

LPF PUBLIC DATA



## Appendix 1

# Internal Audit Report

## Lothian Pension Fund – Information Security Arrangements

22 February 2024

LPF2303

**Overall  
Assessment**

**Substantial  
Assurance**

# Contents

Executive Summary.....	3
Background and scope .....	4
Findings and Management Action Plan .....	5
Appendix 1 – Control Assessment and Assurance Definitions .....	9
Appendix 2 – List of IT Policies.....	10

This Internal Audit review is conducted by the City of Edinburgh Council for the Lothian Pension Fund under the auspices of the 2023/24 internal audit plan approved by the Pensions Committee in March 2023. The objective of this audit is to perform a high-level review of the relevant IT policies that have been published by the end of June 2023, and to provide a high-level assessment of the security improvements that have been put in place to address identified risks.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management’s responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the Lothian Pension Fund. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and members as appropriate.

## Overall opinion and summary of findings

There is a sound system of governance, risk management and control in place for the design and planned rollout of Lothian Pension Fund’s (LPF) IT policies.

The following areas for improvement were noted:

- development of an overarching Incident Management Policy to be used as a policy guideline in developing incident identification, response and reporting across the various systems/vendors. This would help to ensure a proactive and structured approach to the handling of IT and cyber incidents
- of the 39 policies in LPF’s policies roadmap tracker, 2 are still in draft and 9 have yet to be prepared.

## Areas of improved controls and good practice

- a comprehensive suite of IT security policies is in place and has been made available in a central location (SharePoint portal) so as to be easily accessed by employees
- the policies have been aligned with the [ISO27001 standards](#)
- LPF also has a cyber strategy plan (2023-2026) in place to improve the security and resilience of the IT systems
- there is a formalised risk management policy and risk management standard, and a risk log is in place which is reviewed on a weekly basis by the Head of IT
- there is a robust training programme in place that covers training on compliance with policies and phishing testing to help awareness of potential cyber-attacks.

## LPF overall management response

As described in the background section, a number of information security improvement activities have taken place in the last three years. Information Security remains a focus for LPF for the foreseeable future, and these recommendations will be incorporated into ongoing work.

## Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
IT Policies and Procedures			Finding 1 – Incident Management Policy	Medium Priority
			Finding 2 - Policies Rollout	Low Priority
			Finding 3 - Policies Version History	Advisory
IT Security Governance Framework			No findings noted	N/A
Training and Awareness			No findings noted	N/A

[See Appendix 1 for Control Assessment and Assurance Definitions](#)

# Background and scope

At the end of 2021, Lothian Pension Fund (LPF) was assessed against the [NIST \(National Institute of Standards and Technology\) Cybersecurity Framework](#), which provides a recognised set of standards, guidelines, and best practices to manage cybersecurity risk. The assessment concluded that whilst the LPF has several IT policies in place, some of these did not meet best practice. During 2022, LPF has focused on addressing identified gaps, with the IT team working to implement a full suite of policies, standards and procedures which set out on how information security will be managed.

LPF initially obtained [Cyber Essentials](#) certification in June 2022 and attained Cyber Essentials Plus in March 2023. The suite of information security policies was launched in June 2023. The policies follow the [ISO27001 framework](#), although no decision around attaining the certification itself has been made.

## LPF's current information security and information governance arrangements

Over the last 24 months, LPF have made material changes and improvements to their information security and information governance frameworks, including establishing new policies, procedures, and standards. Some of these improvements have just been launched and are not fully embedded.

These activities were a result of the procurement of a new technology managed service for LPF in 2021, and the move from the Council's IT provider (CGI) to Cased Dimensions. A number of assurance activities were carried out:

- August 2021 - Data Protection Impact Assessment on Cased Dimensions governance and security arrangements. Carried out by the Council's Information Governance Unit
- December 2021 – Cyber Security Maturity Assessment. Carried out by Bridewell (an independent cybersecurity consultant).

Two formal projects were established to address findings and recommendations arising from these assurance reviews – Information Security, and Information Governance. Both projects are now complete with any residual activities handed over to business as usual.

## Scope

The objective of this audit was to perform a high-level review of the relevant IT policies that have been published by the end of June 2023, and to provide a high-level assessment of the security improvements that have been put in place to address identified risks.

## Risks

The review also provided assurance in relation to the following LPF risk:

- Cybersecurity - inadequate cyber and data security arrangements to protect LPF from information security threats and cyber-attacks could prevent key operational processes from being undertaken and lead to financial losses and reputational damage.

