports for full transparency as to who has been granted access at any time.

Assessment

🔴 Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.

🟠 Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach

🟢 Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
2.	🟠	**Segregation of Duties Conflict as developers have access to production** We compared all users with the ability to develop changes in development with those with the ability to create/import transports in production and identified the following: • there were 4 users with the ability to develop changes in development and create/import transports in production via STMS. • of the 4 users, 3 users had the ability to develop changes in development and import them into production via Standard Transport Management System (STMS). In response, we compared the list of users that created transports in development and those that created/imported transports in production and noted that there was 1 user that had created transports in development and released the same transports in production. Refer to ***Appendix 2*** for usernames. **Risks** The combination of access to develop and implement those changes in the production environment creates a risk that inappropriate or unauthorised changes are made to data and/ or programs	Management should segregate a user's ability to develop and implement changes. Privileged access to the production environment should be revoked from users that are involved in development. If for operational reasons access cannot be fully segregated, alternative options to mitigate the risk could include performing a review of change implementation activity logs. These should be regularly reviewed for appropriateness by an independent individual with evidence retained. **Management response** Developers hand off their transports to the BASIS and Security teams, so development transports are not promoted into Production by the same person that created it. Security teams are technical stewards of the system, which is the reason for them to be able to transport into production, as they facilitate the transports into production for the rest of the team. However, for patching, security maintenance and system configuration, their day-to-day role also requires them to have permissions to develop and create transports themselves. It would not be feasible for us to have a technical subject matter expert that was only able to transport into production but did not have development permissions also. Transports being promoted into production by the same person that created it only happens by exception and is now logged and monitored through our monthly audit report. In the example provided, the team were in firefighting mode, immediately after the SAP legislative patch had been applied, so is classed as an exceptional circumstance.

Assessment

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

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
3.	🟠	**Users with inappropriate access to maintain all SAP Standard or Customised tables in production** Our IT audit procedures identified 22 Dialog user accounts that were assigned access to maintain all SAP standard or customised tables via SM30 or SM31. Refer to ***Appendix 3*** for the list of users. **Risks** 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.	Management should segregate a user's ability to maintain all the standard or customised SAP tables within production. We recommend that for the users identified, management should consider assigning access to relevant table groups or individuals tables via S_TABU_DIS and S_TABU_NAM authorisation objects rather than assigning the authorisation values to '*'. **Management response** To maintain SAP tables, the client needs to be opened which can only be done through a request to the BASIS team and authorisation from the ICT Operations Manager, which is then also recorded on the monthly audit report for full transparency. The table changes are also logged in addition. Having access to SM30 and SM31 alone is not sufficient to be able to maintain SAP tables. There is occasion where maintenance needs to be carried out, for example, to correct problems that it is not possible to correct through the application front-end. These changes are not transportable, i.e. it is not possible to make the change in the development system and transport it through, so need to be carried out in the production system with the appropriate audit trail and is why the access is required.

Assessment

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

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
4.	●	**Password settings not in line with the organisation's password policy** We noted that the following password settings were not configured in line with the organisations password policy and/or the National Cyber Security Centre (NCSC): • The password policy states that the password length should be 15 characters. The System User Defined value is only set at 8 characters. • The password policy states that users no longer enforce password expiration, which is in compliance with the NCSC, however the system is set for password expiration of 180 days. **Risks** A lack of robust password settings may allow financial information to be compromised by unauthorised users.	Management should ensure that password settings configured on SAP are in line with the organisation's password policy. **Management response** Updating the password policy would potentially be very disruptive and a significant piece of work to test and implement. It is felt that with an on-premise implementation, a user would already need to have access to our internal network, so is potentially a very low risk, and as such, updating the policy has not been a priority to implement. Our preference is to move to single sign on, so efforts have been directed into progressing this.

Assessment

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

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
5.	●	**User access within SAP was kept valid after the user's termination date** It was noted during the audit, that a user was terminated on the 21st of December 2023, however their SAP account was still valid to 30th of January 2024. Upon reviewing the last login dates, we noted that this account had not been accessed since date of departure. Refer to ***Appendix 4*** for the name of the user. **Risks** Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions. There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.	Management should ensure that a comprehensive user administration procedures are in place to revoke application and AD access in a timely manner. For a user administration process to be effective, IT must be provided with timely notifications from HR and/ or line managers Management should consider performing user access reviews on all terminated accounts to ensure all accounts have been disabled in a timely manner. Where old or unused accounts have been identified, these should be immediately revoked. **Management response** Between November 2023 and January 2024, we had long-term absences in the team to mean business as usual activities were impacted. Our standard process for a leaver is that a user has access removed on the date of leaving to mean no functions can be carried out within the system. After two weeks, the account is then disabled. A backup process of all accounts with no activity for three months being disabled is also in place. We are now also looking at building resilience in the team to be able to manage a similar scenario of long-term absences occurring.

