IT Audit Findings

Dorset Council and Pension Fund

Year ended 31 March 2025

Issued July 2025

Sumit Saroha
Engagement Lead, IT Audit
T: +44 (0) 20 7865 2210
E: Sumit.Saroha@uk.gt.com

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

Rupanshu Singh
Associate, IT Audit
T: +44 (0) 20 7865 2501
E: Rupanshu.Singh@uk.gt.com

Edward O Hodgson
Associate, IT Audit
T: +44 (0) 11 7305 7604
E: Edward.O.Hodgson@uk.gt.com

Contents

Section		Page
1.	Executive summary	3
2.	Scope and summary of work completed	4
3.	Summary of IT audit findings	5
4.	Detail of IT audit findings	7

Section 1: Executive summary

01. Executive summary
02. Scope and summary of work completed
03. Summary of IT audit findings
04. Details of IT audit findings

To support the financial statement audit of Dorset Council and Pension Fund ("Dorset") for year ended 31 March 2025, 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. Details of IT audit findings

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
- Capita
- 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

01. Executive summary
02. Scope and summary of work completed
03. Summary of IT audit findings
04. Details 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	Roll Forward ITGC assessment					**n/a**
Capita	Roll Forward ITGC assessment					**n/a**
UPM	Roll Forward ITGC assessment					**n/a**
Active Directory	Detailed ITGC assessment					**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

01. Executive summary
02. Scope and summary of work completed
03. Summary of IT audit findings
04. Details of IT audit findings

SAP ITGC Assessment Findings

	Assessment	Issue and risk	Recommendations
1.		**Users with inappropriate access to ABAP debugger in production** GT noted that access to perform debug in the system had been provided to 8 users from Payroll team to run payroll activities and 3 users from the Business Solutions Engineer team to manage the application respectively, while it should not have been granted to any user in perpetual mode. *Refer to Appendices file, tab "SAP - ABAP Debugger" for further information*. **Risks** Unauthorised access to ABAP debugger increases the risk of: • unauthorised change or deletion of table entries including tables that are typically protected. • the ability to perform debugging functions by inserting break-point statements into program code • the ability to bypass authority checks and execute transactions	The Council has taken initial steps to mitigate the risks previously identified from our work and findings in the prior period, by reviewing the specific debugger users and reducing these from 26 to 11 users. Per discussion with management and control owners it was noted that debug access was retained for the Council's payroll team as they need to manage Z tables (customised tables) and run the payroll. Due to the high frequency of occurrence of these payroll activities, FireFighter IDs or breakglass controls were deemed not feasible to be embedded in the current set up. By removing the debug access from these remaining 11 users, it was found to impact the payroll run activities to the point they were unable to run the Council's payroll. Management are seeking to identify alternate controls to mitigate the high risk of debug access in system for these remaining users. This should be implemented either by effecting the breakglass technology and/or GRC controls mechanism and/or automating certain elements of the payroll process. Whilst this level of access currently remains, this continues to present a risk to the Council of unauthorised access and change functions within SAP, as highlighted in our risk assessment. **Management response** From the recommendation made by Grant Thornton in last year's audit, we have significantly reduced the access to the debug authorisation to mitigate the risk that this issue poses. We have removed it from standard IT support roles and introduced the process that debug needs to requested and approved, before it is granted and logged. There are still some specific scenarios where operationally certain authorisations are still required, which we are working on how we can minimise the access required as much as possible.

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** 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. *Refer to Appendices file, tab "SAP - Developer Implementer SOD" for further information*. **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** At the point the two development users left the authority, they no longer had access to the SAP system by virtue of the fact that their network account was locked and corporate devices were returned. Also, no development changes have been made with those users since they left, and suspicion would have been raised had any transports been created with those users and so would not have subsequently been released into production. The two users have now been locked. The 19 background system user accounts have now been set from dialog to system users to stop the ability for them to be used to log into the system. The two accounts with access to import transport requests (via STMS) belonging to a former member of SAP Support Team and a background user account were both locked at the point the person left the organisation and when the background account was no longer required, so both were not active and could not be used to log into the system. Authorisations have now also been removed as well. The three developers having access to both development and transport changes to production 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, but still allowing us to operate. These three members of the SAP support team do also need to be able to make changes as well, 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. The mitigations in place are that 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 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
3.	●	**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.	Management should ensure that a comprehensive user administration procedures are in place to revoke application and AD access in a timely manner, before or on the leavers last working date. 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** Our standard leaver process is that all system access is automatically removed from the account on the day the employee leaves. In this example, this means on Friday 30th August 2024, the account had no roles or authorisations and so was unable to do or see anything in the system. We then locked the account as part of our weekly leavers process on Monday 2nd September 2024, which then completes the deactivation process. The second stage to this is a manual step and so would not be feasible to carry this action out more frequently than a weekly basis, but with the first stage of removing all access from the account having already completed, means this is an extremely low risk.

