CLWYD PENSION FUND COMMITTEE

Date of Meeting	Wednesday, 23rd March 2021
Report Subject	Business Continuity Policy
Report Author	Head of Clwyd Pension Fund

EXECUTIVE SUMMARY

Business Continuity

A robust approach to business continuity management is an important component of the Clwyd Pension Fund's risk management framework. The success of the existing business continuity arrangements was evidenced by the smooth move to remote working at the beginning of the COVID-19 pandemic. However, given the pandemic and the likely changes to working methods going forward, a review of the Fund's business continuity approach is taking place.

As part of that review a Business Continuity Policy has been developed which establishes the purpose, context, scope and governance of the Fund's approach to business continuity. The Committee are being asked to approve this Policy.

Further work is underway as part of this review of business continuity including:

- Carrying out a Business Impact Analysis
- Developing a Business Continuity Plan
- Identifying gaps and ongoing training needs
- Developing a Testing Schedule.

Cyber Security

The Fund has been carrying out some work in considering its resilience to cyber-attacks. This includes mapping of assets and data as well as asking two of its suppliers to provide further information on how they manage their cyber risk. This report provides a brief update on the work being carried out.

RECOMMENDATIONS	
1	The Committee review and approve the Business Continuity Policy for the Fund.
2	The Committee consider and provide comment on ongoing work in relation to business continuity and cyber security for the Fund.

REPORT DETAILS

1.00	**BUSINESS CONTINUITY AND CYBER-SECURITY DEVELOPMENTS**
	Business Continuity
1.01	Flintshire County Council, as Administering Authority for the Fund recognise that effective business continuity management is an essential element of good governance and risk management in the Local Government Pension Scheme (LGPS). It aims to ensure the Fund can continue to meet its legal and regulatory requirements and reduce operational (continuity-related) disruption risk to acceptable levels if the Fund were to experience a business continuity incident.
1.02	The Fund has carried out a number of tests in recent years to ensure services can continue to be maintained in various scenarios, such as an office fire. The success of the existing arrangements was evidenced by the smooth move to remote working at the beginning of the COVID-19 pandemic. Given the pandemic and the likely changes to working methods going forward, a review of the Fund's business continuity plans and processes is taking place.
1.03	The review of business continuity includes a number of key activities as set out in the roadmap in appendix 2. These include: • Business Continuity Management Policy (see appendix 1) • Strategic Business Impact Analysis (SBIA) – identifying the Fund's critical business processes (i.e. the fund services), the dependencies in place (in the areas of environment, supply, equipment and people) and associated recovery timeframes. It supports the development of appropriate business continuity solutions. • Recovery Time Objectives – identifying the period of time following an incident within which a service must be resumed, or resources must be recovered. • Risk Identification – this focusses on operational resources (dependencies) used principally, but not exclusively, to carry out business activities identified in the SBIA and any event incident or situation that could disable them. This will include identifying gaps where processes need documented or further training is required. • Recovery Strategies – determining the business continuity solutions that should be implemented and how they should be implemented in the event of an incident. • Business Continuity Plan – setting out details of what happens if there is an incident. This includes defining roles and responsibilities, the process to activate the Fund's response, how to manage the immediate consequences of an incident, prevent further loss, what the communications approach is, who are the key interested parties and emergency contacts, and how the Fund will continue or recover key activities within a predetermined timeframe. • Validation and Testing – Developing testing exercises to help identify issues and validate assumptions.

	A key requirement alongside all of this will be ensuring ongoing training is provided so all relevant parties understand the Fund's approach to business continuity. This work is included in the Fund's 2021/22 to 2023/24 Business Plan. Further updates on the progress in these areas will be brought to future Pension Fund Committee meetings.
1.04	The Business Continuity Policy (see appendix 1) is an integral part of this work that establishes the purpose, context, scope and governance of the Fund's business continuity management approach. The aim of the Policy is to: • provide strategic direction for the Fund's approach to business continuity management • define how the business continuity work of the Fund is structured, • set out the Fund's strategic objectives in this area • set out the role of the Pension Fund Committee and Pension Board to oversee this area, and • set out who the officer responsible for this area is and the officer(s) responsible for keeping the information up to date. The Committee are asked to consider and approve the draft Policy.
1.05	**Cyber Security** Another area that is very much aligned to business continuity is cyber risk. Cyber risk is considered a key risk to the Fund, as it is to most organisations nowadays. From a pension scheme perspective, cyber risk can be broadly defined as the risk of loss, disruption or damage to a scheme or its members as a result of the failure of its information technology systems and processes. It includes risks to information (data security) as well as assets, and both internal risks (e.g. from staff) and external risks (e.g. hacking).
	The Pensions Regulator (TPR) has issued guidance in this area for pension schemes. It highlights that pension schemes: • hold large amounts of personal data and assets which can make them a target for fraudsters and criminals and scheme managers need to take steps to protect scheme members and assets accordingly, which includes protecting them against the 'cyber risk'. • should take steps to build cyber resilience – the ability to assess and minimise the risk of a cyber incident occurring, but also to recover when an incident takes place. • should work with all relevant parties (including in-house functions, third party service providers and employers) to define the approach to managing this risk.
	Officers commenced work in this area last year and this continues to be included in the Fund's 2021/22 to 2023/24 Business Plan. Progress made to date includes engagement with two of the Fund's key suppliers to gather information relating to their cyber security controls so that the level of risk to the Fund can be assessed. Information is now being assessed and further clarifications obtained, and an overview of this will be provided as an exempt item to a future meeting.

	Fund officers have also been carrying out a mapping exercise to document and categorise the various interactions relating to data and assets. This in turn will help identify the key areas of risk that need investigation to ensure appropriate cyber resilience exists. Further updates will be provided to both the Committee and the Board on an ongoing basis, and training will also be provided in this area in due course.

2.00	**RESOURCE IMPLICATIONS**
2.01	Expert advice may be required in assessing the technical aspects of cyber risk on an ongoing basis but it is expected that this can be covered by the existing Fund budget.

3.00	**CONSULTATIONS REQUIRED / CARRIED OUT**
3.01	None directly as a result of this report.

4.00	**RISK MANAGEMENT**
4.01	Business continuity management is a core aspect of the Fund's risk management approach. The Business Continuity Policy and overall approach must align with the Fund's existing risk management processes.
4.02	Cyber risk is included as one of the key areas of risk within the Fund's risk register (risk 5 relating to the Fund's objectives/legal responsibilities are not met or are compromised due to external factors). The work outlined in this report is key in bringing this risk closer to target.

5.00	**APPENDICES**
5.01	Appendix 1 – Draft Business Continuity Policy Appendix 2 – Business Continuity Roadmap

6.00	**LIST OF ACCESSIBLE BACKGROUND DOCUMENTS**
6.01	No relevant background documents. **Contact Officer:** Philip Latham, Head of Clwyd Pension Fund **Telephone:** 01352 702264 **E-mail:** philip.latham@flintshire.gov.uk