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

General Applications ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
1.	●	**Inadequate control over privileged accounts within Capita** We observed that the Capita administrative accounts are shared by 6 members of the Technical Support and Development Service. Refer to ***Appendix 5*** for the list of user accounts. We performed mitigating procedures to confirm that the usage of the accounts were restricted to the 6 members. **Risk** 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 implement suitable controls to limit access and monitor the usage of shared 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 – Revs & Bens Capita System** The principle of restricting the number of administrators to minimise the risk of unauthorised or inappropriate changes to the application or database is accepted and already implemented. We believe that the current number is appropriate to our method of operation and the working patterns of the Technical Support & Development Team. Only the six Technical Support and Development team members, which includes the Service Manager, use the “generic database admin account” as it has database administration system permissions which they all need and which other regular users in Revenues and Benefit service wouldn't have (approx. 90 users). We do not consider six users to be excessive and reducing the number of users in the team with access may add risk to the operation of the systems if adequate cover is not available due to sickness, staff leave etc. This access is limited to the necessary users in the service and only those that have database administration duties. The Service Manager accepts the risk. If circumstances change and it is possible to review this, then we will do so. The Head of Service is aware of this and in agreement. The Capita One Revenues and Benefits software does not provide facilities to enhance accountability for users of generic accounts as per the password vault tool suggestion however there is an Audit trail/ Event Log detailing the action of “generic database admin account”’ user (and all users). It is possible to select a combination of date ranges, screen identification numbers and/or usernames, to retrieve a set of events that have occurred, although is limited in detail of some events. The Domain User ID column in the Event Log frame populates with the windows login of the user. This removes the anonymity of a user logged in as “generic database admin account”’ – therefore, generic user account activities are traceable to an individual, and this was evidenced during the review. Until the Audit review, the Event Log had not regularly monitored for “generic database admin account”’ activities, although it is used for other monitoring. Since the review, initial monitoring of the activities performed by “generic database admin account”’ generic user via the event log have commenced and will be undertaken and reviewed to ensure no unauthorised users are accessing the system via the generic user account and additionally monitored to ensure no unauthorised activities are performed. This will be documented and recorded and available for subsequent reviews.

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

General Applications ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
2.	🟠	**User access within Capita and UPM are not appropriately revoked for terminated employees** Application access is not revoked for terminated employees in a timely manner. For a sample terminated user in Capita, we observed that the request to terminate a leaver was submitted 2 business days after the user had left the Council. For a sample terminated user in UPM, we observed that the sample user was deleted from the system 4 business days after they transferred out of the Pensions department. **Risk** Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions. There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.	The Council should ensure that a comprehensive user administration procedures are in place to revoke application and AD access in a timely manner. For a user administration process to be effective, System Support must be provided with timely notifications from HR and/ or line managers The Council should consider performing user access reviews on all terminated accounts to ensure all accounts have been disabled in a timely manner. Where old or unused accounts have been identified, these should be immediately revoked. **Management response** **UPM** • Pension Managers have been advised to notify the Systems Administrators in a more timely manner. **Capita** • Changes to user system access, including revoking all access to the Capita system are generated by the relevant Service Managers and/or Team Leaders. It is the responsibility of those officers to ensure that the information is passed to the Technical Support and Development Team for the user access to be revoked in a timely manner. We recognise that we are relying on information from busy officers who may forget to advise of long-term absence or termination etc, and so we have recently attempted to obtain more timely information direct from HR with regard to starters and leavers, but unfortunately, this has not been possible due to system limitations. • Officers/ Management teams have been reminded to notify the Technical Support and Development Team of new starters and leavers in a timely manner to reduce risk of unauthorised access. • We believe that the Capita system access for terminated employees is usually disabled in a timely manner (from the point of notification) by the Technical Support and Development Team, with our current levels of resourcing, this includes all old or unused identified accounts. • The case we shared with you was notified to the Technical Support and Development Team, 2 business days after the user had left the council.

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

General Applications ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
3.	🟢	**Lack of formal cybersecurity policies or procedures** Upon review of the cybersecurity control environment, we have identified the entity does not perform active backup testing. **Risk** The absence of a specific process to conduct active backup testing pose a control risk to the entity's cybersecurity posture. This deficiency could lead to vulnerabilities and increased likelihood of successful cyber-attacks.	We recommend implementing the following controls: • Establish a structured program for active backup testing to maintain the integrity and recoverability of critical data. • Regular testing should be performed to validate the effectiveness of backup procedures and identify any weaknesses in the backup and recovery processes. **Management response** Backups are verified on creation and integrity checked. Backups are tested in part as deleted information is regularly restored for users and ICT support teams as part of BAU operations. It is acknowledged that the council would benefit from a more formal backup verification policy. The development of this policy and subsequent process will be discussed internally.
4.	🟢	**Lack of formal review of the Service Auditor Report** We noted that the Council does not review the Service Auditor Report (SOC1 Type 2 or a ISAR3402) provided for Capita. **Risk** Without adequate oversight and monitoring over the service auditor report on business controls procedures, there is an increased risk that controls over financial reporting operated by the service providers might not be designed, implemented and operating effectively	The Council should consider formally reviewing the Service Auditor Report for control weaknesses in order to assess the relevance impact on the business functions Consideration should also be given to identifying complimentary user entity controls specified within the report and ensuring that they are implemented and operating effectively within the Council’s IT environment **Management response** We have not received a copy of the required report from Capita, and after reaching out to Capita One operations and technical managers, they have indicated that they are unaware of such a report being available. We have shared a copy of Capita One latest Network Penetration Test report and ISO27001 and Cyber Essentials certification.

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

General Applications ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
5.	🟢	**Lack of review of audit logs for Capita** Information security event logs, which capture the monitoring of activities performed by users with privileged access within Capita were not reviewed. **Risks** Without formal and routine reviews of security event logs, inappropriate and anomalous activity may not be detected and resolved in a timely manner. Additionally, unauthorised system configuration and data changes made using privileged accounts will not be detected by the Council.	Considering the criticality of Capita and UPM for financial reporting, information security events 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 should be logged and formally reviewed. It is recommended that security event logs are reviewed on a regular basis for example daily or weekly, ideally by an IT security personnel / team who are independent of those administrating Capita and UPM and its underlying database. Any issues identified within these logs should be investigated and mitigating controls implemented to reduce the risk of reoccurrence **Management response** Changes to parameters, tables and data by database administrators is already logged. We will discuss a process with SWAP that further reviews the system event logs and actions by administrators, under our continuous audit arrangement.

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

grantthornton.co.uk