Audit West

Final Internal Audit Report

Confidential

APF - Altair - IT System Access

September 2020

Executive Summary

Audit Opinion:

Assurance Rating	Opinion
Level 5 - Full Assurance	The systems of internal control are excellent with a number of strengths, no weaknesses have been identified and full assurance can be provided over all the areas detailed in the Assurance Summary.
Level 4 - Substantial Assurance	**The systems of internal control are good with a number of strengths evident and substantial assurance can be provided as detailed within the Assurance Summary.**
Level 3 - Reasonable Assurance	The systems of internal control are satisfactory and reasonable assurance can be provided. However, there are a number of areas detailed in the Assurance Summary which require improvement and specific recommendations are detailed in the Action Plan.
Level 2 - Limited Assurance	The systems of internal control are weak and only limited assurance can be provided over the areas detailed in the Assurance Summary. Prompt action is necessary to improve the current situation and reduce the levels of risk exposure.
Level 1 - No Assurance	The systems of internal control are poor, no assurance can be provided and there are fundamental weaknesses in the areas detailed in the Assurance Summary. Urgent action is necessary to reduce the high levels of risk exposure.

Assurance Summary:

Assessment	Key Control Objectives
Good	1. Internal Users – Avon Pension Fund staff have access to the system based on the concept of least privilege.
Satisfactory	2. Administrators – High level access is relevant and is effectively monitored to minimise the risk of abuse / error.
Satisfactory	3. External Users – Employers, Third Party Vendors and Scheme Members are only granted access to the system and data based on their individual or business needs and in compliance with data protection legislation, rules and regulations.

Detailed Report

Opinion

Internal Audit has undertaken a review of the access controls over the Avon Pension Fund (APF) Altair system. The framework of internal controls has been assessed and given an assurance rating of "**Substantial Assurance**". A total of 8 audit recommendations are detailed in the Action Plan.

Scope and Objectives

The scope and objectives of our audit were set out in the Audit Brief and a summary of our opinion against each of the specific areas reviewed has been detailed in the Assurance Summary section above.

Context & Audit Comment

The Avon Pension Fund (APF) is responsible for administering pensions in respect of 28,815 active members. Pensions for eligible staff are administered by 403 employers which include councils, government agencies and schools.

The APF uses the Altair application to provide pensions administration for local government pension schemes (LGPS) and a review of this area was part of the agreed Audit Plan for 2020-21. This piece of work reviewed access to the Altair system to ensure that it has been provided based on the concept of “least privilege”. More specifically, the audit reviewed the processes for:

- Creating and removing accounts.
- Password configuration policies.
- Controls over administrator level access.
- Third party access controls.

In order to gain access to Altair, and following management authorisation, users are set up and assigned levels of access appropriate to their roles by the Financial Systems Team. The levels of access assigned, along with any changes made within Altair are monitored and managed by the Financial Systems Team through a series of monthly monitoring tasks. LGPS Employers submit pension scheme data to Altair regularly using either the iConnect pay data submission platform or as a .csv file upload to the B&NES’ secure file transfer solution “Globalscape”. Employers can access their pension information through the Employer Self Service (ESS). Once an employer has been granted access to ESS and they log in with a username and password, ESS enables employers to view and amend (subject to the level of access granted by APF Employer services) their staff data held on the pension administration system. In addition, pension members can sign-up to the Member Self Service (MSS) and view their pension online, update details and use online pension planning tools.

This audit review focused on access to the Altair system, and findings include a lack of a formal access policy, weak password configurations and a limited record of monitoring/housekeeping checks performed. Furthermore, the importance of having an automatic lockout function enabled has been highlighted in respect of the increased emphasis on homeworking, following the outbreak of COVID-19.

We identified the following strengths

- There are documented registration and de-registration procedures in place for Altair.
- A monthly monitoring report is produced and reviewed to ensure users have appropriate levels of access to Altair.
- Altair users are forced to change their password before first use and on password reset requests.
- The Altair System Audit log is reviewed on a monthly basis.
- Temporary passwords are issued to Altair users securely via Council email.
- An up to date signed contract and non-disclosure agreement with the software vendor is in place to allow access to the network.

