Audit West

Final Internal Audit Report

Confidential

APF - System Access Controls

February 2023

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 (RAG) Summary

Key Control Objective:	Altair	ESS	MSS	i-Connect
1. Ensure that the level of system and data access granted to APF employees is commensurate with their roles.				
2. Ensure that APF employers, pension scheme members and third-party vendor access is based on the principle of least privilege and restricted.				
3. Ensure access is regularly reviewed and changes (joiners, movers and leavers) are actioned promptly.				
4. Ensure that the use of administrative (privileged) accounts is limited, restricted to authorised users only and subject to regular review.				
5. Ensure systems are monitored and logs are analysed for unauthorised access which may indicate abuse or a data breach.				
System Assurance Rating:	Level 4	Level 3	Level 3	Level 2

Detailed Report

Opinion

Internal Audit has undertaken a review of the risks and controls related to Avon Pension Fund (APF) - System Access Controls and assessed the framework of internal control at Level 2 – Limited Assurance. A total of 10 audit recommendations are detailed in the Action Plan.

The majority of the recommendations in this report concern i-Connect as a fundamental APF system. A total of two 'high' and six 'medium' recommendations have been made for i-Connect, placing it into the 'Weak' category for the key control objectives reviewed. A further 'high' recommendation has been made concerning employer data access for Employer Self Service (ESS), which is due to be replaced by i-Connect by the end of February 2023. As a result of this, the overall management of the risks facing APF system access has been assessed as 'Level 2 – Limited Assurance'.

Scope and Objectives

The scope and objectives of our audit were set out in the Audit Brief. This review covers the review of the four fundamental systems used by the APF, which were highlighted to Internal Audit by the Financial Systems & Development Manager. These systems are Altair, Employer Self Service (ESS), Member Self Service (MSS) and i-Connect, and a summary of our opinion against each of these is illustrated in the Assurance (RAG) Summary section above. The functions of the systems reviewed are summarised under the 'Audit Summary of Findings' section below.

Context & Audit Comment

As part of the B&NES 2022/23 Annual Audit Plan, Internal Audit has undertaken a review of the risks and controls related to Avon Pension Fund (APF) System Access. This review draws on the guidance issued by the Pension Regulator's 'Cyber Security Principles' as well as the National Cyber Security Centre (NCSC) 10 Steps guidance – Step 6, Identity and Access Management.

The Pensions Regulator outlines cyber security guidance, controls, and principles for pension schemes on its website, (thepensionsregulator.gov.uk). The website guidance states: "trustees and scheme managers are required by law to establish and operate adequate internal controls to ensure their scheme is operated in accordance with scheme rules and the law. The regulator may intervene where trustees and scheme managers fail in their duties to operate adequate internal controls".

To supplement the guidance published by the Pensions Regulator, it is important to reference that the National Cyber Security Centre recognises managing user privileges and user access control as essential control themes in both the '10 Steps' guidance and 'Cyber Essentials' accreditation scheme. Access Control refers to the process that ensures only authorised individuals have systems user accounts, and that those accounts have only as much access as they need to perform their role – known as 'the concept of least privilege'. Every active user account in the Avon Pension Fund facilitates access to devices, applications, and sensitive business information.

'Administrative accounts' are especially highly privileged. Such accounts typically allow:

• Execution of software that can make significant security changes to the system/application.

• Changes to the system/application for some or all users.

• Creation of new accounts and allocation of their privileges.

Compromise of administrative accounts can allow the exploitation of system privileges to facilitate large-scale corruption of information, disruption to business processes and unauthorised access to other devices in the organisation. For example, malware typically executes with the privilege level of the account that the user is currently operating. It follows that the allocation and use of privileged accounts should be closely controlled.

