Item 2(a)

22nd November 2023

Glasgow City Council

Strathclyde Pension Fund Committee

Report by Head of Audit and Inspection

Contact: Duncan Black Ext: 74053

INTERNAL AUDIT – Compliance with Cyber Security Principles

Purpose of Report:

To present the results of the Internal Audit review of the arrangements within the Strathclyde Pension Fund Office to ensure Compliance with Cyber Security Principles.

Note:

In most cases one of four opinions is expressed:

1. The control environment is satisfactory i.e. audit testing found no concerns with the control environment.
2. A reasonable level of assurance can be placed upon the control environment i.e. audit testing found no major weaknesses in the control environment but some improvements could be made.
3. A limited level of assurance can be placed upon the control environment i.e. improvements are necessary to ensure the control environment is fit for purpose.
4. The control environment is unsatisfactory i.e. significant improvements are required before any reliance can be placed upon the control environment.

Recommendations:

The Committee is asked to note the contents of this report and **AGREE** the audit recommendation that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the Action Plan.

Ward No(s): Citywide: ✓

Local member(s) advised: Yes ☐ No ☐ consulted: Yes ☐ No ☐

Glasgow City Council Internal Audit Section
Committee Summary
Strathclyde Pension Fund Office – Compliance with Cyber Security Principles

1 Introduction

1.1 As part of the agreed Internal Audit plan, we have carried out a review of the arrangements within the Strathclyde Pension Fund Office (SPFO) to ensure compliance with the Cyber Security Principles.

1.2 In April 2018, the Pensions Regulator issued its Cyber Security Principles for pension schemes as the large amounts of sensitive data held by pension funds could make them attractive targets for hackers and fraudsters. The Cyber Security Principles aim to provide good practice for pension funds to protect members against 'cyber risk'. The principles can be classed under the following categories: Governance; Risk Management; Access Controls; Incident Response and Training.

1.3 The SPFO is managed by Glasgow City Council (the Council). Consequently, the SPFO is governed by the corporate arrangements within the Council, including policies and procedures, risk management and the management and control of Information Computer Technology (ICT) infrastructure. Therefore, when assessing compliance with the Cyber Security Principles the relevant arrangements and controls in place for the Council as well as those specific to the SPFO were considered.

1.4 The purpose of the audit was to gain assurance that there are suitable arrangements within the SPFO to ensure compliance with the Cyber Security Principles. The scope of the audit included:

- Reviewing governance structures, roles, responsibilities, and accountabilities for cyber risk.
- Ensuring cyber risk is included in the SPFO risk register, that appropriate controls are in place to mitigate the likelihood and/or impact of cyber risk and that cyber risk is reported to the SPF Committee.
- Confirming that appropriate assurance is sought/received from the SPFO's partner organisations regarding cyber risk.
- Ensuring appropriate policies and procedures are in place, including a Cyber Incident Response Plan, and
- Ensuring sufficient training and awareness programmes are in place for relevant officers and Committee Members.

2 Audit Opinion

2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and four recommendations which management should address.

3 Main Findings

Governance

3.1 The Cyber Security Principles state that it is important for pension funds to have appropriate governance structures and for the roles and responsibilities regarding cyber security to be clearly defined, documented, and communicated.

3.2 The Council has sufficient governance arrangements in operation, including documented arrangements for ICT acceptable use, home working, use of passwords and data protection which apply to all staff members, including those within the SPFO. Corporate responsibilities for managing cyber and information security within the Council have been clearly defined within the documentation.

3.3 The Council has implemented a Security Operations Centre (SOC), provided by CGI (the Council's ICT supplier), which monitors the Council's network for unusual activity. SOC analysts provide 24/7 monitoring and alert the Council to potential security concerns, further supporting the existing governance arrangements.

3.4 However we found that the SPF Committee responsibilities in relation to risk (including cyber risk), although undertaken, have not been formally defined in the Terms of Reference.

Risk Management

3.5 The Cyber Security Principles state that those with pension fund responsibilities should ensure they have sufficient understanding of cyber risk and the potential impact of a cyber incident.

