Appendix 1

Internal Audit

2023/24 Annual Report and Opinion

June 2024

Overall Opinion	***Reasonable Assurance***	There is a generally sound system of governance, risk management and control in place. While some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives, individually these do not significantly impair the Lothian Pensions Fund's system of internal control.

Contents

1. Introduction

The Public Sector Internal Audit Standards (PSIAS) requires the Chief Audit Executive to deliver an annual report which provides a summary of internal audit activity for the year, and an annual opinion which concludes on the adequacy and effectiveness of the Lothian Pension Fund (LPF) governance, risk management and control framework.

The annual report includes consideration of:

- a summary of the information that supports the opinion
- disclosure of any impairments to scope and / or independence
- a statement of conformance with the PSIAS including the results of the quality assurance and improvement programme and progress against any improvement plans, and
- consideration of any other relevant issues.

LPF is also required to approve an Annual Governance Statement. The Internal Audit Annual Opinion supports the Annual Governance Statement which is included within the Annual Accounts.

Basis for the opinion

The opinion on the adequacy and effectiveness of the LPF's systems of control is achieved through delivery of a risk-based audit and assurance programme aligned to the LPF's key risks which is approved by the Pensions Committee.

Audit assurance to LPF is not provided in isolation. The opinion also considers reports issued by the External Auditor, the results of other assurance activities performed during the year, and the effects of any significant issues or changes impacting LPF's control environment.

Internal Auditors must consider the probability of significant errors, fraud, non-compliance, and other exposures when developing engagement objectives. No specific procedures were performed during the year to detect fraud; however, the risk of fraud is considered in all Internal Audit work.

The opinion also reflects progress with implementation of management actions from previously completed audits which contributes to strengthening the overall governance, risk, and control environment.

In March 2023, as part of the review of the Internal Audit Charter, the Pensions Committee approved adoption of the Chartered Institute of Public Finance and Accountancy's (CIPFA) standard definitions for audit opinions. Details of the overall definitions are provided within Appendix 2.

Overall Opinion	*Reasonable Assurance*

2. Executive Summary

Overall opinion and summary of key findings

The 2023/24 Internal Audit Annual Opinion confirms that ***'reasonable assurance'*** can be placed on the adequacy of the Lothian Pension Fund (LPF) systems of governance, risk management and internal controls.

The opinion reflects the year 1 April 2023 to 31 March 2024, concluding there is a generally sound system of governance, risk, and control in place. The 2023/24 overall opinion remains aligned to the 2022/23 opinion.

Internal Audit work identified a number of issues, areas of non-compliance and/or scope for improvement throughout the year, which individually do not significantly impair LPF's system of internal control but may put at risk the achievement of LPF objectives if corrective actions are not adequately addressed.

Internal audit activity

The LPF Internal Audit plan approved in March 2023 included circa 105 days across five audits. The audit of Project Forth was subsequently removed due to the project cessation and therefore a total of four audits were completed.

Follow-up of audit actions

In addition, the plan included follow-up of management's progress with implementing actions raised in previous internal audits. The opinion also reflects the progress made in addressing management actions raised.

Key thematic findings and alignment to risk management

LPF undertook a comprehensive review of its Risk Management Framework during 2023 which resulted in a simplified methodology and revised risk

Audit work completed during 2023/24 highlighted potential issues for the following 6 LPF risks, with further detail provided at section 6:

- Business interruption
- Regulatory breach
- Cyber security
- Data management
- Recruitment and retention
- IT systems.

No indicators of fraud were highlighted during internal audit work and our assessment of fraud risk is low.

It should be noted that the opinion does not imply that Internal Audit has reviewed all risks and assurances relating to LPF.

Other sources of assurance

Internal Audit is only one of several sources of assurance over the LPF Group's risks. Assurance is also provided through other assurance activities (for example, external audit, BDO, Mercer and LPF's Risk and Compliance function).

