IT Audit Findings

Dorset Council and Pension Fund

Year ended 31 March 2026

Issued 20/05/2026

Timothy Mukiwa
Engagement Lead, IT Audit
T: +442071844357
E: Timothy.Mukiwa@uk.gt.com

Onkar Falekar
Engagement Manager, IT Audit
E: onkar.Falekar@uk.gt.com

Merin George
Junior OTM, IT Audit
E: Merin.George@uk.gt.com

Sravani Vinjamuru
Junior OTM, IT Audit
E: Sravani.Vinjamuru@uk.gt.com

Contents

Section 1: Executive summary

To support the financial statement audit of Dorset Council and Pension Fund ("Dorset") for year ended 31 March 2026, 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 members of the Dorset team for their support and cooperation in the completion of this IT audit.

Section 2: Scope and summary of work completed

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

- SAP
- R&B
- Active Directory

The following applications were in scope for this audit specific to Dorset Pension Fund:

- SAP
- UPM

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

- Evaluated the roll forward ITGC assessment 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

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 D&I					**n/a**
R&B	Detailed ITGC assessment D&I					**n/a**
UPM	Detailed ITGC assessment D&I					**n/a**
Active Directory	Detailed ITGC assessment D&I					**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: Details of IT audit findings

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
1.		**Users with inappropriate access to Develop and import changes** GT compared all users with the ability to develop changes in development with those with the ability to create/import transports in production and noted that there are 4 users with access to Develop and import changes into the production system creation SOD conflict. **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** The four developers have access to both development and to transport changes into production, this is due to capacity in the support team. We have minimised the number of people that can transport changes into production as much as possible, whilst enabling us to operate. These 4 members of the SAP support team also need to be able to make changes, so we're unable to place a segregation in this area. The alternative would be for someone outside of the SAP support team to apply transport changes to production, which is seen as a greater risk. To mitigate the risk we record the transports that have been promoted to the production system in our monthly audit report and highlight if an exception occurs, which is either; an unexpected user transports a change, or a transport was created and transported by the same person. This report is reviewed by the team Manager by exception. This happens very rarely and has only occurred in the past through a patching activity, where we are in "firefighting mode".

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.		**Users with inappropriate access to Development access in production system.** GT noted that one user has direct development access in the production environment. In addition, the user has access to sensitive transactions SCC4 (Client Opening) and SE06 (Maintain Global Settings) in the production system. However, we further noted that access to transaction SCC4 and SE06 has been removed from this user following our observation being raised. **Risks** Developers with production access can introduce, modify, and execute code without independent review or approval, bypassing change management controls and increasing the risk of unauthorized or inappropriate changes.	Management should remove direct development access to the production environment and enforce strict segregation of duties. Where exceptional access is required, it should be provided on a temporary, approved, and monitored with full logging and post-implementation review. Access rights should be reviewed periodically to ensure alignment with the principle of least privilege. **Management response** Following the draft findings of Grant Thorton we were able to review our ability to provide cover and/ or segregation of duties. To that end as recorded we were able to remove this user from having direct access to development in production to provide enhanced security.

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 Configure and delete audit logs in production system.** GT noted that there are 4 users with access to Configure and Delete audit logs. However, we further noted that access to transaction SM19 (Configure Audit Log) has been removed from the relevant BASIS roles following our observation being raised. **Risks** Inappropriate and anomalous activity may not be detected and resolved in a timely manner.	Management should segregate a user's ability to configure (SM19) and delete (SM18) user security event logs within production. If for operational reasons access cannot be fully segregated, alternative options to mitigate the risk could include usage of Firefighter accounts with a set validity period based on formal approvals. **Management response** As documented, we have removed SM19 (Configure Audit Log) and in so doing negated the requirement to segregate users ability to both configure and delete, as configure is no longer available. To be able to free space on the server we do need to occasionally remove logs, we therefore felt that we are not able to delete SM18, which is the second recommendation.

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.		**Users with inappropriate access to maintain global settings** GT noted that there are 4 accounts that have access to transaction SE06 (Maintenance of Global Settings) in the production system. This level of access poses a risk of unauthorized or inappropriate changes to system-wide configuration settings, potentially impacting system integrity, security, and financial reporting. However, we further noted that none of the users executed transaction SE06 during the audit period. Additionally, access to this transaction has since been removed for the identified users. **Risks** This transaction provides the ability to perform critical system configuration activities. Inappropriate or unauthorized use of this access could result in unapproved changes to system settings, potentially compromising system integrity, operational stability, and compliance.	Management should remove access to maintain global client settings in production environment and enforce strict segregation of duties. Access rights should be reviewed periodically to ensure alignment with the principle of least privilege. **Management response** As documented, none of the four members had utilised SE06 (Maintenance of Global Settings) and we have removed access to SE06 from all four accounts as per recommendation.