We identified the following weaknesses

- A periodic review of iConnect user access is not performed.
- iConnect user accounts do not automatically disable after periods of inactivity.
- The Altair Access Policy is in draft form only and it does not align with the guidance published in the Information Security Policy.
- A schedule of housekeeping tasks is not maintained, resulting in limited accountability or continuity for future checks.
- The Altair password configuration requirements are not aligned with the Council's Information Security Policy.
- The Council's Remote Working Policy document has been superseded and requires removing from the Intranet by Information Governance.
- The Altair application does not automatically lockout users after a period of inactivity.

The assurance rating given is: *'Level 4 – Substantial - The systems of internal control are good with a number of strengths evident and substantial assurance can be provided as detailed within the Assurance Summary'.*

However, a number of weaknesses were identified which would affect the control environment. More specifically, these are the recommendations relating to the Altair Access Policy and the liaison with the vendor to determine the feasibility of the inclusion of system updates in the next release. It is important that all recommendations are implemented by the agreed dates specified in the action plan to mitigate the risks identified.

Audit & Risk Personnel

Lead Auditor: Pat Jenkins.
Audit Manager, IT and Finance: Tariq Rahman.

Acknowledgements:

Sincere thanks to Geoff Cleak, John Hewlett, Matt Williams, Sean Smythe, Claire Newbery, Claire Moon and all service staff for all their help and assistance throughout the Audit Review.

Action Plan

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
M1	A periodic review of user access for the automated Employer pay-data submission system (iConnect) is not performed, and Employers are not monitored to determine whether user access is still appropriate. There may be iConnect users who either have inappropriate levels of access or who no longer require access.	Unauthorised or inappropriate levels of system access, leading to the risk of fraud through the manipulation of pay data.	iConnect user access should be reviewed on at least a quarterly basis to ensure user access to the system is still current and relevant. A record of these checks should be maintained. Employers should be reminded on at least a bi-annual basis to notify APF of any required changes to user access. A record of these checks should be retained.	**Agreed** **Responsible Officers:** Financial Systems & Development Manager, John Hewlett. Pensions Manager, Geoff Cleak. **Implementation Date:** 30th September 2020 The Financial Systems & Development Manager will liaise with the Avon Pension Fund to implement the audit recommendation. Standard paragraph now included in all periodic employer newsletters as a reminder to employers to notify APF of any authorised contact changes.
M2	iConnect user accounts do not automatically disable after periods of inactivity. Accounts remain active unless manual intervention is undertaken to disable the account.	Unauthorised system access and the risk of fraud through the manipulation of pay data e.g. a user may leave but they are still able to log in and submit pay data.	The Financial Systems Team should liaise with the software vendor and arrange for the iConnect application to be configured to automatically disable users after a pre-defined period of user inactivity. Also see M1 above.	**Agreed** **Responsible Officers:** Financial Systems & Development Manager, John Hewlett. Pensions Manager – Geoff Cleak **Implementation Date:** 1st September 2021

				The Financial Systems & Development Manager will liaise with the vendor to determine the feasibility of implementing the audit recommendation.

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer** **Management Comments** **Implementation Date**
M3	The Altair Access Policy is currently in draft form only and therefore it has not been circulated to users.	Existing users may not have been set up in-line with the policy. Users may have excessive access privileges. Potential for GDPR breach.	The draft Altair Access Control Policy should be finalised by the Financial Systems Team, reviewed and approved by the Systems and Development Manager and circulated to all users.	**Agreed** **Responsible Officer:** Financial Systems & Development Manager, John Hewlett. **Implementation Date:** 1st December 2020.
M4	The draft Altair Access Policy does not align with the guidance in the Council's Information Security Policy (InfoSec Policy) document.	Weaker access control is provided than the Council requires, resulting in an increased risk of system compromise.	The Altair Access Policy should align its guidance with the best practice outlined in the Council's InfoSec Policy, where appropriate, to ensure consistency across the authority. The access policy should also include the following elements: 1. Security requirements of the application. 2. Policies for information dissemination and authorisation. 3. Relevant legislation regarding protection of access to data and	**Agreed** **Responsible Officer:** Financial Systems & Development Manager, John Hewlett. **Implementation Date:** 1st December 2020.

