# Pensions Committee

2pm, Wednesday, 28 September 2022

## Lothian Pension Fund - Internal Audit Update as at 31 August 2022

## 1. Recommendations

The Pensions Committee is requested to note:

1.1 The outcomes of the final audit supporting completion of the Lothian Pension Fund (LPF) 2021/22 Internal Audit (IA) annual plan and annual opinion;

1.2 A proposed update to the 2022/23 IA plan agreed by Committee in March 2022 to reflect ongoing progress with Project Forth; and

1.3 Progress with implementation of agreed management actions to support closure of LPF IA findings raised.

**Laura Calder**
Senior Audit Manager, City of Edinburgh Council
Legal and Assurance Division, Corporate Services Directorate
E-mail: laura.calder@edinburgh.gov.uk | Tel: 0131 469 3077

## 2. Executive Summary

2.1 This report provides details of the progress of Internal Audit's (IA) assurance activity on behalf of LPF performed by the City of Edinburgh Council's (the Council) IA function.

2.2 Delivery of the four audits included in the 2021/22 IA annual plan is complete with the final audit which supported LPF's 2021/22 annual opinion presented to the Committee in June 2022.

2.3 The 2022/23 IA annual plan was approved by the Committee in March 2022 and included a focus on Project Forth and Information technology. An update to the plan is proposed to reflect the ongoing progress of Project Forth and enable assurance across a wider range of LPF risks supporting the 2022/23 IA annual opinion.

2.4 As at 31 August 2022, LPF had 13 open IA findings (1 High; 4 Medium; 8 Low) supported by 15 agreed management actions (1 High; 6 Medium; 8 Low). One high rated finding raised in the Cessations audit completed in November 2021 is overdue.

2.5 A report detailing the outcomes of the Risk Management review (Effective) is included for the Committee's review and scrutiny.

## 3. Background

**Internal Audit Annual Plan**

3.1 The LPF IA plan is risk based and is developed from review of the LPF risk register and discussion with management, with the audits included in the plan designed to test the effectiveness of the controls, and governance and risk management frameworks established to mitigate and manage LPF's risks.

**2021/22 Internal Audit Annual Plan**

3.2 Delivery of the 2021/22 LPF IA plan approved by the Pensions Committee in March 2021 is now complete, and included the following four audits:

- Technology Model Development;
- Capital Calls;
- Receipt of Employer Contributions; and
- Risk Management

3.3 Outcomes of the four completed audits included in the plan support the 2021/22 LPF Internal Audit annual opinion presented to Committee in June 2022 and inform the annual Governance Statement included in the financial statements.

**2022/23 Internal Audit Annual Plan**

3.4 The 2022/23 LPF IA plan was approved by the Pensions Committee in March 2022 and includes two large scale reviews with a focus on Project Forth design and implementation readiness, and the adequacy and effectiveness of LPF's technology security assurance arrangements.

**Proposed update to the 2022/23 Internal Audit Annual Plan**

3.5 Arrangements for Project Forth continue to progress, therefore, to ensure adequate assurance is provided to support the 2022/23 IA annual opinion for 31 March 2023, it is proposed that the scope of the larger scale Project Forth review separated into three reviews which will cover a wider scope and range of LPF risks (see para 4.6 for further details).

**Internal Audit Follow-Up Process**

3.6 Where control weaknesses are identified, Internal Audit findings are raised, and management agree recommendations and completion timeframes to address the gaps identified. However, it is the responsibility of management to address and rectify the weaknesses identified via timely implementation of agreed management actions.

3.7 Findings raised by IA in audit reports typically include more than one agreed management action to address the risks identified. IA methodology requires all agreed management actions to be complete in order to close the finding.

3.8 IA define a finding as overdue when associated management actions have not been closed by the original date agreed by management. Overdue findings therefore include those where revised implementation dates have been subsequently agreed.

## 4. Main Report

**Progress with delivery of the 2021/22 LPF IA annual plan**

4.1 All four audits included in the 2021/22 IA annual plan are complete and supported the 2021/22 IA annual opinion reported to Committee in June 2022.

4.2 Details of the outcomes of the remaining review of Risk Management which supported the 2021/22 annual opinion are included below.