## Limitations of Scope

The assessments outlined in the scope were reviewed at a point in time and are not intended to provide ongoing or retrospective assessment of the controls over a period. This audit did not consider third-party supplier policies as this was reviewed as part of the third-party supplier management audit completed separately as part of the 2022/23 internal audit plan.

## Reporting Date

Testing was undertaken between 1 November and 22 November 2023.

Our audit work concluded on 22 November 2023, and our findings and opinion are based on the conclusion of our work as at that date.

# Findings and Management Action Plan

Finding Rating	Medium Priority
----------------	-----------------

## Finding 1 – Incident Management Policy

LPF has a Security Incident Response policy for managing cyber security incidents. It defines the scope, key incident response team members, procedures for incident analysis, logging, categorisation and resolution, thereby enhancing the overall cyber security posture of LPF’s IT systems and data.

We also inspected an incident management handbook for Cased Dimensions (Managed Service provider). This handbook provides an outline of the incident reporting and resolution processes, change control processes, and contacts for escalations from Cased Dimensions.

However, there is no overarching incident management policy in place to be used as a guide for developing incident identification, response and reporting agreements with the suppliers who provide varying IT support to LPF. An overarching Incident Management policy will help ensure a proactive and structured approach to the handling of IT and cyber security incidents, thereby managing the risk of system failures or disruptions that may impact the organisation.

### Risks

- **Cybersecurity** - inadequate cyber and data security arrangements to protect LPF from information security threats and cyber-attacks could prevent key operational processes from being undertaken and lead to financial losses and reputational damage
- **Data Management** - mismanagement or poor maintenance and protection of data could lead to operational errors, regulatory breaches/fines, or reputational damage
- **Business Interruption** - significant and/or extended business interruption (including third-party suppliers) leading to a failure or inability to complete key LPF processes
- **IT systems** - LPF's IT does not meet operational requirements due to inadequate IT hardware or software leading to material or extended service delivery issues.

## Recommendations and Management Action Plan: Incident Management Policy

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officers	Timeframe
1.1	<p>Management should introduce an overarching incident management policy that serves as a baseline guideline in developing incident identification, response and reporting by IT service providers within baseline requirements of LPF. The policy may include, but is not limited to, the following elements:</p> <ul style="list-style-type: none"> <li>• <b>Objectives:</b> clearly defined objectives for the incident management process</li> </ul>	<p>LPF will create an overarching IT incident management policy, and communicate to staff. Where necessary, this will co-ordinate with, and refer to, existing policies and procedures on incident management and security incident response.</p>	Chief Executive Officer	Head of IT	31/12/2024

<ul style="list-style-type: none"> <li>• <b>Scope:</b> specifics on the systems, personnel, and types of incidents covered by the policy</li> <li>• <b>Roles and Responsibilities:</b> identification of key roles and responsibilities related to incident management</li> <li>• <b>Incident Identification:</b> procedures for recognising and reporting potential IT incidents</li> <li>• <b>Incident Categorisation:</b> criteria for classifying incidents based on severity and impact</li> <li>• <b>Initial Response:</b> actions to be taken immediately upon identifying an IT incident</li> <li>• <b>Resolution and Recovery:</b> steps for resolving the incident, restoring normal operations, and preventing recurrence</li> <li>• <b>Training and Awareness:</b> guidelines for educating personnel on incident management procedures.</li> </ul> <p>LPF should then ensure that the policy is communicated to all relevant staff, and there is a periodic review of the policy (at least annually).</p>				
--	--	--	--	--

## Finding 2 – Policies Rollout

Finding Rating	Low
----------------	-----

LPF maintains an IT policy roadmap tracker that comprehensively catalogues essential details pertaining to IT policies. This includes policy name, group categorisation, status (draft/not created/live), designated personnel responsible for delivery, individuals accountable for approval, target completion dates, and relevant comments.

At the time of our review, it was observed that there are 39 IT policies within management’s oversight. Among these, 28 policies have received approval and are operational, 2 are currently in draft status, while 9 policies have not been created. Among the 11 policies (2 in draft and 9 not created), a total of 9 policies have surpassed their designated target completion dates and therefore a delay has occurred in the rollout of these policies. Management have advised that this was primarily due to the staffing challenges and delays in the rollout of the Security Improvement Plan. Please [see Appendix 2](#) for a list of these 39 policies.

Delays in the rollout of policies may result in setbacks to achieving the cyber strategy plan objectives in a timely manner. Consequently, it may impede the overall objective of aligning the IT policies with the cyber strategy plan (2023-2026).

