

Internal Audit Report

Mosaic Application Review

December 2019

To: Interim Director, Adults Social Care
Business Systems Team Manager
Head of Performance and Improvement

Copied to: Assistant Director, Community and Performance – Audit Lead
Strategic Director for Adults & Health
Partner at Better Gov

From: Head of Internal Audit

We would like to thank management and staff of Barnet Council for their time and co-operation during the course of the internal audit.

Executive Summary

Assurance level	Number of recommendations by risk category				
Limited	Critical	High	Medium	Low	Advisory
	-	1	3	-	-
Scope					
<p>Mosaic is used by London Borough of Barnet (the Council) Adult Services as a fully integrated solution for Adult Social Care financial case management. It is designed to support social workers to focus on the service users and their outcomes, providing them with the tools and technology to work innovatively, to assess and understand the service users' needs and to capture these effectively in a single system. The Mosaic system was implemented during April 2017 and has approximately 530 users. The implementation and support of the Mosaic application moved from the vendor Capita, to BetterGov during the second half of 2018. Management did confirm that the project is still in the implementation phases, and the control environment will be developed and enhanced before 'business as usual' is achieved and any actions will be managed through the project.</p> <p>The purpose of the audit was to review the design and effectiveness of controls in relation to the Mosaic system. The review placed specific emphasis on the processes in place to effectively manage IT General Controls (ITGC).</p>					
Summary of findings					
<p>The Council has a number of key controls and processes in place to ensure that users are set up and removed from the system correctly. This includes some key functionalities needed to monitor user activity and protect the system from inappropriate user behaviour. However, the control environment could be strengthened if the Council embeds some more proactive monitoring controls to ensure that the system is being used appropriately, for example: regular user access reviews.</p> <p>This audit has identified 1 high and 3 medium findings:</p> <p>Generic User Accounts (high risk) – There are two generic user accounts in use. Following investigation one of these needs to be disabled and the controls in place regarding use of the second should be documented.</p> <p>User Access Reviews (medium medium) – User access reviews are not performed on a formal periodic basis. We identified two scenarios in our testing where inappropriate access existed (Leavers and Duplicate Accounts) which could have been prevented through the use of a periodic User Access Review.</p> <p>Change Developer Access to Production (medium risk) - Changes can currently be implemented by the two maintenance and support vendors (BetterGov and Capita) and/or the business systems team within Adults & Health. Users with 'Developer Access' can access both the development and production environments. This applies to vendors and business systems teams. This can increase the risk of unauthorised or inappropriate changes being made to the system.</p> <p>Disclosure & Barring Service (DBS) Checks for new users (medium risk) – 6/25 new users and movers tested did not have evidence of DBS checks being performed before being given system access.</p>					

2. Findings, Recommendations and Action Plan

Ref	Finding	Risks	Risk category	Agreed action
1.	<p><u>Generic User Accounts</u></p> <p>Generic User Accounts allow multiple users to use a single account to access the network, application</p> <p>There are 538 Mosaic accounts. 2 of these are Generic User accounts: UAT Administrator and CoreLogic.</p> <ul style="list-style-type: none"> • UAT Administrator – this account was last used March 2017 and has full 'demonstrator' access. The risk of this account being used was mitigate by a password change when the Mosaic system first went live, forcing individuals to log into the system as themselves. • CoreLogic – this account was last used June 2018. Management have stated that access to this account is controlled via the IT department and that they will be aware of any individual logging into the system using this account. The software supplier does need an account in order to provide support for the system and most councils provide this via a generic account. 	<p>If the Council do not assign unique user accounts to individual staff members then unauthorised activity may be performed and not identified, exposing the Council to financial, operational and reputational risk.</p>	<p>High</p>	<ul style="list-style-type: none"> a) We will disable and/or remove both the UAT Administrator and CoreLogic accounts. b) We will monitor user activity for generic accounts. c) We will update the user access process documentation to reflect third party access to the application. <p>Responsible officer: Business Systems Team Manager</p> <p>Target date: Completed.</p> <p>The UAT Admin and CoreLogic accounts have been closed.</p> <p>A new Servelec account has been set up; access to this will be granted and monitored by our IT department in the same way that they did for the CoreLogic account.</p>