**Risk Management (Effective)**

4.3 The review confirmed that LPF's risk management framework is proportionate and adequately designed for the size and structure of LPF and is operating effectively across the organisation providing assurance that risks are being effectively identified; assessed; recorded; and managed such that LPF's objectives should be achieved.

4.4 One medium and two low rated findings were raised highlighting the need to ensure corporate risks are fully aligned with strategic objectives; clear corporate risk definitions are established; risks and controls are clearly articulated across the organisation; and risk management training is provided to new employees.

4.5 The final report is included at Appendix 1.

**2022/23 LPF IA annual plan**

4.6 The 2022/23 IA plan agreed in March 2022 includes two large scale reviews, one of which focused on Project Forth, and the other which considers the adequacy of technology security assurance arrangements.

4.7 Implementation of Project Forth is ongoing, therefore, to ensure adequate assurance is provided to support the 2022/23 IA annual opinion, is it is proposed that the large-scale Project Forth review is separated into three reviews.

4.8 The updated 2022/23 IA annual plan would therefore include:

- Project Forth – Programme assurance
- LPF Information Governance
- LPF Third-party supplier management
- Adequacy of technology security assurance arrangements

4.9 PwC and the Council IA function have confirmed that the four reviews above can be delivered in sufficient time to provide an IA annual opinion.

**Status of Internal Audit Findings as at 31 August 2022**

**Open IA Findings**

4.10 As at 31 August 2022, LPF had 13 open IA findings (1 High; 4 Medium; 8 Low) and 15 supporting agreed management actions (1 High; 6 Medium; 8 Low). The findings were raised across the following reviews:

- Bulk Transfers;
- Cessations;
- Technology Model Development;
- Employer Contributions;
- Capital Calls; and
- Risk Management

4.11 One finding and supporting management action is currently overdue, with the remaining 12 findings and 14 management actions not yet due for completion and implementation currently being progressed by LPF.

**Overdue IA findings**

4.12 As at 31 August 2022, LPF had one high rated overdue finding, originally raised in the Cessations audit completed in November 2021. The finding highlighted the need for LPF to develop affordability and due diligence assessments to support the cessations process. Due to the reducing number and unpredictable timing of cessations, the implementation date for this action has been revised to 31 December 2022.

## 5. Financial impact

5.1 The cost for delivery of the 2022/23 IA annual plan is estimated to be circa £80k. Costs applied will be based on agreed rates as specified in the IA external co-source contract and actual time spent by the Council's IA team as recorded in IA time sheets and will be discussed and agreed with LPF management.

5.2 This will include the costs associated with ongoing follow-up activity; and the costs involved with preparing reports, attending committee meetings, and preparing the LPF annual plan.

5.3 It is also important to note that failure to close IA findings raised and address the associated risks in a timely manner may also have financial impacts which are not yet measurable.

## 6. Stakeholder/Regulatory Impact

6.1 IA findings are raised as a result of control gaps or deficiencies identified during audits. If agreed management actions are not implemented to support closure of Internal Audit findings, LPF will be exposed to the risks set out in the relevant IA reports, including the potential risk of non-compliance with applicable regulations.

## 7. Background reading/external references

7.1 Public Sector Internal Audit Standards

## 8. Appendices

Appendix 1 Annual Plan Scope Limitations

Appendix 2 Final Risk Management Internal Audit Report

## Appendix 1: Annual Plan Scope Limitations

1. Whilst the IA Annual Plan is delivered by the Council's IA team with support from PwC through the Council's established co-source arrangements, IA is not the only source of assurance provided to LPF as there are a number of additional assurance sources (for example, external audit) that the Committee should consider when forming their own view on the design and effectiveness of the LPF control environment and governance and risk management frameworks.
2. Details of additional assurance provided on LPF activities is included in the LPF assurance map maintained by management.
3. Lothian Pension Fund Investments (LPFI Ltd) is a fully owned subsidiary of LPF and has been registered with the Financial Conduct Authority (FCA) since June 2016 to advise on investments, with the exception of pensions transfers and opt outs. Whilst the same operational processes and controls are applied by both LPF and LPFI, IA has not been requested to provide assurance on LPFI investment advice activities, and the extent of their compliance with FCA and other applicable regulatory requirements.
4. Consequently, IA assurance is currently limited to the activities of LPF and the extent of their compliance with Scottish Local Government Pension Scheme (LGPS) regulatory requirements.
5. Where relevant, any LPF control weaknesses identified that could result in potential non-compliance with FCA regulatory requirements are highlighted in IA findings raised for management's attention.
6. All LPF IA reports prepared by the Council are presented to the LPF Pensions Audit Sub Committee for scrutiny, and then referred to the Pensions Committee for information (where appropriate).

