



## **Pensions Committee**

2.00pm, Wednesday, 7 December 2022

### **Risk Management Summary**

#### **1. Recommendations**

---

The Pensions Committee (Committee) is requested to:

- 1.1 note the LPF group's Risk Register and Quarterly Risk Overview, and raise any relevant points arising from the review with the Pensions Committee on 7 December; and
- 1.2 note the intention for the CRO to lead a review of LPF's current Risk Management Framework during 2023, making enhancements to existing arrangements and embedding any improvements as appropriate.

**Kerry Thirkell**

Chief Risk Officer, Lothian Pension Fund

Contact: Kerry Thirkell, Chief Risk Officer, Lothian Pension Fund

E-mail: [lpfgovernancecomms@lpf.org.uk](mailto:lpfgovernancecomms@lpf.org.uk) | Tel: 0333 996 1900

# Risk Management Summary

## 2. Executive Summary

---

- 2.1 This paper provides an overview of monitoring and assurance arrangements operating in LPF during 2022, noting any material observations or exceptions.
- 2.2 This paper also provides the background driving the intention to review the current Risk Management Framework.

## 3. Background

---

- 3.1 Having been in role for approximately 3 months now, initial observations of the new CRO focus around people being at the heart of LPF, demonstrated through quality of care for members, as well as for staff. The diligence and dedication that manifests in high level customer care and service to members and employers, as well as genuine care, support and empathy for staff, all embody LPF's vision and values.
- 3.2 With that in mind, ensuring that LPF continues to meet these standards, and continues to do so within an appropriately robust, pragmatic and flexible Risk Management Framework that meets the expectations and requirements of members, clients and regulators is critical. The green rated Internal Audit review on Risk Management in August is a reassuring assessment on current arrangements, and observations and recommendations from this review, together with the Mercer Operational Risk Review (noted below) will be factored into a broader review and uplift of the Risk Management Framework. Enhancements to this framework will help ensure that LPF are able to operate and demonstrate an appropriate and effective control environment which continues to facilitate and support the forward looking business strategy and objectives.
- 3.3 It is also encouraging to note the achievements and other deliverables during 2022 in respect of the risk, regulatory and control environment at LPF, summarised below. Whilst scope for improvement of processes and controls exists within most firms, a sound risk culture which supports positive behaviours in respect of managing risks to the operation of the Fund, is evident at LPF.

## **4. Monitoring & Assurance Summary**

---

### **BDO Compliance Monitoring Programme ('CMP')**

- 4.1 Throughout the year, BDO have continued to provide routine and ad hoc assurance on behalf of the LPF Risk & Compliance team regarding FCA regulatory compliance requirements for LPFI. Findings are discussed between the Risk & Compliance team and BDO, and actions have been agreed with appropriate business owners as required. These findings are recorded and tracked by the Risk & Compliance team to conclusion and have been reported to management on a quarterly basis during the year. We have observed some common themes on the findings in relation to inadequate documentation, policies and procedures necessary to support and compliment the effective operation of processes and controls. The Risk & Compliance team continue to provide advice and guidance to those business areas where improvements are required.

### **Mercers Systems & Controls Review**

- 4.2 An operational risk review on LPFI was completed in Q1. The purpose of the review focused on systems and controls in place in relation to management of the Fund, covering governance and operational functions which support the investment activities of LPFI. Although satisfactory controls were noted across the firm, several observations were made regarding operational enhancements to the control environment. Appropriate and proportionate actions plans have been agreed with relevant LPF stakeholders and these items are being tracked and reported by the Risk & Compliance team and will be taken into account as appropriate during the review of the Risk Management Framework.

### **Non-FCA Compliance Monitoring Programme ('CMP')**

- 4.3 A broader reaching CMP has been developed during Q4 to provide more substantive oversight and assurance in respect of non-FCA regulatory requirements, predominantly covering The Pensions Regulator ('tPR') requirements. Assurance around tPR compliance was previously provided through compliance attestations with relevant LPF staff, and the move to independent second line monitoring is considered a more effective, robust and objective method of oversight. We expect to develop this complimentary monitoring further during the course of 2023 and meanwhile the results will be reported a quarterly basis.

