Internal Audit Report

Pension Fund Cyber Security Arrangements 2022/23

Final Report

Assignment Lead: Angus Rauch, Auditor
Assignment Manager: Mark Winton, Audit Manager
Prepared for: East Sussex County Council
Date: April 2023

Report Distribution List

Draft Report:
Sian Kunert, Head of Pensions
Michael Burton, Pensions Manager – Governance and Compliance
Paul Punter, Head of Pension Administration
Khy Perryman, Information and Security Governance Manager
Nicky Wilkins, Head of Engagement and Digital Innovation
Darren Stuart, Business Partner IT and Digital

Final Report, as draft with the inclusion of:
Ian Gutsell, Chief Finance Officer
Ros Parker, Chief Operating Officer
Matt Scott, Chief Digital Information Officer

This audit report is written for the officers named in the distribution list. If you would like to share it with anyone else, please consult the Chief Internal Auditor.

Chief Internal Auditor: Russell Banks, ☎ 07824362739, ✉ russell.banks@eastsussex.gov.uk
Audit Manager: Mark Winton, ☎ 07740517282, ✉ mark.winton@eastsussex.gov.uk
Anti-Fraud Hotline: ☎ 01273 481995, ✉confidentialreporting@eastsussex.gov.uk

1. Introduction

1.1. The pension regulators document, cyber security principles for pension schemes states that:

1.2. Pension schemes hold large amounts of personal data and assets which can make them a target for fraudsters and criminals. Trustees and scheme managers need to take steps to protect members and assets accordingly, which includes protecting them against the 'cyber risk'. This is an issue which all trustees and scheme managers, regardless of the size or structure of their scheme should be alert to.

1.3. The 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 (eg from staff) and external risks (eg hacking).

1.4. This review forms part of the agreed Internal Audit Plan for 2022/23.

1.5. This report has been issued on an exception basis whereby only weaknesses in the control environment have been highlighted within the detailed findings section of the report.

2. Scope

2.1. The objective of the audit was to provide assurance that East Sussex Pension Fund complies with the pension regulators cyber security principles for pension schemes. The principles provide guidance over the following areas;

- Governance;
- Controls;
- Incident response;
- Managing evolving risk.

2.2. It should be noted that the document 'Full draft of the new code of practice' contains a number of principles relating to Cyber controls. For the purposes of this audit we compared the principles within the new code of practice to those contained within the Cyber security principles for pension schemes[1]. Whilst broadly similar we have used the principles of the pension regulator rather than the new code as the basis of our assessment in this audit as the draft code had not yet been formally issued at the time of our audit.

2.3. Appendix B provides a summary of the principles we have used as the basis of our evaluation.

[1] Cyber security principles The Pensions Regulator | The Pensions Regulator

3. Audit Opinion

3.1. **Substantial Assurance is provided in respect of Pension Fund Cyber Security Arrangements 2022/23**. This opinion means that controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.

Appendix A provides a summary of the opinions and what they mean and sets out management responsibilities.

4. Basis of Opinion

4.1. We are able to provide an opinion of Substantial Assurance on the basis that, considering all the current cyber security measures in place for the Pension Fund, there is a high level of compliance with the principles set out by the Pension Regulator.

4.2. The controls that exist to manage a cyberattack for East Sussex County Council, apply equally to the pension fund. We also found there are adequate preparations in place to manage an incident, with support from the Information Security Team, should a cyber event occur.

4.3. Frequent backups online and to offline servers ensure that if an attack were to occur, members and the funds data would be backed up ready to continue service as soon as possible.

4.4. The measures around ensuring that staff have the correct knowledge to prevent an attack are sufficient, including phishing testing where the service is testing the employees to ensure that their knowledge is updated in line with emerging threats.

4.5. The council has overarching policies which cover the general use of technology and how to use them in a way which is not exposing the council to external breaches or even an employees compromised technology allowing entry into the systems, exposing them to an increased level of risk. The policies could be more pension specific and updated to ensure that emerging threats and updated technology is being covered.