# *The City of Edinburgh Council*
# Internal Audit

## Lothian Pension Fund - Risk Management

Final Report

16 August 2022

LPF2103

**Overall report rating:**

| | |
|---|---|
| **Effective** | The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved. |

# Contents



This internal audit review is conducted for the Lothian Pension Fund ("LPF", "the Fund") under the auspices of the 2021/22 internal audit plan approved by the Pensions Audit Sub Committee in March 2021. The review is designed to help the Lothian Pension Fund assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

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 a number of 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 Pensions Committee members as appropriate.

# 1. Background and Scope

## Background

Lothian Pension Fund (LPF) is directly regulated by The Pensions Regulator; the Scottish Information Commissioner; and is subject to other public sector rules and regulations. LPF's administration is managed through subsidiary companies, to which corporate law applies.

An operational risk management framework has been established within LPF and is currently owned and managed by the Chief Risk Officer, with support from the Compliance & Risk Manager.

LPF's ongoing application of the established governance and risk management frameworks is monitored by both the Pensions Committee and Audit Sub-Committee.

## Risk Management Overview

Risk management involves identifying, assessing, and supporting the control of threats to the achievement of an organisation's strategic objectives. Risks can originate from a wide variety of sources, including financial uncertainty, regulatory and legal considerations, strategic management decisions, accidents, technology security threats and information risks.

Effective risk management is a fundamental element of good governance and can support efficient and effective resource allocation; well informed decision making; and increase the likelihood of achieving objectives whilst supporting the organisation's sustainability and protecting its reputation.

COVID-19 has demonstrated the increased importance of effective risk management as the pandemic has affected all organisations and has highlighted a significant number of new and emerging risks that may not have been previously considered resulting in development and implementation (where possible) of effective mitigating controls to manage these risks.

Under section 2120 of the Public Sector Audit Standards there is a requirement for internal audit (IA) 'to evaluate and contribute to the improvement of the organisation's risk management processes'.