### Risks

- **Cybersecurity** - inadequate cyber and data security arrangements to protect LPF from information security threats and cyber-attacks could prevent key operational processes from being undertaken and lead to financial losses and reputational damage
- **Data Management** - mismanagement or poor maintenance and protection of data could lead to operational errors, regulatory breaches/fines, or reputational damage
- **Business Interruption** - significant and/or extended business interruption (including third party suppliers) leading to a failure or inability to complete key LPF processes.

### Recommendations and Management Action Plan: Policies Rollout

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officers	Timeframe
3.1	All relevant IT policies should be completed, approved, and implemented in a timely manner.  Additionally, a reassessment of the policy timelines and resource allocation should be considered to ensure timely alignment of the IT policies with the established cyber strategy plan.	LPF will identify a defined list of remaining IT policies to be completed, and a timeframe for completing them. This timeline will be reviewed and approved by the IT Oversight Group, and progress on completion of these policy reported to ITOCG.	Chief Executive Officer	Head of IT	31/03/2025

## Finding 3 – Policies Version History





Following our review of the IT policies, we noted some further improvement opportunities:

- full name (rather than initials) to be provided for individuals responsible for amending and approving the policies
- job titles to be included for individuals amending and approving the policies
- policy owner details to be provided in case of any queries.

<b>Finding Rating</b>	<b>Advisory</b>
---------------------------	-----------------



# Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed		Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory		Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity		Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity		Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	N/A	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Overall Assurance Ratings	
<b>Substantial Assurance</b>	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
<b>Reasonable Assurance</b>	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
<b>Limited Assurance</b>	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
<b>No Assurance</b>	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Finding Priority Ratings	
<b>Advisory</b>	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
<b>Low Priority</b>	An issue that results in a small impact to the achievement of objectives in the area audited.
<b>Medium Priority</b>	An issue that results in a moderate impact to the achievement of objectives in the area audited.
<b>High Priority</b>	An issue that results in a severe impact to the achievement of objectives in the area audited.
<b>Critical Priority</b>	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

## Appendix 2 – List of IT Policies

	Policy Name	Group	Status
1	Asset Management Standard	Information Security	Live
2	Backup Policy	Information Security	Live
3	Bring Your Own Device (BYOD) Policy	Information Security	Live
4	Call Recording Policy	Information Security	Live
5	Change Management Policy - Non-MSP	Information Security	Live
6	Cryptography Policy	Information Security	Live
7	Data Classification and Handling Standard	Information Security	Live
8	Information Security Policy	Information Security	Live
9	Information Security Risk Management Policy	Information Security	Live
10	Information Transfer Policy	Information Security	Live
11	Logging and Monitoring Policy	Information Security	Live
12	Management of Non-Conformance and Corrective Action Policy	Information Security	Live
13	Media Handling Policy	Information Security	Live
14	Network Security Policy	Information Security	Live
15	Vulnerability and Patch Management Policy	Information Security	Live
16	Business Continuity Plan	BCP	Live
17	Business Continuity Report Template	BCP	Live

18	Acceptable Use Policy	Information Security	Live
19	Bring Your Own Device (BYOD) Standard	Information Security	Live
20	Change Management Policy	Information Security	Live
21	Clear Screen and Clear Desk Policy	Information Security	Live
22	Cryptography Standard	Information Security	Live
23	Identity and Access Management Standard	Information Security	Live
24	Information Asset Owner Role	Information Security	Live
25	Information Security Risk Management Standard	Information Security	Live
26	Logging and Monitoring Standard	Information Security	Live
27	Security Incident Response Plan	Information Security	Live
28	Vulnerability and Patch Management Standard	Information Security	Live
29	Third Party and Suppliers Information Security Policy	Information Security	Draft
30	Business Continuity Policy	BCP	Draft
31	Third Party Security Assurance Standard	Information Security	Not created
32	Phishing and Penetration Test Schedule	Information Security	Not created
33	Physical and Environmental Security Policy	Information Security	Not created
34	IT Risk Assessment and Treatment Methodology	Information Security	Not created
35	IT Controls Exception Log	Information Security	Not created
36	Password Policy	Information Security	Not created

37	Supply Chain Security Standard	Information Security	Not created
38	Access Control Procedure	Information Security	Not created
39	Disaster Recovery Policy	BCP	Not created
40	Cyber Security Strategy 2023-2026	-	Live
41	People & Communications Governance Manual	-	Live
42	Disciplinary and Dismissal Policy	Information Security	Live
43	Lothian pension fund managed services handbook	Information Security	Live