MEDIUM RISK EXPOSURE				
	Weakness Found	Implication of Potential Risk	Recommendation(s)	Responsible Officer Management Comments Implementation Date
			services. 4. Standard user access profiles for common job roles in the Council. 5. Segregation of access controls. 6. Requirements for formal authorisation of access requests. 7. Removal of access rights.	
M5	Altair housekeeping & monitoring checks performed by the Financial Systems Team are not logged or recorded.	Lack of accountability for checks performed and inadequate continuity should the member of staff responsible be absent.	To ensure accountability and continuity, a central record of periodic system housekeeping checks should be developed and maintained by the Financial Systems & Project Lead.	**Agreed** **Responsible Officer:** Financial Systems & Development Manager, John Hewlett. **Implementation Date:** 1st December 2020. A new change control master spreadsheet is due to be implemented for all financial systems. The Financial Systems & Project Lead (MW) confirmed that this could additionally be utilised as a recording log for all system maintenance.

LOW RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer** **Management Comments** **Implementation Date**
L1	The password configuration parameters currently in use for Altair do not align with the password for life guidance outlined in the Council's InfoSec policy. The current Altair 'Minimum Password Strength' is set at 'Mild' with a minimum password length of 6 characters, which requires at least four of the below: - Lower Case Characters - Upper Case Characters - At Least One Numeric - At Least Two Numerics - At Least Three Numerics - At Least One Special Character - At Least Two Special Characters However, the Information Security Policy states: Use a minimum of **fifteen** characters with at least one character from three of the following four classes: • Lower case characters • Upper case characters • Numbers • Symbols	Risk of unauthorised system access through exploitation of a weak password configuration.	The Altair Password configuration policy should be updated by the Financial Systems Team to strengthen security and meet the Council's Info Sec Policy guidance. If the current password parameters cannot meet this guidance, then a change request should be raised with the software vendor.	**Agreed** **Responsible Officer:** Financial Systems & Development Manager, John Hewlett. **Implementation Date:** 1st December 2020.

LOW RISK EXPOSURE				
	Weakness Found	Implication of Potential Risk	Recommendation(s)	Responsible Officer Management Comments Implementation Date
L2	The Altair application which is accessed by Internal APF users does not auto-lock or require users to log back in after periods of inactivity. The lack of application automatic lockout is mitigated by an automatic lockout on Council machines.	With increased home and mobile working, there is a heightened risk of sensitive information being exposed (through unlocked computers, shoulder-surfing etc.) without an automatic lock-out enabled.	The Financial Systems Team should liaise with the software vendor and arrange for the Altair application to be configured to automatically lock after a reasonable period of user inactivity.	**Agreed** **Responsible Officer:** Financial Systems & Development Manager, John Hewlett. **Implementation Date:** 1st September 2021. The Financial Systems & Development Manager will liaise with the vendor to determine the feasibility of implementing the audit recommendation.
L3	The Council's Remote Working Policy is out of date and requires review. Due to COVID-19, 'working from home' has been upscaled dramatically by the Council. With the majority of the workforce now stationed predominantly at home or working remotely, the risks associated with the safeguarding of sensitive data are heightened, therefore it is important that an up-to-date remote working policy is in place.	A large proportion of the Council's workforce are stationed at home or remotely, including those with access to sensitive systems. There is an increased risk of loss or unauthorised access to sensitive data.	The Council's Remote Working Policy should be reviewed and updated by the Information Governance Team to strengthen the Council's defences against cyber risks and reflect homeworking on a larger scale.	**Agreed** **Responsible Officer:** Information Governance Manager, Sean Smythe **Implementation Date:** 1st December 2020. The Remote Working Policy has recently been absorbed into the Information Security Policy and more importantly the Acceptable Use Policy. The out of date Remote Working Policy will be removed from the Intranet.