Performance of Internal Audit work

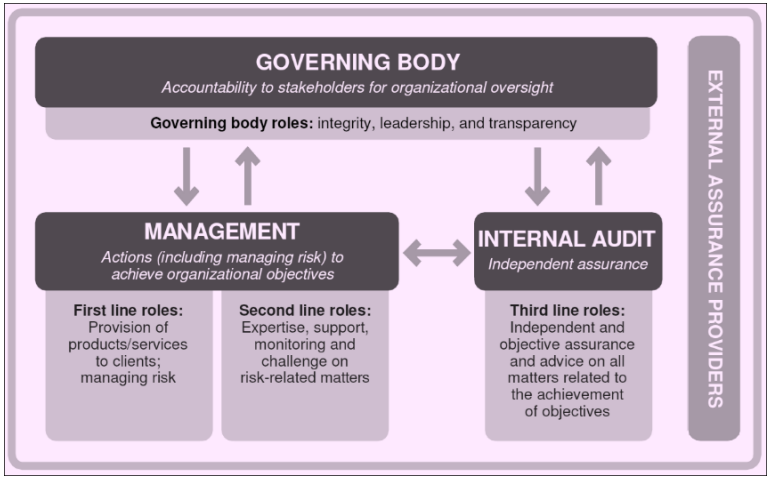
Internal Audit work during 2023/24 was performed by the Council's co-source internal audit provider, PwC. All work was performed in accordance with PwC's Internal Audit methodology which is in conformance with the

registers. At at 31 March 2024, LPF's risk management framework included 26 risks across the LPF Group.

3. Audit approach and responsibilities

The Three Lines Model

The Institute of Internal Auditors 'Three Lines Model' can be translated across the structure and operations of LPF with first line teams and services responsible for ongoing service delivery and risk management; second line teams such as Governance, Risk and Compliance; HR and Finance responsible for providing frameworks, policies, and guidance, and the third line, Internal Audit providing independent assurance. External Assurance is also provided through external audit and other providers such as BDO and Mercer.



Internal Audit Objectives and responsibilities

The objective of Internal Audit is to provide independent and objective assurance and a systematic and disciplined approach to evaluating and improving the effectiveness of the LPF's governance, risk management and control environment.

This is achieved through development of a risk-based internal audit plan which is based on LPF's audit universe, strategic objectives and an assessment of risks and emerging issues affecting LPF with input from management, committee members, and other key stakeholders including the Independent Pensions Observer and External Audit.

Internal Audit performs audit engagements throughout the year in line with the agreed audit plan and emerging areas of risk. Internal Audit reports on the findings and observations for each review and where areas of improvement are identified, findings and recommendations are raised, and management agree actions and timescales by which they will address the gaps identified.

It is the responsibility of LPF's Chief Audit Executive to provide an independent and objective annual opinion on the adequacy and effectiveness of LPF's governance and risk management and control frameworks. The opinion is provided to the Pensions Committee and should inform the Annual Governance Statement.

Management responsibilities

The presence of an effective internal audit team contributes towards, but is not a substitute for, effective control. It is the responsibility of management to establish adequate internal controls so that the activities are conducted in an Public Sector Internal Audit Standards, with oversight from LPF's Chief Audit Executive.

efficient and effective manner, in adherence with legislation, policies and procedures, and that assets and records are safeguarded.

It is also management's responsibility to address and rectify the weaknesses identified by Internal Audit via timely implementation of agreed management actions.

Pensions Audit Sub-Committee and Pensions Committee

The Pensions Committee is responsible for approving the risk based annual Internal Audit Plan. The Pensions Audit Sub-Committee monitors the internal audit plan and reviews all audit and inspection work towards the plan, scrutinises internal audit and external audit reports and monitors governance, risk management and internal control on behalf of the Pensions Committee.

4. Summary of work completed

2023/24 LPF Internal Audit Plan

The 2023/24 Internal Audit Plan was approved by the LPF Pensions Committee in March 2023. The plan included coverage across the LPF group including LPF, LPFI and LPFE.

