Appendix 2

Corporate Audit Committee
Final Version Internal Audit Reports issued
Dec 2022 to June 2023 with Limited Assurance Rating

1. IT Avon Pension Fund System Access Controls

1.1 This review covered the four fundamental systems used by the APF, which were highlighted to Internal Audit by the Financial Systems & Development Manager - Altair, Employer Self Service (ESS), Member Self Service (MSS) and i-Connect.

1.2 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.

1.3 '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.:

- extend capacity and availability monitoring to include the corporate network
- analyse, and plan for, the availability and capacity implications of changing patterns of ICT service consumption and business changes

1.4 The 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.

1.5 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:

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**

1.6 In terms of a ‘red’ assessment against the Assurance Summary and individual systems additional detail is provided:

1.7 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**.

1.8 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 a contributing factor to the risks and weaknesses identified in the review.

Weaknesses

The Level 2 Assurance rating was assessed as appropriate based on the following 'High risk' weaknesses:

Weaknesses
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. **Implication:** Duplicate accounts could lead to inappropriate data access.
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. **Implications:** 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.
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.

Implications:

Access to pensions data that may have been inappropriately granted could go undetected, leading to data breaches.

Potential for ICO action and fines

This audit is to be followed-up in 2023/24 Q1/Q2. The three high-risk and seven medium-risk recommendations were agreed by management to be implemented.

2. Payroll (Service Based Review) – Timesheet Generated Payments

2.1 The purpose of this review was to provide management with an overall assessment on the control environment operating over timesheet generated payroll payments. The following key control objectives were reviewed and assessed as follows:

1) ensure that staff personal data is safeguarded in accordance with the data protection regulations – assessed as ‘Satisfactory’.

2) ensure that monthly timesheets (including overtime) completed by employees and to be processed, accurately record hours worked– assessed as ‘Satisfactory’.

3) ensure that timesheets are processed, resulting in accurate and timely payments and in compliance with Council policy – assessed as ‘Weak’.

2.2 Records across seven service areas / teams were examined to ensure compliance with the Council’s HR Policies and Financial Regulations.

The audit work carried out drilled into seven service areas:

1. Heritage Services
2. Waste – Midland Road depot
3. Recycling – Ashmead Road depot
4. Street Cleansing
5. Passenger Transport – Guide Escorts
6. PALS Cleaning
7. Parks & Trees / Operational Parks

2.3 The third control objective was assessed as ‘Weak’ as audit testing identified:

1) the failure of internal controls and checks to ensure the accuracy of payments for hours worked in Waste Services. Thirteen members had been overpaid for overtime worked and recovery action was required to recover the August 2022 total overpayments totalling £2,250. to control significant weaknesses with the It was identified that the payroll administration varied between service areas and the audit work identified weaknesses in procedures which had led to employees being incorrectly paid.

2) the failure to maintain adequate service procedure notes to guide staff, Reporting Managers and Proxy & Users.

3) Inappropriate proxy user system access rights – testing identified 4 users out of 22 were no longer carrying out proxy user duties.

4) Employees were not completing their own timesheets to claim pay. Reliance on supervisory staff to claim time worked by the employee.

5) the failure to reconcile accuracy of payroll proxy user input – supervisory internal controls.

2.4 Management responded positively to the audit report.

a) Waste Operations Management have advised that they have taken the necessary action to commence recovery of the wage overpayments and the adjustment to employee PAYE and NI contributions.

b) HR Operations Service have proposed a total system re-design. The Senior Auditor that carried out the audit has reviewed the proposed system and has concluded that the new system will effectively response to the 4 high risk, 4 medium risk and 2 low risk weaknesses. In terms of the two remaining weaknesses relating to the completion of GDPR training by those staff processing manual timesheets and insufficient checks to avoid duplication of timesheet payments – all services have responded that recommended actions have or will be taken.

2.5 This audit report will be followed up in Quarter 3 2023/24 to verify that management have taken the agreed actions.

3. Travel Perk – Travel Management System

3.1 Travel Perk is a Travel Management Services solution which gives users the freedom to book travel – air, rail, hotel accommodation, and car rental.

3.2 401 users were registered to use the system and in 2022/23 expenditure totalled £313,978.

3.3 The audit review has highlighted that limited assurance can be provided in terms of:

1. Effective contract management and monitoring arrangements.

2. Spend being compliant with Council travel policies.

3. Effective and accurate recharges to services.

3.4 Weaknesses included:

- There wasn't a dedicated lead contract management/ monitoring service/ officer identified within B&NES with the responsibility for overseeing the travel management services contract with Travel Perk.

- B&NES does not have an approved Travel Policy in place for bookings made via Travel Perk, which ensures that employees are aware of the 'rules' for how to book and expense compliant business travel.

- B&NES have not enabled the 'travel approval' functionality in Travel Perk, therefore, there is limited control over service spending.

- Formal processes are not in place to ensure that spend is periodically reviewed by service managers or subject to independent compliance reviews.

- Formal guidance has not been provided to the SA's which outlines their role, responsibilities and expectations as dedicated SA's. In addition, it is not clear what services/ teams the current SA's are allocated to/ responsible for.

- The current information and guidance available to Managers and users via the dedicated intranet page is considered limited and out of date.

- A formal process is not in place to assess eligibility criteria for access to the system, including approval requirements and the effective removal of leavers.

- The use of Travel Perk by Housing Service to spot purchase accommodation for clients as part of 'homelessness assistance' responsibilities may not be compliant with the purpose of the NEPO507 Framework.

3.5 The Director of People & Policy and Director One West, who manage the Human Resources & Organisational Development Service and Procurement & Commissioning Service respectively, have been asked to jointly consider the report and recommendations and provide a 'management response' to the audit report recommendations.