SURREY COUNTY COUNCIL

LOCAL PENSION BOARD

DATE: **28 JULY 2023**

LEAD OFFICER: **ANNA D'ALESSANDRO, DIRECTOR OF CORPORATE FINANCE AND COMMERCIAL**

SUBJECT: **UPDATE ON CYBER SECURITY AND BUSINESS CONTINUITY**

SUMMARY OF ISSUE:

This report considers the review of Cyber Security work recently completed by the Surrey Pension Team.

RECOMMENDATIONS:

It is recommended that the Board **note** the content of this report.

REASON FOR RECOMMENDATIONS:

The Public Sector Pensions Act 2013 requires Local Pension Boards to assist the Scheme Manager in securing compliance with the Local Government Pension Scheme (LGPS) Regulations and requirements imposed by the Pensions Regulator. This report provides the Board with insight into the activities of the Surrey pension function and furthers the successful collaboration of the Committee and Board in managing risk and compliance and promoting effective governance.

DETAILS:

Introduction

1. The Local Pension Board previously received an update on 29 July 2022 following a light touch review on cyber security and business continuity arrangements in view of the escalating situation in Ukraine and the evolving geopolitical landscape.

Background

2. Following the above update, the decision to move the hosting of Altair to the software provider, Heywood was taken in late in 2022. At the same time, an end-to-end review of all cyber security activity was commissioned and conducted to ensure all issues across the Surrey Pension Team are considered collectively to implement necessary controls to be in place and develop suitable cyber security and business continuity approach.

3. The work entailed a full end-to-end review of cyber security arrangements of all third party providers who provide services to the Surrey Pension Fund (SPF) and with whom the Fund shares information. Cyber security policies or similar documents such as Security Policy/Privacy Notice that touch on cyber security were requested, obtained and reviewed to assess the adequacy.

Summary of information gathered and reviewed

4. The review identified at least 64 third-party providers which were classified into 3 categories – 34 Advisory providers, 23 providers (including Surrey County Council (SCC) as the Administering Authority) with whom the Fund information is shared for several reasons and the remaining 7 with no specific classification – See Annexe.

5. Although there are over 300 employers in the Fund, the arrangements within the 12 major employers in the Fund were used, for this review. This included SCC as the largest employer in the Fund and the 11 districts and boroughs in Surrey. Ongoing future work will include an annual review of a sample of other employers to ensure that their cyber security arrangements are adequate.

6. For the purposes of this review, arrangements in place for a sample of 6 major third parties was chosen and included CFH Docmail Limited, Eversheds-Sutherland, Heywood, Hymans Robertson, Mercer, and SCC. The findings are recorded below.

Detailed findings

7. From the information provided we noted that some organisations have detailed Cyber Security policies and provided either Privacy Notices or ISO 27001 Certificates as proof of their commitment to information security.

8. Achieving ISO 27001 certification by an organisation acts as a business differentiator, affirming to suppliers, stakeholders, and clients that the organisation takes information security management seriously. It demonstrates to other businesses that the organisation can be trusted to manage valuable third party information assets/data and intellectual property. It has implemented an Information Security Management System (ISMS) in line with Clause 4.4 of the standard to assure compliance to an external auditor or an independent ISO certification body such as UKAS, the National Accreditation Body for the UK.

9. Other certification bodies comparable to UKAS exist internationally, which helps maintain the ISO/IEC 27001 Information Security Management standard wherever an organisation aims to achieve ISO 27001 certification. ISO 27001 certification is not only about adequate technical measures in place but also about ensuring that the business controls and the management processes in place are adequate and proportionate for the information security threats and opportunities which have been risk assessed.

Selection of Major Third Parties

CFH Docmail Ltd

10. Version 8 of the Information Security Policy of CFH Docmail Limited was reviewed. The document created in March 2011 had been reviewed annually except in the years 2013, 2016 and 2019. The latest review was completed in August 2022 by the Group Head of QHSE & Compliance and the next review is due in August 2023. Two Certificates of Assurance dated 13 Jan 2022 and 1 Feb 2022 for Profile Versions Beacon and April 2020 respectively were provided by CyberSmart to confirm that CFH Docmail Ltd meets the Cyber Essential's implementation profile at the time of assessment. CFH Docmail Limited also holds the Certificate of Registration from the British Standards Institution (BSI) for their ISMS which affords them ISO/IEC 27001:2013 accreditation until 15 December 2023.

Eversheds-Sutherland

11. Eversheds-Sutherland is a global company which operates in several countries and serves numerous types of clients in various industries. Based on client requirements, the Privacy Notices available on their website is very detailed, comprehensive, and easy to follow. It outlines what the Privacy Notice is about, category, types and sources of personal data collected, who the personal data is shared with and the reason for doing so, where personal data is transferred to, how it is kept secure, for how long it is kept, the individual's privacy rights and how to exercise them etc. There are 2 tables which details the purposes for which personal data and special categories of personal data are processed.