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.	●	**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 SR4010905 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.	Management should ensure that the parameter 'SE06 – System Change Option' settings are consistently set to 'Non-Modifiable' in production client. **Management response** On this occasion SE06 was left open at the point SCC4 was closed. Our standard process is to open and close the production client in both SE06 and SCC4 simultaneously. SCC4 being closed greatly reduced any risk that SE06 being open posed, however, this is not our standard practice and so we will monitor that both SCC4 and SE06 are both closed together to ensure we minimise any future risk.

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.	●	**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.	Management should undertake a review for all IT support partners to confirm how they obtain assurance over appropriate IT controls being implemented / operated by third-party service organisations. This should, as a minimum, include the controls over privileged production or database access, such as: - approving vendor access for specific requirements and disabling after completion - reviewing account activities performed Where independent service organisation assurance reports are available, management should assess the findings and consider whether complementary user entity controls are effective. **Management response** Dorset follow the guidance of our System Provider CIVICA on how to grant them access, maintaining individual access will create more of a risk to the Pension Fund (UPM) if CIVICA neglect to inform us when users leave their business. We are not informed in a timely manner of staff turnover at CIVICA which raises the risk of unauthorised users if they have left the business, and we are not notified.

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.	●	**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. *Refer to Appendices file, tab "Active Directory Accounts" for further information*. **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.	Management should undertake a review of all user accounts on the AD to identify all generic privileged accounts. For each account identified management should confirm: - requirement for the account to be active and be assigned privileged access; - which users have access to the account and business justification for retaining such access; - controls in place to safeguard the account from misuse. Where possible, privileged generic accounts should be removed, and individuals should have their own uniquely identifiable user accounts created to ensure accountability for actions performed. Alternately, management 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 account identified is an application service account. The application captures the AD account name of the logged in user, verifies and logs the action taken. Entra ID logs the actions of this account within the rest of the infrastructure. Whilst a complete log is not stored in one place combining these logs show a complete picture of the account activity.* *Users are only able to use this account to carry out tasks for which they are approved, and this is controlled by the application using the service account rather than the specific permissions of the AD account.* *The account is managed by the application owner. The account is recorded in a secure location and was last used 30/01/2025 18:43:47. This account is monitored in AD in the same way as any other and is subject to the same controls and restrictions as required by the council policy.*

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 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. *Refer to Appendices file, tab "Capita Accounts" for further information*. **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.	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 its underlying database. Any issues identified within these logs should be investigated and mitigating controls implemented to reduce the risk of reoccurrence. **Management response** Security event logs for privileged user accounts used by Technical Support and Development Team are now reviewed by Business Development Team who are familiar with the software but do not have administrative rights, to mitigate the risk of not detecting inappropriate an anomalous activity in a timely manner. Security event logs for privileged user accounts 'academy' used by Capita/MRI Remote Support Team are now reviewed by Technical Support and Development Team to mitigate the risk of not detecting unauthorised system configuration and data changes in a timely manner.

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
4.	●	**Capita Access Termination Process and System Limitation Review** Upon inspection of user access termination request sample, GT noted the following: - the request was raised for Revenues Officer staff, who left the organisation on 19 July 2024 (Friday). - the request was submitted by a business user on 22 July 2024 (Monday) and was disabled by Technical Support and Development Team. GT noted a system limitation was whereby the system does not maintain the date and time stamp of the user's access revocation; hence, we could not verify that the user access from the system was revoked on 22/07/2024. Additionally, although the IT Team actioned the leave request in a timely manner and the access was revoked within 1 business day after the user's termination date, it is best practice to disable users at the end of the users last working day. **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.	It is recommended the notification by business users to Technical Support and Development Team to be submitted before the user's termination date, so that the IT personnel can revoke access at the end of the users last working day. Furthermore, consider the possibility of extending the system tracking to include a date and time stamp for access revocations. This feature will allow for better verification of when access was terminated, thereby improving accountability. **Management response** The Technical Support and Development Team proactively reminds managers to notify them of upcoming changes ahead of the effective date. However, when information is not received in advance, revocation is promptly actioned (1 business day) to mitigate the risk of unauthorised account access by a former employee. When advance notice is provided, the team ensures that access is revoked on or before the user's last working day, or if the user is working beyond normal business hours, it has been actioned on the immediate next working day. We will now communicate that revocation will happen by 4pm on the last employment day. While this approach may result in some access being forfeited on the final day, in most cases, the user's last working day precedes their official employment end date. GT recognised the system limitation within the batch program User Permissions as it does not output a timestamp on revoked accounts. This is out of our control as dependent on Capita/MRI software development. We can however record this manually at the time of revocation to improve accountability and will start to do this upon the next revocation.