3.6 The Council's ICT Security Risk and Issues Forum (SRIF) has responsibility for managing corporate risks relating to cyber/information security for the full Council, including the SPFO. A separate SPFO Corporate Risk Register is maintained, and cyber/information security risks are currently captured within the register. These risks are scored, assigned a responsible officer, have mitigating actions, and are reported to the SPF Committee.

Access Controls

3.7 The Cyber Security Principles state that ICT infrastructure and security should be sufficient for the work undertaken and that physical and virtual access to systems and data should be controlled and monitored.

3.8 All systems used by the SPFO are managed by the Council's Strategic Information, Innovation and Technology (SIIT) team and CGI who have responsibility for the recovery and restoration of these systems. Access to Altair is restricted with permission levels which are reviewed and updated regularly. Independent penetration testing and vulnerability scanning, aimed at identifying gaps in information security compliance and protecting the Council's ICT network from unauthorised access, have been undertaken within the last twelve months. The Council has also implemented controls to restrict staff from accessing unauthorised web content.

3.9 The SPFO shares sensitive data with different partners through a range of data sharing portals. We found that adequate Data Sharing Agreements are in place which include the security measures for any SPFO data held.

Incident Response

3.10 The Cyber Security Principles state that pension funds should have systems and processes in place to ensure the safe and swift resumption of operations following an incident. Incidents should be documented, and major incidents should be followed by a post-incident review with plans being updated to consider lessons learnt.

3.11 The Council and CGI are responsible for the Cyber Incident Response Plan (CIRP) which covers the arrangements to restore Council systems in the event of a cyber incident, including those systems used by the SPFO.

3.12 The SPFO has its own Business Continuity Plan (BCP) which documents the processes to be followed if a significant and disruptive incident occurs to ensure that the critical functions of the SPFO can still be delivered. However, the current recovery actions for a loss of ICT could be more detailed. We also found that the SPFO has not conducted any exercises to test their BCP in the event of a cyber attack/incident.

3.13 A review of ICT network monitoring and testing arrangements (including the recovery and restoration of Council systems) and recovery testing of system backups are managed by the Council's SIIT team and CGI. Information in relation to these areas are regularly reported by CGI to the Council's Security Working Group (SWG) and Extended Information Security Board (EISB). Currently a representative from Financial Services (including the SPFO) attends the EISB and passes important updates to the SPFO management during the Financial Services Leadership Team meetings. However, we found that currently the SPFO is not provided with assurance demonstrating that the Altair servers are being appropriately backed up.

Training

3.14 The Cyber Security Principles state that those with pension fund responsibilities should receive regular training and have

access to the required skills and expertise to understand and monitor the risks from a cyber incident.

3.15 All SPFO employees are expected to annually complete the Council's mandatory online Information Security Essentials training course which provides guidance on password security, security of devices, email security, preventing cybercrime, handling sensitive information and data breaches. Our testing confirmed that SPFO employees comply with this requirement.

3.16 Information security training sessions are offered to all Elected Members. However, this has not been attended by all SPF Committee Members.

3.17 An action plan is provided at section four outlining our observations, risks and recommendations. We have made four recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	0
Medium	Less critically important controls absent, not being operated as designed or could be improved.	2
Low	Lower level controls absent, not being operated as designed or could be improved.	2

3.18 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.19 We would like to thank officers involved in this audit for their cooperation and assistance.