Large quantities of valuable sensitive data and personal assets can make pension schemes a desirable target for cyber criminals. Trustees and scheme managers should take steps to protect their members and assets against cyber risk. 'Cyber risk' is broadly defined as the risk of loss, disruption or damage to a pension scheme or its members as a result of the failure of its information technology (IT) systems and processes. It includes risks to information (data security) as well as assets, and both internal risks (e.g., from staff) and external risks (e.g., hacking).

The purpose of this Internal Audit review was to provide assurance to management over the risks and controls operating for APF systems to ensure that access to data is restricted to authorised users. A review of key control objectives was performed at a high-level, focusing on the allocation, restriction, review, and monitoring of system access.

Audit Summary of Findings

This audit review was predominantly undertaken by using an auditee self-assessment process. A questionnaire document was provided to staff with key responsibilities for APF systems to complete with details of the current arrangements and controls and provide attached supporting evidence where applicable. The explanations and evidence provided were then reviewed and further evidence or clarification was obtained where needed via additional discussions and meetings.

The systems reviewed during this audit are listed under the 'Assurance Summary' above with a Red/Amber/Green (RAG) rating to reflect the level of assurance provided for each risk area. In addition to this, a brief summary of each system, together with any significant findings, is provided below:

Summary of Systems Reviewed

Altair

Altair is the pensions administration software used, by the APF, to provide pensions administration for local government pension schemes (LGPS). Altair is a role-based system with full auditability ensuring users are only able to access the appropriate parts of the system to do their work. Altair was previously reviewed from a system-access perspective as part of 'Altair – User Access', (20-010B), with a subsequent follow-up where a 'Substantial' assurance rating was given.

Altair Member Self-Service (MSS)

MSS is a web-based portal for APF Pension Members. The portal requires members to sign in using a username and password to enable them to access read-only data, update set personal information, perform projection calculations, and trigger workflow cases. No MSS issues have been identified as part of this review.

Altair Employer Self-Service (ESS)

Employers can access their pension information through Altair 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. Employers are granted access to pensions data by the Employer Support Team, during the account setup phase via a simple checkbox, however, it was noted that Employer data access is not regularly reviewed or monitored. Internal Audit were notified during this review that ESS is at the end of its life as of 28th Feb 2023 and will not be part of APF systems going forward.

i-Connect

i-Connect is a platform which automates the submission of pension data. LGPS Employers submit pension scheme data to Altair regularly using either the i-Connect pay data submission platform or as a .csv file upload to the B&NES secure file transfer solution, Globalscape. As a result of this review, i-Connect has been assigned the lowest assurance rating, due to a number of fundamental system access control weaknesses. Unlike Altair, i-Connect does not have a dedicated systems officer or specialist team responsible for the IT system access controls. The lack of a dedicated systems role is understood to be a contributing factor to the risks and weaknesses identified in this review.

Additional systems (excluded from assurance summary)

Scan Client 4

A physical Windows 10 workstation, connected to the B&NES network, is set up in the Civic Centre office. This standalone machine acts as the Pensions scanner PC, using a scanning software called 'Scan Client 4' which interfaces directly with Altair and is also supported by Heywood Technologies. IT Services confirmed that user access is limited to a small number of users in the pensions team. Access requires users to log on to the B&NES network and enter their existing login details. Scanned documents are automatically uploaded into the Altair pensions system.

GlobalScape

Globalscape is a B&NES system and as such, has not been included within this audit review. However, as GlobalScape is a system that is used by APF staff in the context of sensitive data, it is important to note that under a recent audit review of 'COP14 Maintaining Contributions & Member Information' (21-024B), a recommendation was made regarding user recertification.

APF Data Centre (Physical Access)

The APF data centre is located in the server-room at the Guildhall, Bath. Internal Audit were informed by IT Services that this server room has restricted access to a small number of people in IT Desktop and the Infrastructure team, along with the Buildings Facilities Manager. The room is alarmed and is only accessible by ID swipe access and key.

