MAINTENANCE OF ICT CONTROLS

NORTH YORKSHIRE PENSION FUND (NYPF)

	Critical	Significant	Moderate	Opportunity
Findings	0	0	0	0
Overall audit opinion	Substantial Assurance			

INTERNAL AUDIT REPORT

Status: Final

Date issued: 14 August 2025

Responsible officer: Head of Pension Administration

INTRODUCTION

In a digital world, organisations face a growing number of cybersecurity threats as they rely on technology to store and manage data. Implementing robust security measures is essential to protect data, systems, and assets from unauthorized access, loss, misuse, and damage.

In response to this, as part of the General Code of Practice[1], The Pensions Regulator has set out expectations for trustees on the maintenance of IT systems (pages 113-117). In paragraph 5 the standards cover nine separate IT related areas including change management, disaster recover, data back up and additional cyber security controls. Paragraphs 8 and 9 of the Code have specific expectations on assessing and managing cyber security risk.

North Yorkshire Pension Fund IT infrastructure is managed by North Yorkshire Council. Their services encompass critical areas such as network and server management, as well as data and system security. The North Yorkshire Pension fund use the Altair pensions system to administer the pension fund, it is integrated with North Yorkshire Councils payroll and finance system.

OBJECTIVES AND SCOPE

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

- North Yorkshire Council is compliant with the controls set out in the maintenance of IT systems section within the Pensions Regulator code of practice
- North Yorkshire Pension Fund has robust business continuity plans in place.

[1] The Pensions Regulator: General Code of Practice.

KEY FINDINGS

We found the North Yorkshire Pension Fund (NYPF) has in place and fully complies with most of the IT controls as set out by The Pensions Regulator in the Code of Practice. An overview of our assessments made with the Code requirements is included in Annex One. NYPF has in place the necessary IT systems to help fulfil its statutory duties.

All changes to the Altair administration and payments system follow North Yorkshire Council's (NYC) formal change management process. This process includes advance notification to NYPF of any proposed changes, thorough testing, and obtaining approvals before changes are deployed into the live environment. A complete audit log is maintained for all change management activities.

NYC maintains an incident management plan and disaster recovery plan that covers NYPFs data and systems and contains high level roles and responsibilities of teams during an incident. This plan also covers all areas of the information security framework (per ISO 27001) and IT service management framework ISO 20000. We reviewed this area in greater detail as part of NYC IT Disaster Recovery work which reported in June 2025. One area for improvement was that the technology directorate have not yet implemented detailed plans of how they would respond to specific types of incident. Detailed incident response playbooks are being developed to support these plans, and actions have been agreed to have completed these, by 31 December 2025.

Incremental backups of NYPF data are taken every fifteen minutes, with full backups conducted every twenty-four hours. These backups are securely stored in two geographically distinct locations and are protected with access controls, encryption, and anti-malware technologies. As part of the work reported in June 2025, we saw the Council have tested back-ups of individual servers as part of ad-hoc tests and when there has been a business need for it. When completed these have been successful. However full-service backup testing has not yet been undertaken. Officers are putting in place actions that should help enable full-service backup testing to commence in 2026. A testing program will be implemented for those systems and services that are deemed business critical, which includes Altair. The Head of Pensions Administration has agreed to monitor and discuss progress with Technology officers to help ensure changes as planned are being made and enacted to Pensions systems.

NYC has a comprehensive suite of policies governing the maintenance, upgrading, and replacement of IT hardware. While The Pensions Regulator advises having specific policies for software replacement, no such dedicated policy is in place specifically for NYPF at this time. The need for such a policy at NYPF would appear limited given specific procurement and

other rules will be followed if/as the service considers the need to replace Altair.

Specialist IT staff from NYC provide support to NYPF, and the ICT network includes multiple layers of security controls to ensure ongoing protection. The pension fund's governing body is regularly updated on the evolving cyber threat landscape. Cybersecurity is a standing item on the pension fund's risk register and is reviewed frequently by the pension board. Network vulnerabilities are assessed throughout the year with internal and external audits carried out. Officers working with NYPF systems are required to adhere to NYC's IT acceptable use policy and must complete cybersecurity e-learning training every two years

OVERALL CONCLUSIONS

Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

Annex 1 -IT Controls

Standards for maintaining IT systems

Standards for maintaining IT systems:	Our assessment: Has the Control been met.
a. Cyber security measures and procedures should be in place and functioning. See Cyber controls.	Yes
b. Record evidence of how changes are planned and executed within the system.	Yes
c. Scheme and member data should be backed up regularly.	Yes
d. Disaster recovery processes are in place and tested over appropriate periods.	Partially: Test schedule to be implemented in the near future
e. Written policies should be in place for maintaining, upgrading, and replacing hardware and software.	Partially: Not in place for replacing software
f. Request evidence to show there is a schedule for the system to be replaced or updated, to cope with events such as changes to tax thresholds.	Yes
g. Be satisfied that adequate and sufficient hardware and personnel resources, with appropriate functionality and/or skills, exist to carry out the work.	Yes
h. Secure evidence that the IT system can meet current and anticipated system requirements.	Yes
i. Manage planned and potential future upgrades within the administration system.	Yes

Paragraph 5, TPR General Code of Practice p114

Assessing cyber risk

When assessing cyber risk governing bodies should:	
a. Ensure the governing body has knowledge and understanding of cyber risk.	Yes
b. Understand the need for confidentiality, integrity, and availability of the systems and services for processing personal data, and the personal data processed within them.	Yes
c. Have clearly defined roles and responsibilities to identify cyber risks and breaches, and to respond to cyber incidents.	Yes
d. Ensure cyber risk is on the risk register and regularly reviewed. See Internal controls.	Yes
e. Assess at appropriate intervals, the vulnerability of the scheme's key functions, systems, assets (including data assets) to a cyber incident, and the vulnerability of service providers involved in the running of the scheme.	Yes
f. Consider accessing specialist skills and expertise to understand and manage the risk.	Yes
g. Ensure appropriate system controls are in place and are up to date (eg firewalls, anti-virus, and anti-malware products).	Yes

Paragraph 8 p116 TPR General Code of Practice

Managing cyber risk

When managing cyber risk governing bodies should:	
a. Ensure critical systems and data are regularly backed up.	Yes
b. Have policies for the use of devices, and for home and mobile working.	Yes
c. Have policies and controls on data in line with data protection legislation (including access, protection, use, and transmission).	Yes
d. Take action so that policies and controls remain effective.	Yes
e. Have policies to assess whether breaches need to be reported to the Information Commissioner (https://www.ico.org.uk).	Yes
f. Maintain a cyber incident response plan in order to safely and swiftly resume operations. See Scheme continuity planning.	Yes
g. Satisfy themselves with service providers' controls. See Managing advisers and service providers.	Yes
h. Receive regular reports from staff and service providers on cyber risks and incidents.	Yes

Paragraph 9 p116 TPR General Code of Practice

Audit opinions

Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on four grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Finding ratings

Critical	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Significant	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Moderate	The system objectives are not exposed to significant risk, but the issue merits attention by management.
Opportunity	There is an opportunity for improvement in efficiency or outcomes but the system objectives are not exposed to risk.