4.6. Further, the Pension Fund could benefit from further pension specific controls which are in place to focus on the threats towards the fund and not just the wider council.

5. Action Summary

5.1. The table below summarises the actions that have been agreed together with the risk:

Risk	Definition	No	Ref
High	This is a major control weakness requiring attention.	0	
Medium	Existing procedures have a negative impact on internal control or the efficient use of resources.	0	
Low	This represents good practice; implementation is not fundamental to internal control.	1	1
	Total number of agreed actions	**1**	

5.2. Full details of the audit findings and agreed actions are contained in the detailed findings section below.

5.3. As part of our quarterly progress reports to Audit Committee we seek written confirmation from the service that all high priority actions due for implementation are complete. The progress of all (low, medium and high priority) agreed actions will be re-assessed by Internal Audit at the next audit review. Periodically we may also carry out random sample checks of all priority actions.

6. Acknowledgement

6.1. We would like to thank all staff that provided assistance during the course of this audit.

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
1	**Pension Fund Entity** We found that whilst there are generic Council wide policies, procedures and training in place to meet the expectations of the cyber security principles identified by The Pension Regulator, it is not always clear that these also apply to the Pension Fund. Whilst we have obtained assurances that the policies, procedures and training identified during the audit, (including an adequate response from Information Security should a cyber incident occur), do apply to the Pension Fund this could be made clearer.	There may be confusion over the extent to which policies, procedures and training apply to the Pension Fund.	Low	Members of the pension team to meet with IT&D colleagues to agree how to ensure council wide policies and training clearly apply to the pension fund officers and pension fund activities.
Responsible Officer:		Michael Burton, Pensions Manager – Governance and Compliance	**Target Implementation Date:**	July 2023

Appendix A

Audit Opinions and Definitions

Opinion	Definition
Substantial Assurance	Controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Reasonable Assurance	Most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Partial Assurance	There are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk.
Minimal Assurance	Controls are generally weak or non-existent, leaving the system open to the risk of significant error or fraud. There is a high risk to the ability of the system/service to meet its objectives.

Management Responsibilities

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

This report, and our work, should not be taken as a substitute for management's responsibilities for the application of sound business practices. We emphasise that it is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

Appendix B

Cyber Security Principles
Receive regular training and have access to the required skills and expertise to understand and manage the cyber risk.
The cyber risk should be included on your risk register and reviewed regularly (At least annually) and where there are substantial changes to scheme operations
You should assure yourselves that all third-party suppliers have put sufficient controls in place to protect your member data and scheme assets.
All organisations will experience security incidents at some point, even those with the most rigorous controls. As such you should ensure an incident response plan is put in place.
There should be a range of policies and processes in place around; Acceptable use of devices, email and internet (including social media), Use of password and other authentication. Home and mobile working/ Data access, protection, use and transmission, in line with data protection legislation and guidance.
Physical and virtual access should be controlled. Staff should be suitably vetted and have the right level of access for their role. Access should be regularly reviewed and closed down for any leavers
Good monitoring habits is essential in order to effectively response to incidents. Systems and networks should be monitored and logged analysed for any unusual activity or unauthorised access which could indicate an issue or threat.
All staff, and trustees, should receive training appropriate to their role at an appropriate frequency.
There should be systems and processes in place to ensure the safe and swift resumption of operations. This should include an incident response plan.
Critical systems and data should be regularly backed up. This should include, if appropriate, one or more offline back-ups, to stop these from being affected by a cyber incident. Processes to restore backed-up data should be tested.
IT infrastructure and security should be sufficient for the work undertaken. There should be multiple layers of security put around systems in line with the Information Commissioner's Office's (ICO) guidance on IT security.
The pension fund should assure themselves that all third-party suppliers have put sufficient controls in place to protect your member data and scheme assets. They should require suppliers to have, or adhere to, cyber security standards or good practice guides and monitor their performance. Cyber security should be an active consideration in the selection of a supplier and suitable provisions should be included in contracts.