Planned and actual audit coverage

The 2023/24 internal audit plan included a total of 5 engagements as follows:

Audit title	High level scope
Senior Managers and Certification Regime (SM&CR)	Review of the adequacy and operating effectiveness of governance processes established to provide assurance of compliance with the key elements and prescribed responsibilities of the SM&CR.
People Processes	Review of the adequacy and operating effectiveness of established people processes to ensure robust controls are in place, complied with and support achievement of LPF objectives.
Information Security	Review of the design of the suite of IT policies, standards and procedures that have been developed during 2022 to prevent, respond and manage information security across LPF, as well as ensuring they are aligned to the IT strategy.
Business Continuity and Incident Response	Review of the adequacy and operating effectiveness of key controls and processes established to provide assurance that LPF maintains business continuity plans to ensure they maintain services during an emergency or extended incident.
Project Forth	Targeted review in line with project timelines.

A total of 100 days were planned for delivery of the audit work during 2023/24. Following project cessation, the Project Forth audit was removed from the plan in March 2024, therefore 80 audit days were delivered for LPF during 2023/24.

Audit management and committee reporting

A further 5 days were used for audit administration including time for the Chief Audit Executive to perform the annual risk assessment and development of the annual plan, preparation of committee reports, the annual report and opinion and attendance at Committees.

Follow-up of recommendations

In addition, the plan included follow-up of management's progress with implementing management actions raised in previously completed internal audits.

Circa 20 hours (3 days) were used by Internal Audit to review and validate information and evidence provided by management to support closure of management actions previously raised in internal audits.

A further 2 days was spent on planning and performing the annual validation review completed during 2023/24 to validate whether a sample of LPF management actions closed between 1 January 2022 and 31 December 2022 continue to be effectively sustained.

5. Audit outcomes and key messages

Outcomes for the four audits completed during 2023/24 are set out below with the total number of audit recommendations by priority rating. Performance for the previous two years is also provided for comparison.

	Overall Rating	High	Medium	Low	Total
Senior Managers and Certification Regime (SM&CR)	Reasonable Assurance	0	6	1	7
People Processes	Substantial Assurance	0	0	3	3
Information Security	Substantial Assurance	0	1	1	2
Business continuity and incident response	Limited Assurance	5	12	4	21
Total 2023/24 – 4 audits		**5**	**19**	**9**	**33**
Total 2022/23 – 3 audits		4	9	6	**19**
Total 2021/22 – 4 audits		0	9	10	19

Areas of strength identified

- there is a good interpretation of the general Senior Managers and Certification Regime (SM&CR) rules within LPF
- LPF has a comprehensive suite of IT security policies aligned to ISO27001 standards and a Cyber Strategy for 2023-26 is in place
- a comprehensive suite of HR policies are in place with oversight from LPFE and the People Group

Areas for improvement identified

The following areas for improvement were identified during audit engagements, which, if not adequately addressed may have an impact on achievement of related LPF objectives.

Senior Managers and Certification Regime (SM&CR)

- finalising specific SM&CR documents and supporting governance arrangements including prescribed responsibilities, development of a practical handover policy and an appointment and induction process aligned to SM&CR requirements.

Information Security Arrangements

- 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, and roll-out of the policy development framework.

People Processes

- ensuring all interview documents such as scoring matrices are added to PeopleHR, ensuring half-year appraisals are completed on time and reviewing HR policies periodically in line with best practice.

Business Continuity

- undertaking a review of Business Continuity Management capability, experience, guidance, and tools, and enhancing the Business Impact Analysis process to define critical outputs, tolerable levels and acceptable timeframes. Updating the draft Business Continuity Plan to outline step by step instructions for recovery of priority services and ensuring business continuity is embedded in business-as-usual activities / supported by a training and awareness programme.

- a Business Continuity Plan and Security Incident Response Plan is in place.