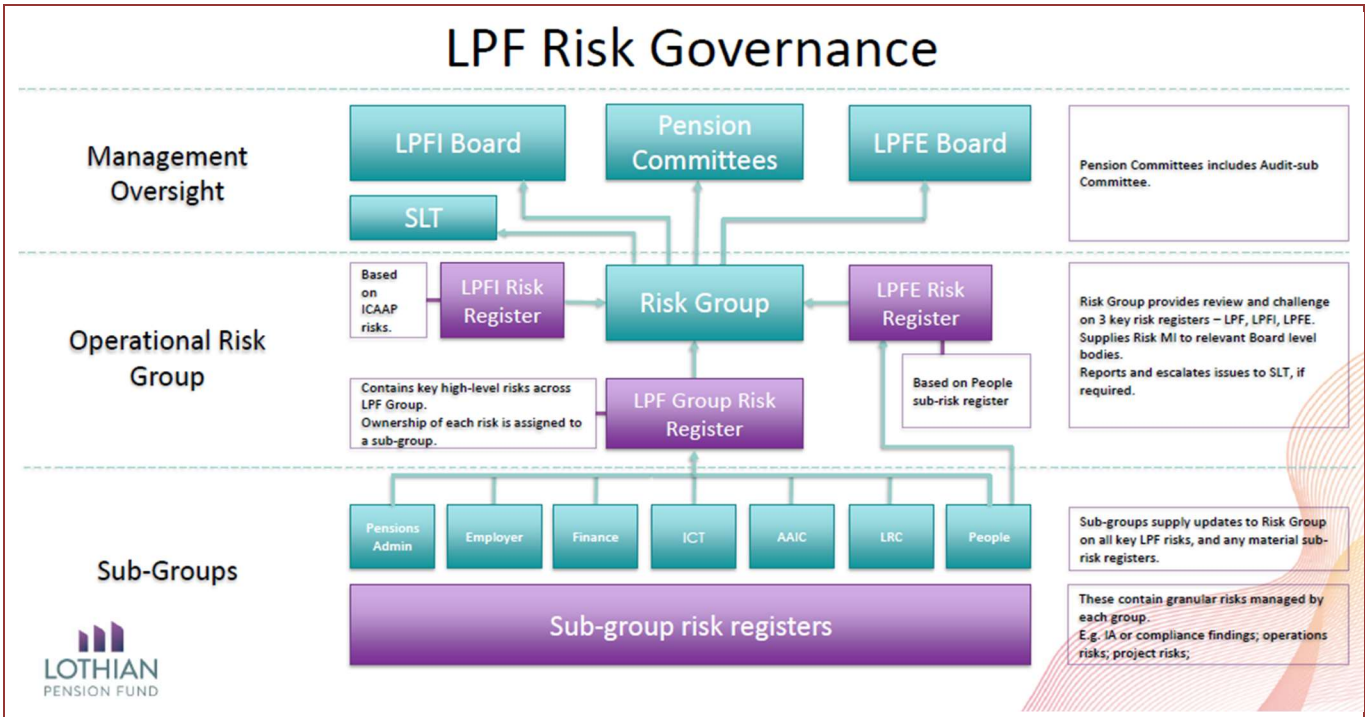
For the purposes of this internal audit, determining whether risk management is effective will be based on an assessment and confirmation that:

- organisational objectives and associated risks support and align with the organisation's mission;
- significant risks are identified and assessed;
- appropriate risk responses are selected that align risks with the organisation's risk appetite; and
- relevant risk information is captured and communicated in a timely manner across the organisation, enabling staff, management and the board to carry out their responsibilities.

## LPF Risk Management Framework

IA held a number of initial meetings with key members of the LPF team to understand the Group's strategic objectives and supporting risk management framework. A document outlining management's overview of LPF's ongoing risk management initiatives was provided and used as a point of reference during the review.

The diagram below also highlights LPF's established risk governance arrangements:




## Scope

The review assessed the design adequacy and operating effectiveness of LPF's operational risk management framework and its application across the organisation. This included a focus on new and emerging risks faced by, and material to the organisation, including any presented by COVID-19. It also included the adequacy of oversight provided by both LPF management and relevant governance forums.

The design and effectiveness of the framework will be assessed against the four key elements of PWC's best practice enterprise risk management (ERM) framework that is based on both COSO Enterprise Risk Management Framework principles, and ISO31000, as detailed below:

| Principle | Description |
|---|---|
| Proportionate | Risk management activities must be proportionate to the level of risk faced by the organisation. |
| Aligned | Risk management activities need to be aligned with the other activities in the organisation. |
| Comprehensive | In order to be fully effective, the risk management approach must be comprehensive. |
| Embedded | Risk management activities need to be embedded within the organisation. |
| Dynamic | Risk management activities must be dynamic and responsive to emerging and changing risks. |

## Limitations of Scope

The review was limited to LPF's parent group operational risk management framework. The following areas were specifically excluded from the scope:

- the LPF Investment (LPFI) subsidiary operational and regulated risk management;
- the LPF Employment (LPFE) subsidiary operational risk management process;

- the management of the risk associated with performing due diligence on individual investments and underlying managers by LPF's investment team and sub-groups; and

- whilst the audit considered the processes supporting identification and inclusion of third-party supplier risks within the LPF risk profile, review of the established LPF supplier management framework was specifically excluded from scope.

The only exception to these scope limitations was to assess whether the group risk management framework (and any separate reporting) adequately and proportionately considers LPFI and LPFE risks, and to confirm that subsidiary risks are effectively identified; assessed; recorded; managed and escalated (when required and appropriate) to LPF.

**Reporting Date**

Our audit work concluded on 13 May 2022 and our findings and opinion are based on the conclusion of our work as at that date.