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.	●	**Inadequate control over Generic account in SAP** GT Noted that a generic user account is used to execute background jobs. However, this user is configured as type "S – Service," which allows interactive login using credentials. This creates a risk of unauthorized system access and inappropriate activities being performed without individual accountability. Furthermore, no controls were identified to restrict access to this user ID or to govern password management, increasing the risk of misuse and control circumvention. However, we further noted that the user type for this account has been changed from Service (Type S) to System (Type B) following the observation being raised. User accounts classified as Type B – System are non-interactive and are not permitted to log on using standard credentials. **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.	Management should undertake a review of all user accounts on the application to identify all [generic/ privileged] accounts. If the account is used solely for executing background jobs and is not assigned to any individual user, it is recommended that the generic user account be reclassified to user type B (System) or user type C (Communication) post internal impact analysis. This change will prevent interactive logon using credentials and reduce the risk of unauthorized access. **Management response** As documented, to mitigate any risk, we have now changed this account to a system user so it can not be logged in with. Also to confirm, this account has never been logged into historically.

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 – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	**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. 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. **Risk** 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	• This deficiency has been remediated.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	**Segregation of Duties Conflict as developers have access to production** GT 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 2 user accounts with no longer required access to develop changes in development environment as well as 19 background system user accounts; • there were 2 accounts with access to import transport requests (via STMS) belonging to a former member of SAP Support Team and a background user account; • there were 3 developers with access to implement changes in production environment, having access to both development and transport changes to production. GT verified that all users were members of the SAP Support or HR Systems teams, hence a general recommendation has been made to remove access for the generic background system accounts and those users no longer requiring SAP development functionality. **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	• This deficiency has been partially remediated. • Refer to SAP ITGC Assessment Finding 1.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	**User access within SAP was kept valid after the user's termination date** A leaver with a leaving date of 30 August 2024, we confirmed that the account was deactivated on 02 September 2024, 2 business days after the leaving date. GT confirmed that this was due to the leaving date occurring on a Friday and the request being actioned the following Monday. **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.	• This deficiency has been remediated.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	**Ineffective production client configuration settings** GT identified that the Global System Change Option (SE06) settings were set to 'Modifiable' within production client. This setting allows direct changes to objects associated with ABAP software components in production. GT have confirmed that the setting was changed as part of an approved request on 04 June 2024 and the 'Changes and Transports for client specific objects' is set as 'No changes allowed'. **Risk** If client settings are not configured to restrict direct changes to repository objects or cross client customising objects in production, there is a risk that there could be unauthorised changes to financially critical production data.	• This deficiency has been remediated.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – UPM

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	**Lack of oversight over third-party users assigned privileged systems access in UPM** GT has identified the following Civica vendor user and generic accounts with privileged access assigned in both application and MS SQL database layers of UPM system: • Application - 1 user and 2 generic accounts; • Database - 32 user and 2 generic accounts. *Refer to Appendices file, tab "UPM Accounts" for further information*. Due to the lack of SOC 1 Type II attestation for UPM system provider Civica, GT is unable to gain assurance over appropriateness of the user access for these accounts or of any activity performed. We noted that the access for these accounts is provided on a permanent basis and neither activity monitoring nor user access reviews are performed by Dorset. Separate inquiry procedures were conducted with the Civica vendor regarding their change management process and privileged access controls. However, no additional evidence was provided to substantiate the high-level control procedures outlined. **Risks** Without adequate oversight over the third-party users of system administration accounts, there is an increased risk of unauthorised or inappropriate changes to the underlying data. In addition, usage of shared/ generic third-party accounts create a lack of accountability around changes made within the system.	• This deficiency has been remediated.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – Active Directory

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	**Lack of oversight over a privileged generic account in Active Directory** GT was not provided with complete evidence relating to the management of the password to 1 generic AD account, such as: - account last log in date; - whether the password is held in secure location/password manager; - whether the password is changed after each use. Furthermore, GT has confirmed that this generic user ID is used as a support account, however, its activity is not logged and monitored. **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 excessive use of accounts with privileged access increases the risk of end-users being able to: - change system configuration settings without authorisation and approval - read and modify sensitive data, - create, modify or delete user accounts without authorisation, - delete or disable system audit logs	• This deficiency has been remediated.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – Active Directory

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	**Lack of formal activity monitoring over generic user ID in Capita** GT confirmed a lack of formal activity monitoring review documentation for the following privileged generic accounts: • 2 generic administrative accounts that are shared by 6 members of the Technical Support and Development Service. • 1 generic user ID with privileged access to the application, which is used by Capita vendor to provide remote support. Furthermore, GT was not provided with last log in dates for these accounts to verify whether their activity falls within the April 2024 to March 2025 audit period. **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 management.	• This deficiency has been remediated.

Assessment
✓ Action completed
X Not yet addressed