6. Alignment with risk management

The 2023/24 Internal Audit annual plan was based on the LPF risk register as at February 2023 and the plan was designed to provide assurance across the LPF very high and high rated risks at that time. Issues identified across the four audits completed during 2023/24 were related to following LPF risks:

- **Cyber Security** – the Information Security audit identified opportunities to strengthen cyber and data security arrangements to protect LPF from information security threats and cyber-attacks which could prevent key operational processes from being undertaken and lead to financial losses and reputational damage were highlighted through audit work.

  As at March 2024, LPF's risk rating for Cyber Security was moderate which is a fair reflection of the governance, risk, and control environment. Given the increasing cyber incidents impacting public sector organisations during 2023/24, control effectiveness should be regularly reviewed and considered closely with other risks such as business interruption, data management and IT systems.

- **Business Interruption** – potential business interruption risks which could have a significant and/or extended business interruption (including third party suppliers) leading to a potential failure or inability to complete key LPF processes were highlighted across 2 audits completed during 2023/24.

  As at March 2024, LPF's risk rating for business interruption was moderate. This scoring should be reviewed based on both audit outcomes and in line with progress of ongoing mitigating actions, to ensure that it accurately reflects the current effectiveness of key controls.

  Management are currently reviewing the key business continuity controls following the Business Continuity audit.

- **Data Management** – the Information Security audit highlighted low/moderate opportunities to management risks associated with mismanagement or poor maintenance and protection of data including

  As at March 2024, LPF's risk rating for Data Management was moderate which is a fair reflection of the governance, risk, and control environment.

- **IT systems** – the Information Security audit highlighted opportunities to improve management of the risk of LPF not meeting operational requirements due to inadequate IT hardware or software leading to material or extended service delivery issues. Recommendations included development of an Incident Management policy to help ensure a proactive and structured approach to the handling of IT and cyber security incidents, and managing the risk of system failures or disruptions that may impact the organisation.

  As at March 2024, LPF's risk rating for IT systems was moderate which is a fair reflection of the governance, risk, and control environment.

- **Regulatory Breach** – the Senior Managers and Certification Regime audit identified opportunities to manage the risk of not meeting regulatory obligations leading to enforcement action or fines and reputational damage including ensuring documenting governance and compliance with SM&CR including SMFs and Certified persons responsibilities and development of a handover policy.

  As at March 2024, LPF's risk rating for Regulatory Breach was moderate which is a fair reflection of the governance, risk, and control environment.

- **Recruitment and Retention** – the People Processes audit identified low priority recommendations to strengthen recruitment and retention related risks including enhancing HR policies, ensuring half-yearly appraisals are completed and ensuring candidate scorings are recorded within People HR.

  As at March 2024, LPF's risk rating for recruitment and retention was high which reflected recruitment and change factors affecting several business areas and dependencies on key roles and functions.

7. Progress with implementation of management actions

A total of 33 management actions were raised across the 4 LPF internal audit reviews completed during the year. The majority of actions were raised in the Business Continuity audit.

Timely and effective implementation of audit actions by management is important to prevent LPF being exposed for longer than necessary to the potential risks associated with the control gaps or deficiencies identified in audits.

Performance in progress with implementing management actions are reported quarterly to the Pensions Audit Sub-Committee for scrutiny.

A total of 20 audit actions (5 high, 13 medium and 2 low rated) raised across 6 previous LPF audits were closed during 2023/24, and all actions for the following 3 audits are now closed. As a result, impacts resulting from exposure to the risks originally raised these audits are reduced:

- **Bulk Transfers** – August 2021
- **Technology Model Development** – February 2022
- **Risk Management** – August 2022

In addition, all of the management actions raised in the following two audits completed in 2023/24 have been closed:

- **Senior Managers and Certification Regime**
- **People Processes**

Annual validation review of previously implemented actions

An annual validation review was completed during 2023/24 to validate whether a sample of LPF management actions closed between 1 January 2022 and 31 December 2022 continue to be effectively sustained.

The audit reviewed two actions which had been implemented by management between 1 January 2022 and 31 December 2022. Both management actions sampled continued to function as originally validated.