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

	Expected control name and description	Reason/Justification
1.	**Segregation of duties for UPM and Capita** Administrative privileges (including generic super user access rights) to the network, applications and their associated databases are restricted to those users requiring this level of access (in line with their roles and responsibilities). Privileged duties do not conflict with other roles. **Creation and modification of vendor accounts for UPM** Access to any application (in line with the starter's roles and responsibilities) is requested and approved by the new starter's line manager (or equivalent person) before being granted by someone from IT. **Vendor change management for UPM and Capita** Vendor develops changes which are tested in an environment separate from the production environment. Vendor developers do not have continuous access to the production environment and cannot implement their own changes into the production environment.	GT was unable to obtain SOC 1 Type II reports for Capita and UPM systems, as the vendors Capita One and Civica do not undergo the level of attestation required to gain assurance over the design and effectiveness of the vendor-related controls. Within the audit period of 2024/2025, GT was not able to provide assurance over the vendor segregation of duties controls in relation to privileged accounts on Capita and UPM application and database layers. Additionally, the lack of assurance applies to change management controls of both systems, such as those specifically governed by the Capita and Civica vendors. These include development and implementation of changes, segregation of development, testing and production environments as well as developer vs. implementor segregation of duties. *Please note, this observation is subject to GT obtaining further evidence of Civica vendor controls as requested on 24/04/2025.*
2.	**User access termination for UPM** For leaver control, requests to revoke access to any in scope application is initiated by HR and / or their line manager ahead of the actual leave date and access revoked in a timely manner.	For UPM system, in the course of 2025 IT audit activities, it has been indicated that there were no leavers during the 2024/25 financial year. However, GT noted a system limitation whereby the date when users were terminated from the system is not displayed on the deleted users' page. Consequently, GT was unable to verify the resolution of the control finding from the previous year, and thus, cannot obtain assurance regarding this matter. *Please note, this observation is subject to GT obtaining complete HR list for the full audit period in review and subsequent analysis of UPM user list and HR leaver data as requested on 10/04/2025.*
3.	**Generic user accounts management UPM and Active Directory** Access to generic or shared accounts must be strictly controlled, justified, and approved. Only authorised users should be allowed to access passwords for privileged generic IDs, and only for specific, approved purposes. Generic credentials should be stored in a password vault. Access should be time-limited, with credentials automatically rotated or expired after use.	Specific to privileged generic accounts identified for UPM and Active Directory, GT was unable to gain assurance over the password keeper software. Specifically, this is in relation to identifying the personnel managing access to the following keepers: Server/Storage, Client Devices, Place - DBA, Place - GIS, SAP - Windows PWDs, Cireson & Server Manager, and Place – Applications. Additionally, GT was not able to verify whether the keeper software is in-house, or vendor developed. *Please note, this observation is subject to GT obtaining further evidence regarding the password keeper software, as requested on 22/04/2025.*

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	**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 partially remediated. • The number of users with ABAP debugger has been reduced from 26 to 11 in 2024/2025 audit period. • 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
X	**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. **Risk** 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 2.
X	**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. **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 improvement point has not been remediated. • Refer to SAP ITGC Assessment Finding 3.

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
✓	**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.	• This finding has been remediated upon further analysis of the password settings of SAP. The password length has been increased to 15 and the password expiration has been set to appropriate parameters.
✓	**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. **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.	• This deficiency has been remediated, upon further evaluation provided within the roll forward scope of the IT audit period of April 2024 to March 2025.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – General Applications

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	**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.	• This deficiency has been partially remediated. • Refer to General Applications ITGC Assessment Finding 4 and section “Controls for which assurance could not be provided”, point 2.
X	**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. **Risk** 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.	• This improvement point has not been remediated. • Refer to General Applications ITGC Assessment Finding 3. The finding additionally applies to UPM and Active Directory – refer to General Applications ITGC Assessment Finding 1 and 2.

Assessment
✓ Action completed
X Not yet addressed

Review of findings raised in prior year – General Applications

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	**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	• This improvement point has not been remediated. However, there has been additional information obtained during the 2024 to 2025 audit period, thus providing further context to this deficiency. • Refer to section “Controls for which assurance could not be provided”, point 1.
✓	**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.	• This deficiency has been remediated upon further analysis and evaluation of the cybersecurity environment and the specific industry context of Dorset Council & Pension Fund.
✓	**Inadequate control over privileged accounts within Capita** We observed that the Capita administrative generic accounts are shared by 6 members of the Technical Support and Development Service. 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.	• This deficiency has been remediated. • We have confirmed user access to generic user accounts is appropriately restricted to members of Technical Support & Development team and the activities performed on these accounts are traceable to individuals logging in, which was verified by the review of the Capita system audit logs.

Assessment
✓ Action completed
X Not yet addressed