TEESSIDE PENSION FUND

Administered by Middlesbrough Council

AGENDA ITEM 7

TEESSIDE PENSION BOARD REPORT

26 FEBRUARY 2024

DIRECTOR OF FINANCE – DEBBIE MIDDLETON

Update on Work Plan Items

1. PURPOSE OF THE REPORT

1.1 To present Members of the Teesside Pension Board (the Board) with information on items scheduled in the work plan for consideration at the current meeting.

2. RECOMMENDATION

2.1 That Board Members note this report and provide any comments or suggestions in relation the proposed work plan.

3. FINANCIAL IMPLICATIONS

3.1 There are no specific financial implications arising from this report.

4. BACKGROUND

4.1 At its meeting on 19 July 2021 the Board agreed an updated work plan for the coming months and years which set out areas for the Board to discuss or consider at subsequent meetings (see Appendix A). These were typically areas that the Pensions Regulator and/or the Scheme Advisory Board (SAB) had identified as important for Local Pension Boards to consider.

4.2 The two items scheduled for consideration in the work plan for this meeting are Internal controls and managing risks and the Fund's approach to cyber security, these are covered in the rest of this report.

5 INTERNAL CONTROLS AND MANAGING RISKS

5.1 The Pensions Regulator's recently published General Code of Practice gives the following very broad definition of Internal Controls:

"Internal controls refer to all the following:

- the arrangements and procedures to be followed in the administration and management of the scheme
- the systems and arrangements for monitoring that administration and management, and
- arrangements and procedures to be followed for the safe custody and security of the assets of the scheme."

This paper will focus on the Pension Fund's internal controls in relation to managing risks.

5.2 The Fund's Risk Management Policy (attached at Appendix B) details the risk management strategy for the Fund, including:

- The risk philosophy for the management of the Fund, and in particular attitudes to, and appetite for, risk.
- How risk management is implemented.
- Risk management responsibilities.
- The procedures that are adopted in the Fund's risk management process.
- The key internal controls operated by the Administering Authority and other parties responsible for the management of the Fund.

5.3 Effective risk management is an essential element of good governance in the LGPS. By identifying and managing risks through an effective policy and risk management strategy, the Fund can:

- Demonstrate best practice in governance.
- Improve financial management.
- Minimise the risk and effect of adverse conditions.
- Identify and maximise opportunities that might arise.
- Minimise threats.

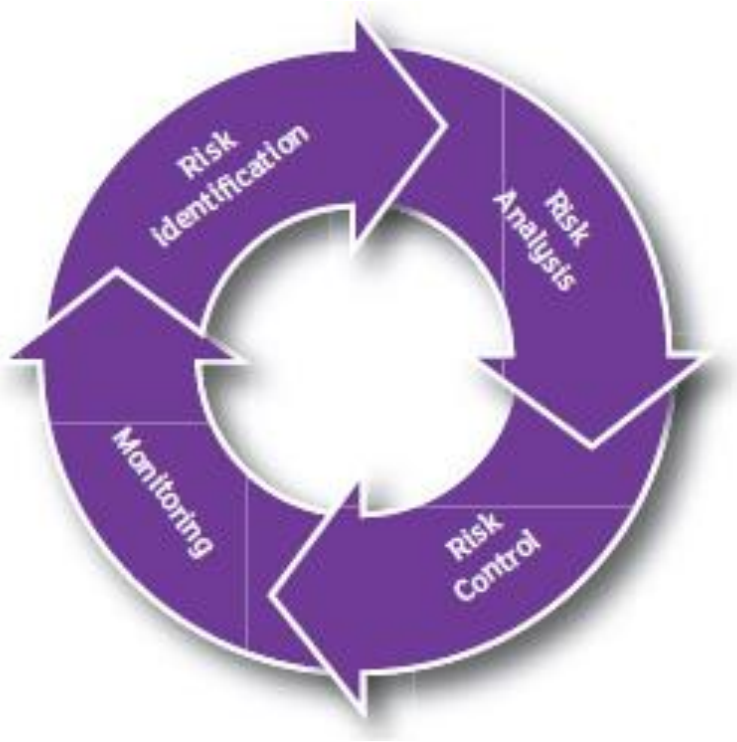
5.4 In relation to understanding and monitoring risk, the Administering Authority aims to:

- Integrate risk management into the culture and day-to-day activities of the Fund.
- Raise awareness of the need for risk management by all those connected with the management of the Fund (including advisers, employers and other partners).
- Anticipate and respond positively to change.
- Minimise the probability of negative outcomes for the Fund and its stakeholders.
- Establish and maintain a robust framework and procedures for identification, analysis, assessment and management of risk, and the reporting and recording of events, based on best practice.
- Ensure consistent application of the risk management methodology across all Fund activities, including projects and partnerships.