Ref	Finding	Risks	Risk category	Agreed action
2.	<p><u>User Access Reviews</u></p> <p>It is good practice to perform formal, periodic reviews of user access. This control ensures that users have appropriate system access relevant to their job role.</p> <p>Although the Adults & Health (A&H) Business Systems team has a process and capability to conduct user access reviews, due to the stage of implementation, user access reviews have not been performed on a formal periodic basis. Instead, they have been performed on an ad-hoc basis, for example, when there have been numerous changes within a certain team.</p> <p>During our fieldwork we identified the following access issues:</p> <ul style="list-style-type: none"> • Leavers – 6/23 leavers between 01 January 2019 and 31 July 2019 still had their accounts on the application after their leaving the council. In addition, one leaver had accessed the application after their leave date. • Duplicate accounts – We identified 2 workers with duplicate accounts in the system 	<p>If periodic user account reviews are not performed, then inappropriate access levels may not be identified. This could result in inappropriate transactions not being identified/stopped, or lead to data breaches, exposing the Council to fines and reputational damage.</p> <p>Unauthorised transactions may be made if access is inappropriate. This can also increase the potential for fraudulent or erroneous activity on the application.</p>	Medium	<p>User Access Review</p> <ul style="list-style-type: none"> a) We will be formalising our user access reviews policy to be undertaken bi-annually and will include current accounts review including system admin and change developers. b) We will agree a turnaround time to resolve any discrepancies raised by the line managers during the review. <p>Leavers</p> <ul style="list-style-type: none"> c) In conjunction with the HR team, we will develop a process to ensure that the A&H Business Systems Team is informed on a timely basis of any staff that are leaving the Council. This could include a daily/weekly leaver's report that is sent to the A&H Business Systems Team on an automated basis for the IT team to action. Improvements will also be made as part of HR's SLAM (Starters, Leavers and Movers) project d) The 6 leavers identified will have their access removed.









Ref	Finding	Risks	Risk category	Agreed action
				<p>e) The 1 leaver, that was identified that had accessed their account after they had left, will be investigated as to how it was done and whether any unauthorised activity was performed by them.</p> <p>Duplicate workers</p> <p>f) We will review the potential duplicate workers and remove as appropriate.</p> <p>Responsible officer: Business Systems Team Manager</p> <p>Target date: Completed.</p> <p>Further work to improve notification of leavers will take place as part of the 'Starters, Leavers and Mover's (SLAM) Project as recommended.</p>
3.	<p><u>Change Developer Access to Production</u></p> <p>Some members of the IT team have 'Developer Access'. This allows the user to process changes to the application.</p> <p>These changes are usually developed and tested on a separate environment to the Production environment, with a clear distinction and separation between the environments. Developers should not have access to both the development and the production environments.</p>	<p>Unauthorised changes may be made. This can also increase the potential for fraudulent or erroneous activity on the application.</p>	Medium	<p>a) We will ensure that Developer's access to the production environment is limited to only when required. The change control process is clearly documented and will ensure that all changes go through the documented approval process before any changes are made to the system. The financial payments system is not our</p>

Ref	Finding	Risks	Risk category	Agreed action
	<p>Changes can currently be implemented by both the vendors (BetterGov and Capita) and/or the business systems team within Adults & Health and users with 'Developer Access' can access to both the development and production environments. This applies to vendors and business systems teams.</p>			<p>social care database but a corporate system. Mosaic acts as our case management system and changes on this is strictly through our change control boards.</p> <p>b) Management will review the controls in place to ensure that any unauthorised changes are in the production environment are found and investigated. For example generating a periodic report of all changes made to the Production environments and verify that all changes were approved. This report could be signed off by Assistant Director, Community and Performance</p> <p>Responsible officer: Business Systems Team Manager</p> <p>Target date: 31 March 2020</p>
4.	<p><u>New User Process – Disclosure & Barring Service (DBS) Checks</u></p> <p>A DBS check should be performed for all new system users. For Staff in Adult Social Care this is done as part of the recruitment 'on-boarding' process and is line management responsibility, however, other departments may require access (e.g. finance) and</p>	<p>Officers may have inappropriate access to sensitive information. This could result in financial and/or reputational risks materialising.</p>	Medium	<p>a) Business Support team will revise starter forms adding that a DBS check is needed. Checkboxes are only to be completed for non-A&H staff.</p> <p>b) The Business Systems Team will send reminders to the Line</p>