We identified the following strengths

- Employer and third-party database amendments are logged as part of the overnight audit reporting process.
- Automatic locks, after periods of inactivity, are in place for Council-controlled machines.
- A network access protocol contract between B&NES and the software vendor, Heywood, is signed and in place.
- Reminders to update employer system access are published in a quarterly newsletter.
- User accounts are automatically disabled if there is no login activity within 30 days.
- Access to the Guildhall Server Room is restricted.
- Access to the Pensions scanning system is appropriately restricted.

We identified the following weaknesses

- Periodic review of i-Connect user access rights is not performed.
- I-Connect and ESS do not have policies regarding data access, protection (including encryption), use and transmission, in line with data protection legislation.
- An authorisation process and a record of all privileges allocated is not maintained for i-Connect, ESS and MSS.
- APF systems ESS and i-Connect do not have documented registration and de-registration procedures in place.
- i-Connect generated logs are not periodically reviewed to detect anomalies and suspicious activity.
- i-Connect users are not required to sign/agree to a statement confirming to keep passwords confidential.
- Late reporting of leavers by line managers are not being tracked and reported.
- Inactive i-Connect user accounts are not periodically monitored, reported, and disabled.
- User account naming conventions are not applied across all APF systems, increasing the risk of duplicate accounts.
- Employer Access to datasets (i-Connect & ESS) is not periodically monitored to identify instances of inappropriate data access.
- There are several generic user accounts for i-Connect that require evaluation.

Audit & Risk Personnel

Lead Auditor: Pat Jenkins

Acknowledgements:

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

Action Plan

HIGH RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
H1	**i-Connect User Account Naming** i-Connect user accounts do not follow a naming convention, increasing the risk of duplicate accounts. Internal Audit reviewed the user list provided and identified 12 instances of duplicate email addresses and four duplicate user names.	Duplicate accounts could lead to inappropriate data access.	Establish account naming conventions for i-Connect accounts. • Review the username & email address duplicates detected by Internal Audit • Review existing accounts against the convention. • Where appropriate, rename the accounts and update any linked descriptions.	**Agreed** **Responsible Officers:** **Senior Financial Systems Control & Development Officer, Cassi Gough** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** Existing generic names in the process of being changed. CG will convert all current accounts to new naming convention (in progress – 1st March) New users we will use first name surname naming convention. (In place). MW will add this to access policy for naming convention. (In place). Target completion date by 1st

				March.
H2	**i-Connect Generic User Accounts** There are various generic user names on the i-Connect user listing. Internal Audit were advised that generic user accounts were being phased-out, however, it is important that a review of generic accounts is performed swiftly, in line with the recommendation made under M2 - User Account Naming.	Generic logins, if shared or not linked to an individual, present a risk of non-accountability given that the ability to audit and monitor a specific user's actions is lost. When account sharing is commonplace, there is an increased risk of unauthorised use and data breach through the loss of Generic Login credentials.	Carry out a formal review of all generic i-Connect user accounts and ensure: • Access is appropriately restricted. • Credentials are securely issued and stored. • Use of Generic logins is recorded to maintain an accountability trail. • An individually identified owner is assigned who is responsible and accountable for the use of Generic logins. • Disable any generic accounts that should not be in use.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** Need for reviewing & monitoring seems clear User Generic accounts are being removed. (In progress – 1st March) Internal Generic accounts only used for testing internally by APF staff, to be added to user access policy. (In place). Target completion date by 1st March.

H3	**ESS/i-Connect - Employer Data Access** Employer access to datasets is not periodically monitored to identify potential instances of inappropriate data access. Access to relevant pensions data is granted to users by the Employer Support Team during the account setup phase via a simple checkbox. Periodic reviews of APF Employer data access are not performed. Without review, access to data that may have been inappropriately granted (checking the wrong box) may go undetected, leading to potential data breaches.	Access to pensions data that may have been inappropriately granted could go undetected, leading to data breaches. Potential for ICO action and fines	Implement a monitoring schedule to periodically review that the data access granted to employers is appropriate. Note: i-Connect will be used in place of ESS from mid-February 2023, however, this recommendation will still apply to i-Connect.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** Monthly housekeeping, new process to review user access to payroll and data. (In progress – 1st March) File to be stored in shared drive. Report now available in Insights reporting tool. To be written in a monthly schedule run by Financial Systems (FS). Immediate effect. Target completion date by 1st March.