# 2. Executive summary

## Total number of findings: 3

| Summary of findings raised | |
|---|---|
| **Medium** | 1. Alignment of corporate risks with strategic objectives |
| **Low** | 2. Maintenance of risk registers |
| **Low** | 3. Risk management training for new starts |

## Opinion

**Effective**

The Lothian Pension Fund (LPF) risk management framework is adequately designed for the size and structure of LPF, and operating effectively across the organisation, providing assurance that risks are being effectively identified; assessed; recorded; and managed such that LPF's objectives should be achieved.

To help embed risk management across the organisation, the Senior Leadership Team (SLT) meets monthly and has oversight of LPF's key risks through the corporate risk register, and the Risk Management Group (RMG) meets quarterly and has responsibility for the oversight of the risk management framework. This includes being the reporting point for material incidents; monitoring the sub-group approach to risk management; ensuring appropriate levels of risk management training and awareness; horizon scanning for future risks; and risk reporting to board-level bodies. The Chief Risk Officer is an attendee at both the SLT and RMG meetings.

We confirmed that the LPF risk management framework could be further strengthened by confirming the completeness of the current population of corporate risks; ensuring that they are fully aligned with strategic objectives; creating clear corporate risk definitions; ensuring that risks and controls are clearly articulated across the organisation; and providing risk management training for new employees.

Consequently, one medium and two low rated findings have been raised.

The medium rated risk management finding raised in the Settlement and Custodian Services audit completed in June 2020 that highlighted the need to improve regulatory and risk management oversight of custodian processes performed by Northern Trust has also been closed based on the work completed during this review.

### Areas of good practice

The following areas of good practice were also noted during our review:

1. **Management and oversight of risk** - Risk management is embedded into the regular operations of LPF. This was evident through the quarterly RMG meetings, the monthly SLT meetings which have a standing agenda item for 'Risk Management and Compliance' and the regular review and updates to the corporate and operational risk registers throughout the year, this was evident from the action logs and the individual risk registers. The Pension Committee also has a key oversight role and a Risk Management Summary paper from the CRO is presented to each meeting.
2. **Ensuring the risk framework is dynamic -** The RMG drives risk management and has responsibility across all areas of the LPF risk management framework. The RMG meet quarterly and review the risk landscape of the organisation using the risk registers at corporate and subgroup

level. This includes assessing key risk events, escalated risks from the operational risk registers, emerging risks (horizon scanning) and risk management training needs. The output of the group includes the actions and decisions log, the updated LPF Group Risk Register, an annual risk report for the Audit Subcommittee, and a quarterly Risk update for the Pension Committee.

3. **Responsibility for risk management -** Roles and responsibilities are defined in risk guidance documents and through risk management training that was completed by all LPF employees in Q1 2021. Additionally, risk management communications have been issued to all employees through 2021 from the CRO and CEO, reinforcing the importance of everyone's role in managing risk. We also understand that employees are required to set a risk related performance goal each year as part of their objectives which helps reinforce a culture of accountability for risk management.
4. **Ongoing initiatives to improve the risk management framework -** management has advised that the following risk management initiatives are progressing:
    - A review of the risk policy, which is contained within the corporate risk register, to be a standalone policy covering all elements of the LPF risk framework.
    - A review of the RMG membership to align to the LPF developing 'People' initiatives, ownership and accountability.
    - Consideration of an additional resource in the Risk and Compliance Team.
    - Consideration of a risk tracking software which would link to the existing Compliance Monitoring Programme (CMP) system.
    - Ongoing review of the risk governance processes to ensure ongoing focus on key risks and maintaining a 'live' risk culture.
    - Review of the frequency and content of annual risk management training delivered through the ComplianceServe system, including review of the frequency and detail of the training to ensure it continues to be effective.
    - The Risk and Compliance Team complete specialist continuous professional development, including membership of the Institute of Risk Management (IRM). The CRO presently Chairs the IRM's Scottish Group gaining access to a network of resources on emerging issues and best practice in the risk sector.

# 3. Detailed findings

| 1. Alignment of corporate risks with strategic objectives | Medium |
|---|---|

Risk management involves identifying, assessing, and supporting the control of threats to the achievement of an organisation's strategic objectives.