Ref	Finding	Risks	Risk category	Agreed action
	<p>DBS should be completed before they are given access to the system.</p> <p>We tested to confirm this had occurred for all new users and movers sampled. In 6/25 instances it was not clear whether a DBS check had been performed as the DBS 'tick box' had not been completed in the user form.</p> <p>Management have stated that after reviewing the 6 instances, that all the individuals had DBS checks completed and that the tick boxes on the form were not ticked</p>			<p>Managers that a DBS check must be conducted and confirmed when requesting new access.</p> <p>c) We will remove access or ensure checks are performed if they have not been completed.</p> <p>Responsible officer: Business Systems Team Manager</p> <p>Target date: 31 March 2020</p>

Appendix 1: Definition of risk categories and assurance levels in the Executive Summary

Note: the criteria should be treated as examples, not an exhaustive list. There may be other considerations based on context and auditor judgement.

Risk rating	
Critical 	Immediate and significant action required. A finding that could cause: <ul style="list-style-type: none"> Life threatening or multiple serious injuries or prolonged work place stress. Severe impact on morale & service performance (e.g. mass strike actions); or Critical impact on the reputation or brand of the organisation which could threaten its future viability. Intense political and media scrutiny (i.e. front-page headlines, TV). Possible criminal or high profile civil action against the Council, members or officers; or Cessation of core activities, strategies not consistent with government's agenda, trends show service is degraded. Failure of major projects, elected Members & Senior Directors are required to intervene; or Major financial loss, significant, material increase on project budget/cost. Statutory intervention triggered. Impact the whole Council. Critical breach in laws and regulations that could result in material fines or consequences.
High 	Action required promptly and to commence as soon as practicable where significant changes are necessary. A finding that could cause: <ul style="list-style-type: none"> Serious injuries or stressful experience requiring medical many workdays lost. Major impact on morale & performance of staff; or Significant impact on the reputation or brand of the organisation. Scrutiny required by external agencies, inspectorates, regulators etc. Unfavourable external media coverage. Noticeable impact on public opinion; or Significant disruption of core activities. Key targets missed, some services compromised. Management action required to overcome medium-term difficulties; or High financial loss, significant increase on project budget/cost. Service budgets exceeded. Significant breach in laws and regulations resulting in significant fines and consequences.
Medium 	A finding that could cause: <ul style="list-style-type: none"> Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale & performance of staff; or Moderate impact on the reputation or brand of the organisation. Scrutiny required by internal committees or internal audit to prevent escalation. Probable limited unfavourable media coverage; or Significant short-term disruption of non-core activities. Standing orders occasionally not complied with, or services do not fully meet needs. Service action will be required; or Medium financial loss, small increase on project budget/cost. Handled within the team. Moderate breach in laws and regulations resulting in fines and consequences.
Low 	A finding that could cause: <ul style="list-style-type: none"> Minor injuries or stress with no workdays lost or minimal medical treatment, no impact on staff morale; or Minor impact on the reputation of the organisation; or Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule; or Handled within normal day to day routines; or Minimal financial loss, minimal effect on project budget/cost.
Level of assurance	
Substantial 	There is a sound control environment with risks to key service objectives being reasonably managed. Any deficiencies identified are not cause for major concern. Recommendations will normally only be Advice and Best Practice.
Reasonable 	An adequate control framework is in place but there are weaknesses which may put some service objectives at risk. There are Medium priority recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any High recommendations would need to be mitigated by significant strengths elsewhere.
Limited 	There are a number of significant control weaknesses which could put the achievement of key service objectives at risk and result in error, fraud, loss or reputational damage. There are High recommendations indicating significant failings. Any Critical recommendations would need to be mitigated by significant strengths elsewhere.
No 	There are fundamental weaknesses in the control environment which jeopardise the achievement of key service objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.

Appendix 2 – Analysis of findings

Area	Critical		High		Medium		Low		Total
	D	OE	D	OE	D	OE	D	OE	
Access to the system, information and resources	-	-	-	-	3*		-	-	3
Enforcing appropriate segregation of duties	-	-	-	-	-	-	-	-	-
Management and monitoring of users	-	-	1*		-	-	-	-	1
Password Controls	-	-	-	-	-	-	-	-	-
Job Scheduling	-	-	-	-	-	-	-	-	-
Back-ups and Disaster Recovery	-	-	-	-	-	-	-	-	-
Change Management	-	-	-	-	-	-	-	-	-
Total	-	-	1		3		-	-	4

*Findings #1 and #2 relate to both Control Design and Operating Effectiveness issues.

