Lancashire Local Pension Board
Meeting to be held on Tuesday, 17 October 2023

Electoral Division affected:
N/A;

Cyber Security Project - Update

Contact for further information:
Junaid Laly, Special Projects Pension Lead, 01772 532767,
Junaid.Laly2@lancashire.gov.uk

Brief Summary

The Pension Regulator published a draft of the new General Code of Practice in March 2021 which covers occupational, personal, and public service pension schemes. It provides draft guidance in relation to exercise of the functions under relevant pensions legislation and sets out draft standards, conducts and practice expected from those who exercise each function.

The Fund officer have reviewed the modules under the draft code and determined that the Cyber Controls module (ADM016) is a priority area within the new General Code. This report provides an update on the activity taken to date.

Recommendation

The Board is asked to consider and comment on the activity outlined in this report.

Detail

The Pensions Regulator published a draft of the General Code of Practice (GCoP) in March 2021, and it is intended that it will replace 10 of the existing codes of practice. The officers of the Fund undertook a gap analysis of the draft General Code of Practice to understand and identify areas which require attention once the final version of the General Code is published.

The findings of the gap analysis were presented to the Local Pension Board in July 2022. The gap analysis split the modules from the draft code into the following categories:

- New requirements with potential gaps
- Existing requirements which incorporate new guidance within the module
- Existing or New requirements with no gaps identified.

Following this analysis, the Officers have given the General Code modules a priority order and determined Cyber Controls module (ADM016) to be an area which should be prioritised as a new mandatory requirement with potential gaps.

Activity to date

July/August 2022

Aon, who are experts in the pensions sector offered all LGPS funds an opportunity to have their cyber controls assessed at a high level and provide a report in relation to cyber resilience. The questionnaire assessed the Fund against the following areas:

- Strategy, Governance and Documentation
- Pension Committee, Pension Board and Officers
- Fund Governance, technology, and procedures
- Administration (including pensioners' payroll)
- Other third-party providers
- Member Data
- Assets and Cashflows
- Dealing with pension fund members
- Incident response
- Financial input

After submitting responses to Aon, they provided a basic assessment report which showed the Fund score and a comparison against other LGPS Funds.

The results of the assessment indicated a need for further information on the third-party providers cyber controls.

December 2022

Following Aon's assessment, the Fund developed a Cyber Assurance questionnaire and sent it to Lancashire County Council Digital Services, Local Pensions Partnership Administration Limited, Local Pensions Partnership Investments Limited, Mercer and Northern Trust to assess their internal cyber controls.

The aim of this questionnaire was to gather information relating to provider assurance as the Pension Regulator's guidance states that we 'should assure ourselves that all third-party suppliers have put sufficient controls in place with regards to cyber security'.

Feb - April 2023

The responses to the Cyber Assurance questionnaire submitted by providers in December allowed the Fund to re-submit the scorecard to Aon which assessed the same 10 areas.

The results of this second submission showed scores with the Fund scoring above average in several areas where previously the score was below average (due to lack of information).

An annual report on Cyber Security was provided to the Board at its meeting on 24th January 2023 which provided useful background/context to this paper.

May 2023 - September 2023

Although there is a good level of officer knowledge surrounding the requirements specified in the Cyber Controls module of the General Code of Practice, due to the technical nature of Cyber Security the fund officers do not have the necessary level of knowledge to assess third party cyber controls. Therefore, it is deemed good practice to acquire specialist support to assist the Fund Officers in progressing with this project. This will also provide a level of external independent input to the assessment of third-party providers.

During this period Fund Officers developed an action plan using the second Aon assessment and identified actions to evolve towards complying with this module.

Following the development of the action plan, the Fund engaged with three industry specialists who are also experienced in the LGPS arena to identify what support is available in fulfilling these objectives and how their offering fits with the requirements of the Fund.

In addition, there was a workshop on cyber security for Board and Pension Fund Committee members in July 2023, a copy of which is in the online pensions library for Board members.

Next Steps

The following areas have been determined as actions to work towards being compliant with the Cyber Controls module of the General Code of Practice.

The Fund officers will be undertaking the activity with support from external consultants.

Activity	How	Output
Assessment of Providers		
• Gain understanding of service providers controls	• Cyber assessment questionnaire[1]	• Assurance of third-party providers cyber controls – Cyber report
• Data Mapping	• Identification of points for mapping and mapped process	• Clear mapped data flows for all stakeholders[2]

[1] This questionnaire asks providers to explain its approach to cyber security across five key cyber security functions. This will provide a risk score and highlights areas where responses indicate gaps in cyber resilience.
[2] This work would be prioritised to ensure key providers data flows are assessed first i.e., 1. LPPA as they hold membership data, 2. LCC as they hold fund financial and member information on Oracle/EPIC

• Action plan for providers compliance towards GCoP	• Create action plan for any areas of concern	• Improved cyber security compliance – Linked to Risk Register below
Risk Register		
• Fully assessed Risk with mitigations • Clear controls and actions • Assess the risk rating	• Review of Cyber Risk alongside report • Following assessment of providers controls and actions will be able to be documented. • Review and allocate appropriate risk rating considering Risk Management Framework	Robust Cyber Security risk on the Risk register with regular monitoring
Cyber Policy		
• Development of Cyber Policy • Assessment of Cyber Policy • Consideration of impact on other Fund policies e.g Breaches • Implementation and Engagement	• Write Fund specific Cyber Security Policy • Specialist review draft cyber policy • Review other fund policies to incorporate New Cyber Policy • Engagement with key stakeholders to approve and implement policy	• New Cyber Security Policy for the Fund • Updated fund policies if required. • Knowledge and understanding enhanced - all stakeholders understand their role and responsibilities, associated risks. ○ Fund policy published

Timescales for Delivery

Although the activity above has been determined to allow the Fund to work towards the Cyber Controls module, a definitive timescale for delivery will be dependent on the appointment of the cyber specialist. It is intended that the appointment of the specialist will be done in Q3 2023/24.

Feedback from industry specialists estimate the project should take approximately 12-18 months to complete. Though this varies according to the number of providers which need to be assessed.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

The treat of cyber-attacks is a growing, evolving and very real threat for organisations. The Lancashire County Pension Fund require regular updates from all stakeholders to ensure that the risk is being managed appropriately.

This supports compliance with the draft general code of practice requirements.

Local Government (Access to Information) Act 1985
List of Background Papers

Paper	Date	Contact/Tel
N/A	N/A	N/A

Reason for inclusion in Part II, if appropriate

N/A