Pension Fund IT Security

North Yorkshire County Council

Internal Audit Report

Business Unit: Strategic Resources
Responsible Officer: Corporate Director of Strategic Resources
Service Manager: Head of Pensions Administration
Date Issued: 27 September 2022
Status: Final
Reference: 32270/002

	P1	P2	P3
Actions	**0**	**1**	**4**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

North Yorkshire County Council (NYCC) is the statutory administering authority for the North Yorkshire Pension Fund (NYPF), which is part of the Local Government Pension Scheme (LGPS). NYPF covers staff working for local authority employers, and other employers admitted by agreement, in the North Yorkshire area.

In April 2018, The Pensions Regulator published Cyber security principles for pension schemes ('the Principles'), highlighting the need for trustees and scheme managers to take steps to protect their members and assets from cyber risks given the large amounts of personal data and assets that they hold. Key areas covered by the Principles included IT governance, controls for physical and logical IT security, and incident response.

NYPF uses the Altair system for administration purposes, to calculate pension benefits, and to make payments to scheme members. The system and data are hosted by NYCC. There are also two associated systems: I-Connect, which allows employers to upload information, and Member Self-Service, an online portal for scheme members. These systems are also supported by NYCC, so it is important that NYPF has assured itself that NYCC has effective cyber security controls in place. The audit reviewed the controls for the Altair system, including any assurances provided by NYCC about its cyber security arrangements, using the Principles as a guide.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system ensure that:

- There are suitable governance arrangements in place regarding cyber security.
- Access to the Altair system and associated modules is suitably secured and managed.
- There are appropriate backup, recovery and incident management arrangements in place for the Altair system.
- The Altair system is kept secure through timely and effective application of updates and patches.

Key Findings

North Yorkshire Pension Fund (NYPF) has generally suitable cyber security arrangements in place that largely follow the guidance provided by the Pensions Regulator.

NYPF's providers of IT systems and services, Aquila Heywood and NYCC Technology & Change (NYCC T&C), adhere to several good practice standards for IT security: ISO 27001 Information Security Management, ISO 20000 IT Service Management (NYCC only), Cyber Essentials, and the Government's Public Services Network standard (PSN, NYCC only). However, it was noted that NYPF do not receive regular confirmation from NYCC T&C of their continuing adherence to these standards as part of their Service Level Agreement. Roles and responsibilities are defined in an SLA between NYPF and NYCC T&C and in the contract with Aquila Heywood.

All but one staff member (a recent transfer from another department) had completed mandatory training on information security and completion rates are monitored monthly by the Head of Pensions Administration (HPA). In March 2022, NYCC T&C implemented additional monthly training through the Boxphish learning platform. Most staff (65%) had completed at least 3 of the 4 training courses issued through Boxphish at the time of the audit, but the HPA does not currently receive completion reports to enable regular compliance monitoring. Committee and Board members are provided with training through the Hymans LGPS learning platform. NYCC T&C maintains a suite of policies governing access to and use of IT, which NYPF staff are required to comply with. Overall, governance arrangements are reasonable.

Access controls for the Altair system are reasonable. The current password settings for the system are reasonably strong, but it was noted that they no longer meet NYCC T&C's policy requirements following a change to the password policy in June 2022. Appropriate processes are in place for providing and revoking access for users and there are suitable controls over generic and third-party accounts. However, audit testing found that reviews of user roles and access rights are not undertaken periodically as recommended by the guidance. We also found that controls to prevent users from amending their own pension records had not been implemented for two users. Officers corrected this error during the audit, but periodically reviewing user roles and access rights may prevent this error from reoccurring in future.

Backup, recovery and incident management arrangements are generally satisfactory. Backups are taken regularly and monitored to confirm they are successful. They are stored for 30 days and replicated to NYCC's secondary site. Recovery testing is carried out periodically by NYCC Technology & Change on a range of systems, including Altair. The next recovery test is planned for September - October 2022 as part of a server replacement project. A summary of these arrangements is documented in the SLA, but the SLA does not require NYCC T&C to provide regular assurances over these arrangements to NYPF.

