Purpose: For Noting

# Board Report

| | |
|---|---|
| Committee | **ISLE OF WIGHT LOCAL PENSION BOARD** |
| Date | **5 APRIL 2023** |
| Title | **CYBER SECURITY CONSIDERATIONS** |
| Report of | **PENSION FUND MANAGER** |

## EXECUTIVE SUMMARY


1. This report provides the local pension board with information about the key cyber security controls in place from its two major IT suppliers – Isle of Wight Council and Heywood Pension Technologies.

2. This initial high-level information is intended to provide the board with assurance that suitable controls are in place with both suppliers.

3. Further work will be required to develop fund-specific policies and processes for cyber security, which will be heavily reliant on the controls in place for these two suppliers.


## RECOMMENDATION

4. That the board notes the controls in place for both Isle of Wight Council and Heywood Pension Technologies.

5. That the board agrees the next steps in gaining further assurance in terms of cyber controls.

## BACKGROUND

6. At its meeting on 26 October 2022, the Local Pension Board considered the output of the Aon cyber risk assessment questionnaire which had been completed by the Pension Fund Manager.

7. At that meeting it was noted that the pension fund is primarily covered by the cyber security processes of Isle of Wight Council, as administering authority for the fund, and also places heavy reliance on the controls operated by Heywood Pension Technologies, the fund's administration software provider.

ISLE OF WIGHT COUNCIL

8. Information has been sought from Isle of Wight Council's Information and Communications Team (ICT), specifically the Strategic Manager – ICT and Digital Services, who is the council's nominated Senior Information Risk Owner (SIRO), and the Information Security Manager, who is also the deputy SIRO.

9. The Isle of Wight Council Information Security Policy was approved by the council's Information Security Group on 3 March 2023. The link to this published document is provided in the background papers section of this report.

10. This policy sets the standards expected in order to maintain the security of information within the council, and covers all aspects of security when handling, obtaining, recording, using, sharing and disclosing data or information, whether held in physical, electronic or verbal form.

11. Although the SIRO confirmed that council has not sought accreditation under ISO27001 (an international standard for information security management systems and their requirements), the policy states it is managed in line with the requirements of that standard.

12. The board may wish to consider whether the council's Information Security Policy covers the general principles identified within Cyber controls section of the Pension Regulator's draft new code of practice, which is included at Appendix 1 to this report.

13. Following that high level assessment, further analysis of some of the key provisions may be undertaken to confirm the board's understanding of their applicability to the pension fund.

14. The Information Security Manager has provided the council's Public Services Network (PSN) connection compliance certificate, covering the 12-months from 15 February 2023 to 15 February 2024, presented as Appendix 2 to this report.

15. According to the GOV.UK website (link provided in Background Papers section below), the PSN compliance process "exists to provide the PSN community with:

    (a) confidence the services they use over the network will work without problems.
    (b) assurance that their data is protected in accordance with suppliers' commitments.
    (c) the promise that if things do go wrong, they can be quickly put right."

16. The Information Security Manager has stated that the Council undertakes comprehensive penetration testing (simulated cyber-attacks on computer systems to check for exploitable vulnerabilities) annually and are required to remediate any issues found. The end result of such testing and corrective actions is assessed by the Cabinet Office and the certificate is issued to evidence Cabinet Office approval that the Council has proven that its network is secure enough to connect to central government networks via the public services network.

17. In due course, the board may wish to obtain further assurance from the council that the controls identified in the policy have been tested and are operating effectively. This may include consideration of the results of penetration testing, disaster recovery simulations and internal audit assurance reports. The council's Information Security Manager has agreed to attend a future board meeting to provide assurance on these matters if requested.

## HEYWOOD PENSION TECHNOLOGIES

18. Heywood Pension Technologies (HPT) were re-appointed as the fund's pension administration software provider in June 2022, for a ten-year contract starting on 1 January 2023.

19. HPT were asked to provide details of their information security protocols, including accreditation under ISO27001 or similar. Information was also sought about their business continuity and disaster recovery plans, and the results of the most recent penetration testing.

20. A copy of their summary response, including copies of the two certificates, is attached to this report at Appendix 3.

21. All documents referenced in that response (Business Continuity Policy, Business Continuity Plan, Disaster Recovery Policy and Cyber Security Review 2023) have been provided to the Pension Fund Manager. It is not deemed appropriate to publish these with this agenda pack, as they contain commercially and personally sensitive data to HPT. Copies of these documents can be provided to board members on request.

22. The executive summary of HPT's 2023 Cyber Security Review states there were no critical or high rated issues identified with their Cloud infrastructure, the servers used for that environment, or any of their product portfolio. The report further confirms that the small number of medium and low rated issues identified have been added to the security log for triage, prioritisation and remediation as appropriate. The next review is scheduled for January 2024.

23. The fund's client relationship manager from HPT has indicated that he and relevant colleagues would be happy to attend a briefing session for board members in due course to provide further assurance on their cyber security protocols.

## STRATEGIC CONTEXT

24. The primary objective of the fund is to provide pension and lump sum benefits for members on their retirement and/or benefits on death, before or after retirement, for their dependents, in accordance with the Local Government Pension Scheme (LGPS) regulations and statutory provisions. The committee aims to operate the fund in such a manner that, in normal market conditions, all accrued benefits are fully covered by the value of the fund's assets and that an appropriate level of contributions is agreed by the employer to meet the cost of future benefits accruing.

25. The understanding and monitoring of cyber security controls support the following agreed objectives:

    (a) Ensure compliance with the LGPS Regulations, other relevant legislation and the Pensions Regulator's Codes of Practice.

(b) Ensure Fund is managed, and its services provided, by people with the appropriate knowledge and understanding.
(c) Understand and monitor risk and compliance.
(d) Data is protected to ensure security and authorised use only.

## FINANCIAL / BUDGET IMPLICATIONS

26. The fund pays an annual license and maintenance fee to Heywood Pension Technologies for the supply of the pension administration software.

27. Through internal recharges, the fund incurs an annual service charge from the council's ICT department.

## APPENDICES ATTACHED

28. Appendix 1: extract from the Pension Regulators' draft new code of practice – Cyber controls.

29. Appendix 2: Isle of Wight Council PSN connection compliance certificate.

30. Appendix 3: Heywood Pension Technologies responses and certification.

## BACKGROUND PAPERS

31. Isle of Wight Local Pension Board 26 October 2022, item 8 Cyber Risk https://iow.moderngov.co.uk/documents/s9396/ITEM%208%20Cyber%20Risk%20Assessment.pdf

32. Isle of Wight Council Information Security Policy v5.2 – March 2023 https://www.iow.gov.uk/documentlibrary/download/information-security-policy1

33. Gov.uk guidance: Public Service Network (PSN) compliance https://www.gov.uk/guidance/public-services-network-psn-compliance

Contact Point: Joanna Thistlewood, Pension Fund Manager, ☎ 821000
e-mail *jo.thistlewood@iow.gov.uk*