Heywood

12. Heywood Pension Technologies provide the Altair software system from which the Surrey Pension Administration functions are conducted. Review of V2 of the document dated 18 February 2022 and titled 'Selected Policies and Procedures' (Commercial in Confidence) recorded that they hold ISO 27001: 2013 accreditation. The first edition (V1) was dated 16 February 2022 and subsequently revised 2 days later to include Disaster Recovery. The document contains Information Security Management Policy, Access Management Policy, Business Continuity Policy, Disaster Recovery Policy, and Data Protection Procedure. Each of these sections details sub-areas covered within these headings. It is understood that cyber security arrangements for Atmos used for mortality screening by SPF are managed by Heywood.

Hyman Robertson

13. Hymans Robertson LLP is the SPF's Actuary and provided a document titled "The Protection of Client Data Document" prepared by their Information Security Manager and updated in July 2022. The measures in place are described under the headings of Governance, Data Handling Processes and Procedures, Information Exchange Security, External Data and System Protection, ISMS (ISO/IEC 27001:2013 certified), Web, Internal Data and System Protection, Third Parties, Business Continuity, Staff Vetting, Training, Security Incident or Data Breach Reporting and Audits and Security Checks. They confirmed taking information security very seriously and have invested considerable time and money to ensure that data is handled safely and securely. They continue to seek improvements to processes and systems to prevent abuses.

Mercer

14. The SPF uses Mercer as one of their consultants for their investments. They are part of the global Marsh and McLennan Group and their confidential Information and Cyber Security Programme guide (last revised on 21 May 2020) details the arrangements in place in numerous sections to confirm that their policies and procedures are based on common cyber security frameworks and standards including, but not limited to, ISO/IEC:27001 and the NIST SP800-53 Risk Management Framework. They have a dedicated Chief Information Security Officer and outline the roles and responsibilities for staff and allow the Company to take disciplinary action for violation of the policies, up to and including termination of employment or contract for services. The Company also undertakes regular audits and risk and compliance assessments which are regularly shared with their external auditors as part of Sarbanes-Oxley S404 reviews. They implemented an Information Classification Policy in 2018 and continue to use it. Security of personnel, physical and environment, communications and operations management, network, access controls, incident management, disaster recovery etc. are also highlighted. However, the document was last revised on 21 May 2020.

Surrey County Council

15. The council continues to have a comprehensive IT Security policy and a Business Continuity Plan (BCP) which are regularly updated. The Fund draws on and uses the council's policies and BCP arrangements. The programme to align and embed systems, processes, and culture within the Surrey Pension Team (SPT) is ongoing. The aim is to enable the SPT to operate its pension related activities separate from the council operations while providing excellent and consistent customer service to all its customers and stakeholders to meet the SPT's Vision and Mission. This cyber security review of the various external organisations that support the operations of all the teams within SPT may allow the first steps in developing a specific cyber security policy and BCP for the SPF. This would clearly draw on and align with SCC best practice in this area.

Other large employers (SCC and Districts and Boroughs)

16. SCC is the largest employer in the SPF and the arrangements in place have been described in para 15 above. In addition, there are 11 districts and boroughs in the SPF and policies, or privacy notices were made available for 5 councils (Elmbridge BC (EBC), Epsom & Ewell BC (E&EBC), Guildford BC (GBC), Runnymede BC (RBC) and Waverley BC (WBC)) from their websites and reviewed.
    - EBC has a Data Protection Policy dated October 2020 and a Privacy Notice.
    - E&EBC has a Privacy Notice.
    - GBC has a brief statement on how the data obtained is used.
    - RBC has a detailed Privacy Policy which also includes a section on Privacy Notices for each Department within RBC and must be selected to view. It showed that Democratic Services, Information Governance and Legal Teams hold the same Privacy Notice on data.
    - WBC detailed their Privacy Notice and Data Protection in a single document.

17. Hard copies provided by 3 councils (Mole Valley DC (MVDC), Reigate & Banstead BC (RBBC) and Surrey Heath BC (SHBC)) were reviewed. They included Information Security Policies for MVDC (approved Version 7.0 of 22 Feb 2022) and SHBC (v2022) and the latter was pending review. RBBC provided a brief ICT Code of Practice document dated March 2021 and confirmed that they do not have a Cyber Security Policy.

18. Tandridge DC was unable to provide a policy but confirmed that it holds ISO 27001 accreditation, but a copy was not provided. Woking BC provided a link to their ICT Security Guidance (2020).

19. Information has not yet been received from Spelthorne BC.

Other Third- Party Providers

20. In addition to the third-party policies reviewed in paras from 10 to 14 above, documents for Cyber Security arrangements in place have been provided by ABRDN, Aztec, CEM Benchmarking, Darwin Property Investment Management, Deepstore, Glenmont Technology, ITM, Newton IM (BNY Mellon), Northern Trust, Pantheon and Pendragon. Links were made available to access other identified third parties. However, these were not selected for detailed review at this time.