However, it is currently unclear whether the corporate risks reported by LPF detailed below are complete (for example, there is currently no reporting on financial and budget management; fraud; and reputational risks) and aligned with the strategic goals and priorities set out in the LPF Strategy and Business Plan 2022/23 (in draft at the time of this review).

The LPF corporate risk register includes risk across the following categories, however these are not currently supported by definitions:

- Assets and Investment Management
- Employers and liability management
- People and communications
- Members & pension administration
- ICT and systems
- Governance
- Information Governance
- Legal, Risk & Compliance
- Supplier management and procurement

**Risks**

The potential risks associated with our findings are:

- LPF may not be identifying and reporting on its full population of potential risks and may not identify risks that could potentially impact on delivery of strategic objectives.

**1.1 Recommendation: Aligning corporate risks with strategic objectives and risk definitions**

1. Management should review the current population of LPF corporate risks to confirm that they are complete and ensure that they align with the strategic objectives and goals set out in the LPF Strategy and Business Plan.
2. Risk definitions should be established for each risk category; agreed by management; and communicated across LPF for ongoing reference when identifying and assessing risks.

**1.1 Agreed Management Action: Aligning corporate risks with strategic objectives and risk definitions**

We will look to re-review our risks with this finding in mind and use it as an opportunity to step back and consider more holistically the risks we capture and how we can effectively manage and cascade granularity of definition with both ongoing operational risk management and reporting/governance in mind.

The Risk Management Group (RMG) does seek to do this on an ongoing basis, and to strike the important balance between maintaining and reporting on the right number of risks (omitting gaps) and distracting the focus away from critical risks/strategic analysis with too much detail, but this is a helpful and timely point to review this. We will consider within RMG and report back through the usual channels with any updates arising.

| | |
|---|---|
| **Owner**: Richard Carr, Interim Executive Director, Corporate Services<br><br>**Contributors:** Hugh Dunn, Service Director, Finance and Procurement; David Vallery, Chief Executive, Lothian Pension Fund (LPF) ; Sean Reid, Compliance and Risk Manager (LPF); Kirsten Smith, Compliance and Risk Manager (LPF); Susan Handyside, Governance Manager (LPF) | **Implementation Date:**<br>31 March 2023 |

| **2. Maintenance of risk registers** | **Low** |
|---|---|

**1. Articulation of risks**

Clearly defined risks help to ensure a consistent understanding of the risk which enables management to have a clear view on the risk rating and the key controls in place that directly mitigate the risk identified. It can also help to focus on the key actions that can be completed to manage and further mitigate the risk. As a result, best practice is to define a risk using the following syntax:

*[Event that has an effect on objectives] caused by [cause] resulting in [consequence].*

Some risks included in the LPF subgroup risk registers do not provide adequate detail to clearly define the risk, for example, "Dividend / Tax monitoring" in the accounting register and "Failure to attract talent" in the People register.

**2. Definition of risk ratings**

At subgroup level there is no definition for Low, Medium, and High-risk impact and likelihood assessments. There is an expectation that they are commonly understood but there is no evidence that they have been clearly defined in training or guidance documents.

**3. Articulation of controls**

We noted that some controls included in the corporate risk register are not recorded using best practice descriptions (who, what, why, how and when characteristics as noted in appendix 3), for example 'Asset liability studies', 'Staff forum', 'Regular contact with employers' and 'Staff training' are all noted as controls in the corporate risk register.

Furthermore, there are no control or action owners noted in the corporate risk register.

**Risk**

The potential risks associated with our findings are:

- Risks and / or controls are not clearly understood / are misinterpreted.
- Inconsistent risk and control effectiveness assessment outcomes.
- Inappropriate mitigating actions are agreed and implemented.

**2.1 Recommendation: Maintenance of risk registers**

LPF management should:

a) Review the risks included in the risk registers and ensure they are appropriately articulated.
b) Agree definitions of Low/Medium/High impact and likelihood assessments and embed their application at risk subgroups.
c) Review the controls listed in the corporate risk register to ensure that they are appropriately articulated in line with the who, what, why, and how control description principles included at Appendix 3 in this report.
d) Ensure that all mitigating actions are specific, measurable, achievable, realistic and timely.