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
M1	**i-Connect User access reviews** i-Connect application users are not subject to periodic review and reapproval.	Risk of unauthorised or inappropriate access, leading to compromise of sensitive data and leaving the system open to abuse	Establish a process to periodically review and re-approve i-Connect user access rights to verify that user access is appropriate for business needs. Users' access rights should be reviewed at regular intervals, e.g., annually.	**Agreed** **Responsible Officer:** **Senior Financial Systems Control & Development Officer, Cassi Gough** **Implementation Date: 01/03/2023** **Management Comments:** As per H3 above. Monthly and quarterly housekeeping checks. Target completion date by 1st March.
M2	**i-Connect Access Policies** i-Connect and ESS do not have system access policies. It is acknowledged that supplementary information is available via wider Council policy documentation, for example, the B&NES Acceptable Use Policy.	Users could be set up on APF systems with incorrect levels of access, compromising the protection of sensitive data. Higher level privileged user access may be granted without appropriate authorisations. Risk of system abuse and fraud with an elevated level of permissions.	The Financial Systems & Development Manager should ensure that system access policies are created for i-Connect and ESS. An overarching policy that covers all APF systems should be considered in order to streamline documentation. System access policies should include the following: • User access control procedures (for starters, leavers, and employment changes). • Password control (user responsibilities and system parameters). • Outline of system role profiles.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** Would be easy to replicate similar policy to Altair access policy but subject to the above recommendations being incorporated.

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
			Where relevant system access policies already exist, ensure that they are appropriately disseminated to staff. A record of staff, together with the date, and distribution list should be retained	FS to write systems access policy for APF (in place). MW has written report with Macros to ID users that have either not set up the account or not logged in for 3 months. (In place). Target completion date by 1st March.
M3	**i-Connect & ESS Registration & De-Registration Procedures** i-Connect and ESS do not have documented registration and de-registration procedures in place.	Incorrect user permissions could be applied on initial setup which could lead to inappropriate data access. System accounts could remain active after the user has left the Council, or their role, resulting in potential data breaches and ICO action.	The System Administrators for i-Connect and ESS should produce procedures for the creation of users, amending users' access rights, and deactivation of users. Ensure that the procedures include: 1. How users are created and deleted. 2. Assigning each User a unique user ID (to enable Users to be linked to and accountable for their actions). 3. Checks are undertaken to ensure that the level of access is appropriate for business purpose (It should not compromise segregation of duties). 4. Users are given a written statement of their access rights. 5. Users are required to sign statements indicating that they understand the conditions of access. 6. A formal record is maintained of all Users registered to user the system.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** ESS is end of life 28 Feb 2023. Being decommissioned early March by Heywood/BANESIT (in place). New user procedure to be written (MW/CM). Target completion date 1st March 2023 (in progress – 1st March) (1) (2) Detailed in Procedure Guide (in progress – 1st March)