Future work following this review

21. Further work is likely to include:

    a. Reviewing the arrangements in place for all employers and any other known stakeholders and/or third parties in the Fund.

    b. Reviewing all the contracts that are in place for pensions and ensuring adequate contract monitoring arrangements and business continuity plans are in place.

    c. Ensuring appropriate implementation of all of Surrey Pension Team's processes and workflows in a joined-up manner in the relevant systems (Altair, My Surrey, i-Connect, Pension Dashboard etc.).

Conclusion

22. A sample of arrangements in place have been covered in this report providing assurance in those areas reviewed.

23. Significant reliance is placed on third-party and other related stakeholders for cyber security arrangements. Consideration will be given to the development of a comprehensive SPT specific Cyber Security Policy and Business Continuity Plan which can be regularly reviewed and maintained.

CONSULTATION:

24. The Chair of the Local Pension Board has been consulted on this report.

RISK MANAGEMENT AND IMPLICATIONS:

25. Risk related issues have been discussed and are contained within the report.

FINANCIAL AND VALUE FOR MONEY IMPLICATIONS

26. The performance of the pensions function does present potential financial and value for money implications to the Pension Fund.

DIRECTOR OF FINANCE, CORPORATE AND COMMERCIAL COMMENTARY

27. The Director of Finance, Corporate and Commercial is satisfied that all material, financial and business issues, and possibility of risks have been considered and addressed.

LEGAL IMPLICATIONS – MONITORING OFFICER

28. There are no legal implications or legislative requirements.

EQUALITIES AND DIVERSITY

29. There are no equality or diversity issues to be addressed.

OTHER IMPLICATIONS

30. There are no other implications.

WHAT HAPPENS NEXT

31. The following next steps are planned:
Reports will be brought to the Local Pension Board as appropriate.

Contact Officers:

Siva Sanmugarajah	Risk & Compliance Manager
Paul Titcomb	Head of Accounting and Governance

Consulted:
Local Pension Board Chair

Sources/background papers:
Annexe – Third Party categorisation

Third Party categorisation

Third Party	Activity	Information Shared or Advisory
Surrey CC	Administering Authority	Shared
ABRDN	Asset Manager	-
AON	Actuary	Shared
Atmos	Mortality Screening	Shared
Barclays	Banking	Shared
Barnett Waddingham	Actuary	Shared
Black Rock	Investment Advisor	Shared
Border to Coast	Pooling Partner	Shared
Browne Jacobson	Legal Advice	Advisory
Byhiras	Software Provider	-
Capital Dynamics	Asset Manager	Advisory
Capita	Consulting	Advisory
CBRE	Asset Manager	Advisory
CEM Benchmarking UK Ltd	Information	Advisory
CFH Docmail	Software Provider	Shared
CIPFA	Professional Institute	Advisory
Club Vita	Data collection and analysis	Shared
Darwin Investments	Asset Manager	Advisory
Deepstore (microfiche)	Archive Data Storage	Shared
Digital Mail	Mailhouse	Shared
DWP	Advisor	Advisory
East Sussex Council	LGPS Fund	Advisory
EMAP	Information Service	Advisory
Equitable Life	AVC'S	Shared
Eversheds	Legal Advice	Shared
GAD	Reg's Information	Advisory
Glennmont	Asset Manager	Advisory
Goldmansachs	Asset Manager	Advisory
Gov Emails	External Provider	Shared
Grant Thornton	Auditor	Shared
Heywoods	Software Provider	Shared
HG Capital	Private Equity	Advisory
HSBC	Banking	Shared
Hymans Robertson	Actuary	Shared
IGA Talent Solutions Ltd	Resourcing	Advisory
ITM	Data Validator	-
Legal & General	Investment Manager	Advisory
Lincoln Pensions Ltd	Advisor	Advisory
Living Bridge (ISIS)	Asset Manager	Advisory
Local Government Association	Information/Guidance	Advisory
Mercer	Actuary/Administrator	-
Minerva Analytics Limited	Voting & RI Consultant	Advisory
MJ Hudson	Independent Investment Advisor	Advisory
Morgan Stanley liquidity funds	Investment Manager	Advisory
Office of National Statistics	Information	Advisory
Natwest	Banking	Shared
Newton Investment Management	Asset Manager	Advisory
NIDB - SYPA	Data Validator	Shared
Northern Trust	Custodian	Advisory
Oracle	Software Provider	-
Pantheon LTD	Private Equity	Advisory
Pensions & Lifetime Savings Association	Information	Advisory
Pentag	Reg's Information	Advisory
Perspective Publishing Limited	Asset Manager	Advisory
Phoenix Software	Software Provider	-
Prudential	Inhouse AVC'S	-
Redactive	Publishing Agency	Advisory
Restore	Record Management	Advisory
Squire Patton Boggs	Legal Advice	Advisory
Standard Life	Inhouse AVC'S	Shared
Tyne and Wear Pension Fund	LGPS Fund	Advisory
Utmost Life	Inhouse AVC'S	Shared
West Midlands Pension Fund	LGPS Fund	Advisory
Western Union	Overseas Payment Provider	Shared

This page is intentionally left blank