**2.1 Agreed Management Action: Maintenance of risk registers**

| | |
|---|---|
| Likewise, we will look to re-review the sub-group registers (and tie-in with main group register) with these points in mind We will consider within Risk Management Group (RMG) and report back through the usual channels with any updates arising. | |
| **Owner**: Richard Carr, Interim Executive Director, Corporate Services<br><br>**Contributors**: Hugh Dunn, Service Director, Finance and Procurement; David Vallery, Chief Executive, Lothian Pension Fund (LPF); Sean Reid, Compliance and Risk Manager (LPF); Kirsten Smith, Compliance and Risk Manager (LPF); Susan Handyside, Governance Manager (LPF) | **Implementation Date:**<br>31 March 2023 |

| **3. Risk management training for new starts** | **Low** |
|---|---|

The current LPF new start induction process does not include risk management training.

Risk management training is available and was rolled out across LPF via the ComplianceServe portal in Q1 2021 with a completion deadline of Q1 (31 March 2021). Training records show that 69 employees completed the training (65 by the deadline of 31 March 2021, 3 completed in early April and one in October 2021).

**Risk**

The potential risks associated with our findings are:

- New LPF employees may not be aware of the LPF risk management framework and their responsibilities for risk within the organisation.
- LPF could be exposed to risks that are not identified and effectively managed.

**3.1 Recommendation: Risk management training for new starts**

Management should consider how new LPF employees can receive an appropriate level of risk management framework training as part of the induction process.

This could include an assessment on whether the risk management e-learning module on the ComplianceServe portal could be completed at induction process in addition to the ongoing annual training completed by existing employees.

**3.1 Agreed Management Action: Risk management training for new starts**

We will look to build in the proposed new overarching risk management policy into our induction and onboarding procedures to address this finding.

| | |
|---|---|
| **Owner**: Richard Carr, Interim Executive Director, Corporate Services<br><br>**Contributors**: Hugh Dunn, Service Director, Finance and Procurement; David Vallery, Chief Executive, Lothian Pension Fund (LPF) ; Sean Reid, Compliance and Risk Manager (LPF); Kirsten Smith, Compliance and Risk Manager (LPF); Susan Handyside, Governance Manager (LPF) | **Implementation Date:**<br>30 September 2022 |

# Appendix 1: Basis of our classifications

| Finding rating | Assessment rationale |
|---|---|
| **Critical** | A finding that could have a:<br>• ***Critical*** impact on the operational performance; or<br>• ***Critical*** monetary or financial statement impact; or<br>• ***Critical*** breach in laws and regulations that could result in material fines or consequences***; or***<br>• ***Critical*** impact on the reputation of the Council which could threaten its future viability. |
| **High** | A finding that could have a:<br>• ***Significant*** impact on operational performance; or<br>• ***Significant*** monetary or financial statement impact; or<br>• ***Significant*** breach in laws and regulations resulting in significant fines and consequences***; or***<br>• ***Significant*** impact on the reputation of the Council. |
| **Medium** | A finding that could have a:<br>• ***Moderate*** impact on operational performance; or<br>• ***Moderate*** monetary or financial statement impact; or<br>• ***Moderate*** breach in laws and regulations resulting in fines and consequences; or<br>• ***Moderate*** impact on the reputation of the Council. |
| **Low** | A finding that could have a:<br>• ***Minor*** impact on operational performance; or<br>• ***Minor*** monetary or financial statement impact; or<br>• ***Minor*** breach in laws and regulations with limited consequences; or<br>• ***Minor*** impact on the reputation of the Council. |
| **Advisory** | A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice. |

# Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives included in the review are:

| Audit Area | Control Objectives |
|---|---|
| Governance | • There is a clearly defined risk strategy that outlines how effective risk management will support achievement of organisational objectives, including both strategic and operational decision making.<br>• LPF's risk appetite and tolerance levels have been defined and agreed by the Committee.<br>• The organisation's risk profile is linked to, and informs, the business planning and corporate strategy setting processes, with risk being understood and (where appropriate and material) discussed as part of the processes.<br>• Risk is considered as part of significant strategic and operational decisions.<br>• Committee terms of reference include their responsibilities for scrutiny and oversight of the LPF risk appetite; risk profile; and established risk management processes.<br>• All sets of committee papers include appropriate consideration of associated material risks as informed by the LPF Risk Appetite and Tolerances statement. |
| Policy, roles and responsibilities | • There is an up to date risk management policy in place that aligns with LPF's risk management strategy and is regularly refreshed and reviewed and approved by senior management.<br>• LPF's risk management policy and processes set out the framework and approach for the consistent and effective management of risk.<br>• The risk management strategy, policy and processes are made available and clearly communicated to all employees.<br>• Risk management roles and responsibilities (including those of the relevant committees; LPF's Chief Executive; senior and operational management) are clearly defined, understood and communicated throughout the organisation.<br>• Third party contracts for outsourced services include clear third party responsibilities for escalating any relevant risks to LPF. |
| Risk identification and assessment | • Identification of risks is focussed on what could prevent achievement of the strategy.<br>• There is a consistent way in which risks are described and documented.<br>• Ownership of risks is clearly defined at an appropriate level.<br>• Risks are identified, assessed, managed and reported in accordance with established risk management policy and processes.<br>• Operational risk registers are maintained by all key functions across LPF.<br>• Risk registers include an appropriate assessment of any relevant third party risks for key outsourced processes, including provision of technology systems. |

| Audit Area | Control Objectives |
|---|---|
| Risk treatment and contingency planning | ● There is a formal, consistent risk identification and assessment approach, using defined impact and likelihood criteria.<br>● There is a consistent approach applied supporting identification; documentation and assessing the effectiveness of established controls and new controls and mitigations implemented to treat the risks identified.<br>● Control and action owners are clearly identified. |
| Monitoring, escalation and reporting | ● There is a clearly defined process for reviewing and updating risk registers on a regular basis across LPF.<br>● There is a clearly defined process that supports the collation and assessment of enterprise / organisational risks based on consideration (and if appropriate aggregation) of underlying operational risks.<br>● There is a defined process and criteria for escalating risks to the appropriate senior management and governance forums that is consistently applied.<br>● There is concise and timely, reporting of accurate risk information, through all levels of the organisation and to relevant committees, that supports risk-informed decision making.<br>● An appropriate process has been established to support escalation of relevant LPFI and LPFE risks to LPF management and relevant committees. |
| Training and awareness | ● The second line risk management team has the appropriate skills and experience to perform their risk management responsibilities appropriately.<br>● Training and further support on risk management is available to all employees.<br>● Completion and attendance of risk management training is monitored and followed up to ensure all LPF staff are aware of their responsibilities for risk management.<br>● LPF's approach to risk management is clearly conveyed through appropriate and accessible documentation, tools, guidance materials and training. |

# Appendix 3: Documenting controls - best practice and insight

**A definition of a key control**

*"Controls that are fundamental to the success of an operation, upon which others depend. They cover areas of highest risk and strategic importance. A key control is therefore one which is essential to achieve the system of control objective and the absence of which would lead to material or significant loss, harm, failure, or error".*

**Documenting controls**

Documenting controls appropriately is a key skill that will help ensure consistency of understanding of the nature and consequences of the risk, its rating to the business and the actions that should be pursued to improve the controls to mitigate the risk. There are 5 key things include when writing up a control:

| | | |
|---|---|---|
| **Who?** | **Who is responsible for performing the control?** | The **Retrospective PO report is reviewed monthly** by the **financial controller** to **ensure that spend is appropriate**. The report **should be signed and dated as evidence of review and expectations followed up accordingly.** |
| **What?** | **What are the overarching components of the control being performed?** | |
| **When?** | **How often does the control take place?** | |
| **Why?** | **Why is the control in place?** | |
| **How?** | **How is the control performed and evidenced?** | |

There are also some common pitfalls to watch out for:

- Use of an individual's name but not title/role;
- Reference to 'the system', but not specifying what this system is;
- Overly long and unclear narratives that describe the process instead of the control;
- Not documenting thresholds that are in place; and
- Forgetting to describe how 'errors' are handled.