3.20 It is recommended that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Responsibilities for cyber risk have been clearly defined in the Terms of Reference for the SPF Committee.				
1	Risk responsibilities (including those in relation to cyber/information security risks) are not set out in the Terms of Reference (ToR) for the SPF Committee. This may result in cyber/information security risks and mitigating actions not being properly scrutinised.	SPFO management should update the ToR for the SPF Committee to ensure that the document reflects the members' risk responsibilities, including those relating to cyber security.	**Low**	**Response:** Accepted. SPFO management will update the ToR for Committee to ensure the document reflects risk responsibilities including cyber security. **Officer Responsible for Implementation:** SPFO Director **Timescales for Implementation:** 31 December 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Appropriate arrangements exist to protect the security of SPF data.				
2	Recovery testing of system backups is managed by the Council's SIIT team and CGI. However, we found that currently the SPFO is not provided with any assurances (for example reports) showing that Altair servers are being regularly backed up. This increases the risk that the SPFO management are unaware if the system would be recovered should an incident occur.	SPFO management should liaise with the Financial Services Business Partner to determine whether it is possible to obtain regular reports confirming successful backups of the Altair servers and any recovery tests that have been undertaken.	**Medium**	**Response:** Accepted. SPFO management will liaise with Financial Services Business Partner to determine whether it is possible to obtain reports confirming successful backups and any recovery tests that have been undertaken. **Officer Responsible for Implementation:** Principal Pensions Officer (Compliance) **Timescales for Implementation:** 31 December 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Appropriate incident response arrangements are in place.				
3	The Council is responsible for a Cyber Security Incident Response Plan which covers the arrangements to restore Council systems in the event of a cyber incident, including those systems used by the SPFO. The SPFO has its own BCP to be followed if a significant and disruptive incident occurs to ensure that the critical functions of the SPFO can still be delivered. The plan has entries for a loss of ICT for up to 7 days. However, the recovery task to be completed for a loss of ICT between 3-7 days is "continue to monitor timescales for return to business as usual". The BCP does not provide guidance for any other actions, for example communicating with members and employers to alert them that operations had been impacted and that calculations etc. could take longer than normal. We were advised that a new SPFO BCP is currently being developed as part of the wider Financial Services exercise. We also found that within the SPFO there are currently no exercises undertaken to routinely test the BCP in the event of a cyber attack/incident.	SPFO management should: • Ensure that the new SPFO BCP includes any possible additional actions required in an event of a long-term loss of ICT and is finalised in a timely manner. • Ensure that the BCP is tested on a regular basis. Lessons learned exercises should be carried out following tests or live events and action taken to address any issues identified as part of this process.	**Medium**	**Response:** Accepted. SPFO Management will ensure the new BCP includes actions required in the event of long-term loss of ICT and will also ensure the BCP is tested on a regular basis. Lessons learned exercises will be carried out following tests and action will be taken to address any issues identified. **Officer Responsible for Implementation:** Pension Scheme Manager **Timescales for Implementation:** 31 March 2024

No.	Observation and Risk	Recommendation	Priority	Management Response
	There is an increased risk that the SPFO's BCP is not fit for purpose and cyber and/or information security risks are not appropriately managed if a critical event were to take place.			

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: There is sufficient training and awareness on Cyber Security in place for relevant officers and Committee Members.				
4	Elected Members are trained on cyber security as part of the information security training drop-in sessions, however we found that this has not yet been attended by more than 50% of the SPF Committee Members. This increases the risk that the SPF Committee Members are not fully aware of the potential impact of cyber/information security risks on the SPFO.	SPFO management should liaise with the Council's Member Support Services to determine whether additional drop-in sessions could be offered to SPF Committee members and/or training materials could be issued to the members who were unable to attend the training.	**Low**	**Response:** Accepted. SPFO management will liaise with the Council's Member Support Services to determine whether additional drop-in sessions or training materials are available to elected members who did not attend the information security training. **Officer Responsible for Implementation:** Pension Scheme Manager **Timescales for Implementation:** 31 December 2023

Policy and Resource Implications

Resource Implications:

Financial:	Internal Audit services are included within the Central Support Services cost.
Legal:	None
Personnel:	None
Procurement:	None

Equality and Socio-Economic Impacts:

Does the proposal support the Council's Equality Outcomes 2021-25? Please specify.	No specific proposals are included within this report.
What are the potential equality impacts as a result of this report?	No significant impact.
Please highlight if the policy/proposal will help address socio-economic disadvantage.	There are no equality impacts as a result of this report.

Climate Impacts:

Does the proposal support any Climate Plan actions? Please specify:	Not Applicable
What are the potential climate impacts as a result of this proposal?	Not Applicable
Will the proposal contribute to Glasgow's net zero carbon target?	Not Applicable
Privacy and Data Protection Impacts:	None

5 Recommendation

5.1 The Committee is asked to note the contents of this report and **AGREE** the audit recommendation that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the Action Plan.