Key:

- Control Design Issue (D) – There is no control in place or the design of the control in place is not sufficient to mitigate the potential risks in this area.
- Operating Effectiveness Issue (OE) – Control design is adequate, however the control is not operating as intended resulting in potential risks arising in this area.

Timetable					
Terms of reference agreed: 17/08/2019	Fieldwork commenced: 05/08/2019	Fieldwork completed: 18/09/2019	Draft report issued: 11/10/19	Management comments received: 23/12/19	Final report issued: 24/12/19

Appendix 3 – Identified controls

Area	Objective	Risks	Identified Controls
<p>Access to the system, information and resources</p>	<p>Access to information held within the application is managed and restricted to authorised individuals only. The number of high-risk users is kept to a minimum and their activities are periodically reviewed and monitored.</p>	<p>Individuals may gain access to unauthorised and/or sensitive information if:</p> <p>Access is granted to unauthorised staff to view and make inappropriate changes to the data.</p> <p>Access is not granted in line with the approved security policy and procedures.</p> <p>Access is not commensurate with their job role and/or no longer required to perform their job role.</p> <p>Access is not promptly removed when user access is no longer required.</p>	<p>A documented 'Creation and Maintenance of Mosaic Accounts Policy' document has been developed and is available.</p> <p>A 'User Request Form' and a 'Change in User Access Form' is available for line management to use to request for new or modify access for staff.</p> <p>A 'Leavers Form' is available to request for removal of user access for staff that are leaving the Council.</p> <p>The 'User Request Form' confirms if the user has undertaken a DBS check.</p> <p>It is an expectation that all users who have access to Mosaic have completed a DBS check. See Findings 1, 2 and 4.</p>
<p>Enforcing appropriate segregation of duties</p>	<p>There are sufficient segregation of duties in place for key job profiles (tasks).</p>	<p>There may be an increased risk of fraud and error where:</p> <ul style="list-style-type: none"> • Management have not identified all job profiles (tasks) that require segregation of duties. • Users have access to critical tasks, which should be segregated. • The system is not configured to 	<p>Only one primary role can be applied to each user within Mosaic.</p> <p>The role applied is based on a user's job role. The role can be supplemented with a secondary 'approver' role which will allow the user to approve weekly or one off amounts depending on their level within Adults and Health.</p> <p>A Segregation of Duties Matrix has been developed but is currently a work-in-progress.</p>

		<p>automatically enforce segregation of duties.</p> <ul style="list-style-type: none"> Weak password controls might result in unauthorised access and segregation of duties conflicts. 	
Management and monitoring of users	<p>Privilege users only perform tasks appropriate to their role. Inappropriate user activity is identified and investigated.</p>	<p>Unauthorised or inappropriate changes may be made without these activities being detected if:</p> <ul style="list-style-type: none"> Privilege user activity is not monitored to identify the performance of inappropriate tasks. There are inappropriate system and user logs maintained showing user activities which can be reviewed and where appropriate reported. User accountability cannot be easily determined during formal investigation. Logs can be turned off without formal approval and justification, which is appropriately evidenced. 	<p>Mosaic has an audit tool which allows management to review the 'footprint' of a user which can list the information a user has accessed, created, edited and/or deleted.</p> <p>There is a 'System Admin Tool' within the live and developer versions of Mosaic which allows those with access to change the privileges of users.</p>
Password Controls	<p>Ensure that the security of applications is maintained and prevents unauthorised access.</p>	<ul style="list-style-type: none"> User passwords may not be secure and could be at greater risk of being compromised or hacked if 	<p>Mosaic users use their Windows passwords to access the system and therefore no separate password is required for the Mosaic system.</p>