Overdue Management Actions

As at 31 March 2024, there were at total of 26 open audit actions with the following 11 overdue management actions which were passed their original implementation date. This was an increase of 8 when compared to the closing position for the previous year (2022/23):

- **Information Governance** – 7 overdue actions
- **Third Party Supplier Management** – 2 overdue actions
- **Senior Managers and Certification Regime** – 2 overdue actions

The final actions for the Senior Managers and Certification Regime audit were closed in May 2024.

Actions closed due to management's acceptance of risk

No actions were closed based on management's acceptance of risk during the period 1 April 2023 to 31 March 2024.

Rebased Management Actions

In March 2024, revised dates were provided to the Pensions Audit Sub-Committee for the following remaining actions related to the Information Governance audit completed in May 2023:

Rebased audit actions

Recommendation title	Management actions
1.1 - Policy, Standards & Procedures Implementation	incorporate data strategy, data archiving, and information governance controls into new or existing documentation
3.3 - Retention schedule guidance	document guidance on how retention periods are determined, including how CEC's requirements are tailored to LPF update retention schedule to align with LPF's data assets
6.1 - Information Asset register review and update	review and update its information asset register, and ensure the asset register, system list, third party supplier list, and retention schedule align
6.2 - Update of registers to illustrate system dependencies	update existing registers (which may include third party supplier list, system lists, refreshed information asset register) to capture details; and create overview diagram(s) to illustrate the flow of business-critical systems

8. Conformance with Public Sector Internal Audit Standards

LPF Internal Audit delivery model

During 2023/24, all Internal Audits for LPF were delivered by the Council's co-source partner PwC with oversight from the Council's Principal Audit Manager and Chief Audit Executive.

The Chief Audit Executive also completes the risk assessment process to support the annual plan, attends and reports to the Pensions Audit Sub-Committee quarterly and prepares the Internal Audit annual report and opinion.

Independence and limitations of scope

In line with PSIAS, Internal Audit must be independent, and all internal auditors must be objective in performing their work. To ensure conformance with these requirements, Internal Audit has established processes to ensure that both team and individual independence is consistently maintained and that any potential conflicts of interest are effectively managed.

We do not consider that we have faced any impairments to our independence during 2023/24, nor do we consider that we have faced any scope or resource limitations when completing our work.

Quality Assurance and Improvement Programme

External Quality Assessments (EQA) should be completed every five years. In 2021/22, an EQA was performed for the Council's Internal Audit function by the Chartered Institute of Internal Auditors (IIA) and the results reported to Committee in December 2022. There are no outstanding actions from the 21/22 EQA. The next EQA for the Council's Internal Audit function is due to be performed in 2026/27.

Ongoing reviews to ensure quality on an audit by audit basis are in place. This includes Chief Audit Executive review and sign-off of planning and reporting for all audit work, and ongoing supervision and review of fieldwork throughout by a manager.

Periodic assessments are conducted through self-assessments and Internal Quality Assessments (IQA) on a recurring basis. All LPF audit work was performed in accordance with PwC's Internal Audit methodology which is in conformance with the Public Sector Internal Audit Standards, with work reviewed by a PwC manager and Partner and with oversight from LPF's Chief Audit Executive.

Appendix 1 – Outcomes and status of 2023/24 LPF Internal Audits

Audit title	Outcome	Status % actions completed	
People Processes	Substantial Assurance	**Closed**	**100%** All actions closed
Senior Manager and Certification Regime	Reasonable Assurance	**Closed**	**100%** All actions closed
Information Security	Substantial Assurance	**Action tracking**	**50%** 1 action closed 1 action not yet due
Business Continuity	Limited Assurance	**Action tracking**	**0%** Phased implementation

Appendix 2 – Overall Assurance and Priority Definitions

Overall Assurance Ratings	
Substantial Assurance	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.
Reasonable Assurance	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.
Limited Assurance	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.
No Assurance	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	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	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.