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
			7. Immediately removing or blocking access rights of Users who have changed roles or jobs 8. Periodically checking for and removing or blocking redundant user IDs and accounts. 9. Ensuring that redundant User IDs are not issued to other Users.	(3) As part on new monthly housekeeping (in place). (4) Access policy to be distributed to existing users and all new users on sign up (in progress – 1st March) (5) Users must sign an end user licence on first log in (box tick) (in place). (6) Recorded in ERM and part of the monthly housekeeping (in place). (7) Reliant on employers advising us of changes and inactivity is monitored via disabling housekeeping (in place). (8) Monthly housekeeping (in place). (9) Record of usernames to be kept and checked. (in place).
M4	**i-Connect Inactive Users** Periodic checking for inactive i-Connect user IDs and accounts is not performed.	Exploit of inactive i-Connect user accounts in a cyber-attack.	Set up automated reports of i-Connect user accounts that are inactive for 30 days or more and disable the inactive accounts. A record of these checks should be retained.	**Agreed** **Responsible Officer:** **Senior Financial Systems Control & Development Officer, Cassi Gough** **Implementation Date: 01/03/2023** **Management Comments:** Report could be run & reviewed monthly. Policy to be set up to disable after 90

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
				days. 30 days is too short due to the nature of the work with monthly uploads. (In place).
M5	**i-Connect Review of System Logs** i-Connect generated logs are not periodically reviewed to detect anomalies and suspicious activity. Unsuccessful attempts should be reported and identify the time, terminal, logo and file or data element for which access was attempted.	Security issues, including attempts to exceed access authority or gain system access, for example, during unusual hours, may go undetected that could compromise the IT infrastructure.	Periodically review i-Connect system-generated logs to detect anomalies and suspicious activity. Unsuccessful access attempts should be reported and the time, terminal and file or data element for which access was attempted should be recorded. Note: The frequency of review of access reports should be commensurate with the sensitivity of the information being protected. Consideration should also be given to reviewing the frequency (for example on an annual basis) to ensure that it remains operationally relevant.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** i-Connect is a 3rd party cloud-based software, APF/FS do not have access to audit reporting within i-Connect. Unable to report on unsuccessful log ins etc. All updates to the Altair database via i-connect are recorded as part the nightly Altair audit and can be investigated if required on an individual member cases by case basis.

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
M6	**i-Connect, ESS and MSS Authorisation of 'Privileged' accounts** An authorisation process and a record of all privileges allocated to staff is not maintained for all the APF systems reviewed. Note: Access approval for privileged Altair user accounts was found to be appropriate, however, no assurance could be provided over the adequacy of privileged account approval for other APF systems.	There may be users with inappropriate privileged levels of user access without proper authorisation.	Implement an authorisation process that applies to all privileged system users across APF systems. Maintain a record of all users and their allocated privileges (this could be via a system-generated report). Ensure that: • Authorisations for special privileged access rights are reviewed regularly e.g., quarterly. • Privilege allocations are checked at regular intervals to ensure that unauthorised privileges have not been obtained. • Changes to privileged accounts are logged for periodic review.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** Regular review needed of access – this should be doable but need to ensure audit trail available. ESS is end of life 28 Feb 2023. Being decommissioned early March by Heywood/BANESIT (in place). Will review process for existing users and delete where appropriate. Process for new users for Admin Authority sign off needed. This will be Detailed in Procedure Guide, (in progress – 1st March)

MEDIUM RISK EXPOSURE				
	Weakness Found	**Implication of Potential Risk**	**Recommendation(s)**	**Responsible Officer Management Comments Implementation Date**
M7	**Track & Report Late Leaver Notifications** Line managers of APF system users have a responsibility to notify APF systems administrators of leavers, however, this is not always carried out in a timely manner. To mitigate the risk of past users remaining active on systems, there is a 30 day auto-disable in place, however, late notifications of leavers are not tracked and reported.	System users and employers may be left active or gain inappropriate access levels to systems or data.	Monitor inactive user accounts for follow up with line management. A record of all inactive user accounts should be retained.	**Agreed** **Responsible Officer:** **Financial Systems & Project Lead, Matt Williams** **Implementation Date: 01/03/2023** **Management Comments:** Financial Systems Team should be able to undertake this via information from iTrent A policy already exists to monitor existing user activity (in place). New automated report in place detail any APF staff leavers, runs every Monday. All APF leavers will now be picked up with 7 days of their leaving date. (In place).