NYPF has business continuity and disaster recovery plans that cover most of the areas recommended by the Pensions Regulator's cyber security guidance. However, they do not cover external communications with stakeholders, plan testing or post-incident review. NYCC T&C maintains a comprehensive disaster recovery plan that is regularly tested.

Suitable processes are in place to ensure timely and effective application of updates to Altair. Heywood provide an update schedule for releases for the year ahead. Communication takes place between Heywood, NYPF and NYCC T&C to coordinate releases. Requests for change are logged and approved, with comprehensive testing of system functionality taking place before updates are deployed to the live system.

Overall Conclusions

A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 NYPF business continuity and disaster recovery plans

Issue/Control Weakness	Risk
NYPF's business continuity plan does not cover all areas recommended by the Pensions Regulator's cyber security guidance.	If NYPF's business continuity plan is incomplete or not kept up to date, incident response may be less effective or timely.

Findings

Our review of NYPF's business continuity (BCP) and disaster recovery (DR) plans found that they cover most areas recommended by The Pensions Regulator guidance. However, information on external communications, testing and post-incident reviews are not included. It was also noted that the BCP had not been properly reviewed since 2017.

The Pensions Regulator's cyber security guidance for incident response states that a plan should include: roles and responsibilities; critical functions and processes; a communications plan; and arrangements for notifying stakeholders (e.g. The Pensions Regulator or the Information Commissioner's Office) of an incident. Incident notification should cover the process, timescales and threshold for doing so. The plan should also cover a range of scenarios based on the scheme's functions, assets and likelihood of different types of incident. Incidents should also be documented and post-incident reviews carried out.

While key stakeholders are mentioned in the scenarios in the BCP, it does not specify the time limits, thresholds, process or contact details for external stakeholders such as the Pensions Regulator or Information Commissioner's Office.

A range of scenarios are covered in which the plans might be activated. However, the plans do not include a testing schedule or requirements for post-incident reviews. NYPF officers stated they planned to review the scenarios with NYCC Technology & Change (an action in NYPF's risk register), but this had not happened at the time of the audit. Carrying out this review and including ongoing requirements for testing and post-incident review may provide more resilience to NYPF's BC and DR plans.

Agreed Action 1.1

1. The BC and DR plans will be reviewed and updated to meet current Pensions Regulator standards. The BC plan will be updated to include arrangements for plan testing, post-incident reviews, and for contacting external stakeholders.

2. The plans will be reviewed annually, and this review will be included in the governance document review tracker.

Priority	2
Responsible Officer	Head of Pensions Administration
Timescale	31 March 2023

2 Assurances about contingency arrangements and good practice standards

Issue/Control Weakness	Risk
NYPF does not routinely receive assurances from its providers of IT systems and services of their continued conformance to good practice standards for cyber security as recommended by the Pensions Regulator's guidance on cyber security.	NYPF may not be assured that suitable cyber security arrangements are in place and continue to be maintained by Aquila Heywood and NYCC Technology & Change.

Findings

NYPF does not receive regular assurances from its IT providers (Aquila Heywood and NYCC T&C) that they continue to follow recognised good practice standards for IT security, meaning that NYPF may not be receiving the assurances it requires about cyber security. The Pensions Regulator guidance states that pension funds should assure themselves that suppliers adhere to good practice standards and that they may wish to ask for relevant accreditations and reports as evidence of adherence to standards.

In particular, NYPF does not receive ongoing assurances over two areas:

1. NYCC T&C's and Aquila Heywood's continued accreditation to recognised standards, such as ISO 27001 and 20000, Cyber Essentials and PSN.
2. NYCC T&C's backups and recovery testing arrangements for the Altair system and its BC & DR plans. Arrangements are summarised in the draft SLA, but NYCC T&C is not required to evidence that these are maintained and tested regularly.