5.5 To assist in achieving these objectives in the management of the Fund, the Administering Authority will aim to comply with:

- The CIPFA Managing Risk publication.
- The Pensions Act 2004 and the Pensions Regulator's Codes of Practice as they relate to managing risk for public service pension schemes.

5.6 The Fund's risk management process is in line with that recommended by CIPFA and is a continuous approach which systematically looks at risks surrounding the Fund's past, present and future activities. The main processes involved in risk management are identified in the figure below and detailed in the following sections:



Risk Identification

The risk identification process is both a proactive and reactive one: looking forward i.e. horizon scanning for potential risks, and looking back, by learning lessons from reviewing how previous decisions and existing processes have manifested in risks to the organisation.

Risk Analysis

Once potential risks have been identified, the next stage of the process is to analyse and profile each risk. Risks will be assessed by considering the likelihood of the risk occurring and the impact if it does occur, with the score for likelihood multiplied by the score for impact to determine the current overall risk rating.

When considering the risk rating, the Administering Authority will have regard to the existing controls in place and these will be summarised on the risk register.

Risk Control

Risk control specifies actions taken to reduce the likelihood of a risk event happening, the frequency it could happen and reducing the impact if it does occur. Possible courses of action against risk:

- **Tolerate** – the exposure of a risk may be tolerable without any further action being taken; this is partially driven by the Administering Authority's risk 'appetite' in relation to the Pension Fund;
- **Treat** – action is taken to constrain the risk to an acceptable level;
- **Terminate** – some risks will only be treatable, or containable to acceptable levels, by terminating the activity;
- **Transfer** - for example, transferring the risk to another party either by insurance or through a contractual arrangement.

The Fund's risk register details all further action in relation to a risk and the owner for that action.

Risk Monitoring

Risk monitoring is the final part of the risk management cycle and is the responsibility of the Pension Fund Committee. In monitoring risk management activity, the Administering Authority / Committee considers whether:

- The risk controls taken achieved the desired outcomes
- The procedures adopted and information gathered for undertaking the risk assessment were appropriate
- Greater knowledge of the risk and potential outcomes would have improved the decision-making process in relation to that risk
- There are any lessons to be learned for the future assessment and management of risks.

Risk Reporting

Progress in managing risks will be monitored and recorded on the risk register. The risk register (see attached Appendix C), including any changes to the internal controls, will be provided at least annually to the Pension Fund Committee. The Pension Fund Committee will be provided with updates on a quarterly basis in relation to any changes to risks and any newly identified risks and a formal review will be carried out at least twice a year.

As a matter of course, the Teesside Pension Board will be provided with the same information as is provided to the Pension Fund Committee and they will be able to provide comment and input to the management of risks.

In order to identify whether the objectives of this policy are being met, the Administering Authority will review the delivery of the requirements of this Policy on an annual basis taking into consideration any feedback from the Teesside Pension Board.

The risks identified are of significant importance to the Pension Fund. Where a risk is identified that could be of significance to the Council it will be included in the Risk Register.

Risk Matrix

The risk matrix is adapted from the one used by the Council and the External Auditor's assessment of materiality (for the 2022/23 audit £50 million) is used the high value for the purposes of scoring the identified risks.

Likelihood	5	**Almost Certain >80%**	Low (5)	Medium (10)	Medium (15)	High (25)	High (35)
	4	**Likely 51% - 80%**	Low (4)	Low (8)	Medium (12)	High (20)	High (28)
	3	**Possible 21% - 50%**	Low (3)	Low (6)	Medium (9)	Medium (15)	High (21)
	2	**Unlikely 6- 20%**	Low (2)	Low (4)	Low (6)	Medium (10)	Medium (14)
	1	**Rare <6%**	Low (1)	Low (2)	Low (3)	Low (5)	Low (7)
			1	**2**	**3**	**5**	**7**
			Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**

6 CYBER SECURITY

6.1 The Fund is responsible for the personal data of over 80,000 scheme members, ongoing payments to almost 27,000 pensioners and maintaining secure financial records in relation to around £5 billion of assets. All the Fund's transactions are carried out electronically and all of its records are held electronically. This means cyber security – the security of those records, transactions and the systems that facilitate them – is of prime importance.