		<p>a robust user password policy is not in place and relevant management procedures are not implemented appropriately. This could lead to unauthorised access to systems:</p> <ul style="list-style-type: none"> • If system passwords which provide access to the database/data file are not restricted and follow strong password rules, the level of protection against unauthorised access will be reduced. 	<p>Passwords are governed by the Windows Group Policy:</p> <ul style="list-style-type: none"> - Max password age: does not expire - Min password age before it can be changed: 5 days - Minimum length: 14 characters - Passwords must meet complexity requirements and contain 3 of the following 4 categories: uppercase, lowercase, base 10 digits and non-alphabetic characters. <p>Customer and Support Group (support team by the vendor, Capita) run a script every week to disable Windows accounts that have not been accessed for 60 days.</p> <p>Accounts which have been disabled for six months are manually deleted from the directory.</p>
Job Scheduling	Inappropriate or unauthorised changes are made to the job scheduling or batch processing queues, which can result in delays for processing of payments and updating of data.	<ul style="list-style-type: none"> • The job schedule queue causes system disruption and outages due to failed updates. • The job schedule queue does not update all necessary interfacing systems • Failed job queues are not detected, reported and appropriately resolved. • Inappropriate or unauthorised changes are made to the queue. 	<p>Approvals and information from Mosaic is updated onto Integra (Finance System) each night.</p> <p>A weekly reconciliation is performed between Mosaic and Integra and sent to the Financial Affairs Team for review.</p> <p>An extract from Mosaic and Client Automated Billing System (CABS), is generated every week and sent to the Financial Affairs Team for review. It details the invoices which are outstanding and are to be included in billing cycles.</p>
Back-ups and Disaster Recovery	The Council is confident that data is backed up with an appropriate frequency in line with business needs, and	The Council may not be able to resume operational service within an agreed time period and recover sufficient data if	The Capita backup as a Service (BaaS) includes the standard backup cycle of daily incremental backups with a 30-day retention period.

	recoverable to ensure business continuity.	periodic testing is not carried out to confirm that data is backed up and recoverable as agreed with the business.	<p>All environments are also backed up weekly with a full backup.</p> <p>The process is documented within the High-Level Design document for Mosaic which has been signed off by the Council.</p> <p>Backup reports are reported to Operations Manager, CSG, on a daily basis by email.</p> <p>Disaster recovery policy is documented in a formal contract between Barnet Council and Capita, which also includes recovery times.</p> <p>Disaster recovery tests are completed on a quarterly basis by Capita.</p>
Change Management	Functionality changes/upgrades are applied to the application with appropriate oversight and governance mechanisms (such as testing approval, and post implementation review) prior to, during and after release.	Functionality changes/upgrades may be applied to the application, which are incompatible and/or the impacts not fully understood. This could disrupt the availability of the system for staff, thus hindering the ability to meet business objectives and compromising information security. This could arise if changes / upgrades are not logged, reviewed and approved at appropriate stages.	<p>Depending on the type of change the process is overseen by either Capita or BetterGov.</p> <p>Capita</p> <p>Capita oversee the Corporate IT Change Management Process which is used for large changes such as changes to infrastructure, upgrades, network changes, backups etc.</p> <p>There is a policy in place to describe the process (P0030 Change Management Policy & Procedure for the London Borough of Barnet). The process describes how requests for changes are to be raised, the change types, categories as well as roles and responsibilities in the process.</p> <p>Requests for Changes (RFC) are approved by:</p> <ul style="list-style-type: none"> - Change Manager or Change Assessor; and - Change Assessors <p>For changes classed as above 'minor' additional approval must be sought from:</p> <ul style="list-style-type: none"> - Technical Change Approval Board; and - Customer Change Approval Board <p>Environments for testing separate to the on the live system. There are separate test environments for Mosaic.</p>

			<p>BetterGov</p> <p>BetterGov oversee business/front-end changes (e.g. changes to forms within Mosaic to align to business processes).</p> <p>The documented 'Mosaic -Change Management Approach' describes the approach to be taken which describes different types of changes (major, BAU, regular or emergency'.</p> <p>All requests for changes are recorded on a Change Control Log document stored by the programme team.</p> <p>For a change to be implemented:</p> <ul style="list-style-type: none"> - A change document is produced which includes recommendations, the process to be adopted, reporting, critical success factors, training considerations, risks, summary of next steps, list of individuals who have been consulted, customer acceptance plan and any other information which is relevant. - The change is approved at the weekly Mosaic Change Board - The change is ratified at the monthly Mosaic Programme Board which is held monthly - Changes are developed in the testing/development environments. - SRO (Courtney Davis, Assistant Director Communities and Performance) approves the change. - The change is released as part of a wider change release cycle. <p>There is segregation of duties between the person who approves the change and the person who makes the change.</p> <p>Where considered as being required, training and awareness will be provided as well as other support (e.g. floor-walkers to be available on the day of release). See Finding 3.</p>
--	--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix 4 – Internal Audit roles and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken the review of *Mosaic Application Review*, subject to the limitations outlined below.

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Specifically we will not: Review the service management agreement between the Council and the performance of the Vendor (Better Gov) and other IT service providers.

Future periods

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.