Audit testing confirmed that NYCC T&C and Aquila Heywood are accredited to the standards noted above and that NYCC T&C have suitable backups and recovery testing arrangements for Altair and BC & DR plans. Therefore, NYPF is not exposed to significant risk, but periodically obtaining these assurances will provide NYPF with greater assurances about cyber security and help it to meet the Pensions Regulator's guidance.

Agreed Action 2.1

A programme of regular reporting will be agreed with NYCC T&C and documented in the Service Level Agreement. This will provide assurance that standards continue to be met and accreditation continues.

Priority	3
Responsible Officer	Head of Pensions Administration
Timescale	31 March 2023

3 Monitoring of Boxphish training completion rates

Issue/Control Weakness	Risk
NYPF does not currently receive Boxphish training records to enable monitoring of completion rates.	Lack of training or awareness of cyber security risks may increase the likelihood or impact of an incident.

Findings

In March 2022, NYCC T&C implemented additional monthly cyber security training through the Boxphish learning platform.

Most NYPF staff (65%) had completed at least 3 of the 4 training courses issued through Boxphish at the time of the audit, but 12 (35%) staff had not completed any of the courses. NYCC T&C Information Security team stated they monitor completion rates at their monthly security meetings. However, the Head of Pensions Administration does not receive reports to enable monitoring by NYPF and had not been notified by T&C of the completion rates noted above.

Providing the HPA with training records and documenting this in the SLA with NYCC T&C may provide NYPF with greater assurances about cyber security and help it meet the Pensions Regulator's guidance on cyber security.

Agreed Action 3.1

Quarterly reports will be requested from NYCC T&C from the Boxphish learning platform. These will be reviewed and monitored to ensure that staff complete training.

Priority	3
Responsible Officer	Head of Pensions Administration
Timescale	31 March 2023

4 Altair password settings

Issue/Control Weakness	Risk
Password settings for the Altair system are not in line with NYCC T&C's password policy.	Weaker password settings increase the risk of unauthorised users gaining access to the system.

Findings

Following a review in June 2022, the NYCC IT Access policy now requires that passwords meet the minimum standard of twelve characters long and a minimum of three types of character. The current settings for Altair passwords meet the requirement for types of character, but they do not meet the minimum length standard and therefore are not in line with NYCC policy.

Altair passwords are currently required to be changed every 2 months. This exceeds the requirement set out in the NYCC IT Access policy which requires passwords to be changed every 90 days.

Agreed Action 4.1

Password requirements within Altair will be reviewed and amended to ensure that they are in line with NYCC T&C's IT Access policy.	**Priority**	3
	Responsible Officer	Head of Pensions Administration
	Timescale	30 September 2022

5 User roles and access rights

Issue/Control Weakness	Risk
User accounts and user roles are not routinely reviewed to ensure they are appropriate and still required.	Users may have access that they no longer require or is inappropriate to their role.

Findings

The Pensions Regulator's guidance on cyber security recommends that user access to systems and data is regularly reviewed, but NYPF does not currently have a process in place for routinely reviewing Altair user accounts and roles. Two particular issues were noted in relation to user access and roles:

1. Altair users should have a National Insurance Number filter on their account to prevent them from making changes to their own or a family member's pension account. Audit testing found two system users did not have a National Insurance Number filter (these have now been added). Officers stated it was possible these were not available when the accounts were set up and they had not subsequently been added.

2. A range of Altair access roles are in place for staff with different job roles. Currently, a number of payroll staff have the 'Client' user role, which officers noted is intended for use by third party organisations, such as Heywood. There is a planned review of access level requirements for payroll staff to ensure that their roles are appropriate.

Currently, periodic reviews of user accounts and roles is not undertaken as is recommended by the Pension Regulator guidance.

Agreed Action 5.1

1. Quarterly reviews of user accounts and roles will be established to ensure user access and roles are at the appropriate level for all users.
2. The use of the 'Client' user role for payroll staff will be reviewed to ensure they have the appropriate user role. Roles will be amended as needed following the review.

Priority	3
Responsible Officer	Head of Pensions Administration
Timescale	30 September 2022

Audit Opinions and Priorities for Actions

Audit Opinions

Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit.

Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions

Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.