6.2 In maintaining secure systems and data, the Fund relies on the systems and processes the Council (as Administering Authority for the Fund) has in place, the security around some third-party systems (such as NatWest's Bankline) and also in the systems in processes maintained by its key partners such as XPS Pensions Administration ('XPS') our outsourced pensions administrator. Looking at each in turn:

6.3 <u>Council Cyber Security</u>

6.3.1 The Council's Information and Communication Technology (ICT) team has robust systems and procedures in place to ensure the Council's network is secure and that access to it is strictly controlled. Across the Council, staff are categorised according to the degree of contact they have with systems and data in the course of their daily work, and appropriate training is provided accordingly. For example, staff who have regular contact with personal data and/or management of staff and/or have access

to a broad range of network ICT applications are required to carry out advanced level data protection and cyber security training, and to have regular refresher training.

6.3.2 The Council has a robust business continuity plan, and each functional area is required to consider how it could continue to operate in the event of widespread network issue or unavailability.

6.3.3 The Fund has set up and maintains a business continuity plan setting out how it can continue to function in the event some or all of its systems became unavailable. The functionality relating to pension administration – the collection of contributions and the calculation and payment of benefits – is covered by XPS's business continuity plan. The remaining functionality, such as the requirement to continue maintaining the Fund's investments, making payments and receiving income appropriately is covered in the Fund's business continuity plan, which is reviewed and (if necessary) updated twice a year.

6.4 Third Party Systems Cyber Security

6.4.1 The Fund relies on a number of external third-party software systems to carry out essential functions. One of the most significant of these is the Bankline system provided by NatWest, the Council's and so the Fund's bank, which is used to facilitate payments to and from the Fund's account. These payments are both ongoing transactional payments, such as receipt of contributions and payment of benefits, as well as payments made and received in respect of the Fund's investments.

6.4.2 Bankline is a secure system which can only be accessed using the smartcards and card readers allocated to each user. The system is set up to allow further security to be applied by the organisation using it. This security has been utilised to ensure every payment from the Fund requires a different inputter and authoriser and every payment above £10 million requires an additional authoriser. Defined procedures have been set up and are followed in relation to payments, with a requirement for the inputter and authoriser to always check back to source documentation to verify amounts and account details. In addition, there is an audit trail built into the Bankline software which records the details of who makes any changes made to the details set up on the system and when those changes are made.

6.5 XPS Cyber Security

6.5.1 XPS has a comprehensive approach to cyber security and have achieved certification under information security management standard ISO27001. Their approach is summarised in the Information Security Summary document included in Appendix D, which covers:

- Information Governance and Risk Management
- Infrastructure & Application Security
- User Awareness & Phishing
- Malware Prevention

- Data Loss Prevention Controls
- Secure Configuration
- Access Control
- Home and Mobile Working
- Threat Intel & Monitoring, and
- Incident Management

6.5.2 XPS also has comprehensive business continuity plans in place, these are also summarised in Appendix D. XPS carefully control access to data, ensuring users only have access to the minimum level of data they require to carry out their role.

6.5.3 Also included within Appendix D is a copy of an Administration Update & Security presentation setting out some further aspects of XPS's approach to cyber security.

7. NEXT STEPS

7.1 Further updates on internal controls and managing risk and on cyber security will be provided to the Board as required or as scheduled in the Work Plan.

AUTHOR: Nick Orton (Head of Pensions Governance and Investments)

TEL NO: 01642 729024

Appendix A

Teesside Pension Board Work Plan		
Date of Board meeting and any standard items scheduled	**Suggested areas of focus (from the Pensions Regulator's list)**	**Suggested activities (including from the Scheme Advisory Board guidance)**
July 2021 Draft Report and Accounts		
November 2021 Annual Review of Board Training	Pension board conflict of interest	Review the arrangements for the training of Board members and those elected members and officers with delegated responsibilities for the management and administration of the Scheme
February 2022	Reporting breaches Maintaining contributions Reporting duties	Review procurements carried out by Fund
April 2022 Annual Board Report	Internal controls and managing risks	Review the complete and proper exercise of employer and administering authority discretions.
July 2022 Draft Report and Accounts	Record keeping Resolving internal disputes	Review performance and outcome statistics Review handling of any cases referred to Pensions Ombudsman
November 2022 Annual Review of Board Training	Regulator Code of Practice Gap Analysis	Review the outcome of actuarial reporting and valuations.
February 2023		Review the outcome of actuarial reporting and valuations.
April 2023 Annual Board Report	Communicating to members Publishing scheme information	Review standard employer and scheme member communications
September 2023 Annual Review of Board Training	Pension board conflict of interest	Review the arrangements for the training of Board members
November 2023 Draft Report and Accounts		
February 2024	Internal controls and managing risks	Review the Fund's approach to cyber security
April 2024 Annual Board Report	Pension Board statutory responsibilities	Pensions Dashboards
July 2024 Draft Report and Accounts		
November 2024 Annual Review of Board Training		Review the arrangements for the training of Board members and those elected members and officers with delegated responsibilities for the management and administration of the Scheme