### **FCA Regulatory Compliance: Variation of Permission**

- 4.4 The Risk & Compliance team worked closely with the Investments and ICT functions during the year to ensure that we were able to articulate and demonstrate appropriate systems and controls within the firm that would support the proposed increase to the assets under management (AuM) by the removal of the private

restriction on AuM. The completion of testing and implementation of the Charles River Front Office Order Management System (CRIMS) and its ongoing assurance, in addition to the new IT arrangements delivered through a managed service provided by Cased Dimensions, supported the successful application to the FCA. FCA granted a Variation of Permission to LPFI on 21 September allowing us to actively engage with Fife and Falkirk in respect of further executing their chosen strategies. Prior to this confirmation, supplementary short term controls had been set up within CRIMS to manage our proximity to the AuM restriction, to ensure the threshold was not breached. In addition, the Investment team worked diligently during this period so they were able to anticipate and be ready to react to any possible actions or market movements which could inadvertently result in these thresholds being breached. No AuM restriction breaches occurred during this period.

#### **FCA Regulatory Compliance: ICARA**

- 4.5 LPFI is required to hold adequate financial resources (also referred to as regulatory capital or capital adequacy) and to establish systems and controls to manage potential harms. The FCA rules on this were previously known as the Internal Capital Adequacy Assessment Process (ICAAP), and in 2022 were replaced by the Internal Capital Adequacy and Risk Assessment (ICARA). These systems and controls must include a process to assess and allocate additional capital where a residual, material risk remains.
- 4.6 The Risk & Compliance team coordinated completion of the LPFI ICARA, collaborating with the Finance function and supported throughout the process by BDO. A workshop to provide training to the LPFI board and other stakeholders, as well as facilitate feedback on key risks and assumptions to be taken into account in the new model, took place in June and the LPFI risk register helped to inform the assessment of any additional capital allocations under ICARA. Whilst LPFI's ICARA data was submitted as required to the FCA on 30 September, the supporting documentation does not require formal submission, but rather requires to be maintained by regulated firms, and updated as required to reflect material changes to business profile and identified risks. Consequently the Risk & Compliance and Finance teams will be reviewing the current document to take account of the removal of the private restriction on AuM, as well as developing supporting policies and procedures.

#### **Information Governance**

- 4.7 The Information Governance framework has been reviewed during the year, following recommendations for improvement by CEC's Information Governance Unit (IGU). IGU have provided input and recommendations on the new framework. In Q2 2022, enhanced data protection policies and related procedures were implemented, and LPF-wide data protection training carried out. Confirmation has been sought from CEC that recommendations have been satisfactorily addressed. Further training

and establishing regular monitoring is expected to be carried out in Q4 2022. Information Governance is a pending Internal Audit review in Q1 2023.

### **Supplier Management**

- 4.8 Improvements to the Third Party Supplier Management framework have been introduced during the course of the year, with clearer governance, ownership and checks and controls introduced. An updated policy was published and communicated to colleagues in June and embedding of the policy requirements and supporting processes and controls is underway. The pending Internal Audit review in Q1 2023 will provide an opinion on the design and operational embeddedness of the framework and highlight any further areas where improvements could be made.

### **Issues & Incidents**

- 4.9 Enhancements have been made to the recording and reporting of issues and incidents which facilitates a more integrated approach to risk management. This allows for themes and trends to be timeously identified and acted upon before a risk crystallises into an event requiring remediation. The Risk & Compliance team continue to work with business stakeholders to promptly remediate incidents and ensure preventative actions are taken where required, and actively track the completion of open issues, which have either been identified by business areas themselves, or relate to findings from Line 2 or Line 3 reviews.
- 4.10 At the time of writing, there are no open incidents. A small spike in the number of incidents that have required regulatory submissions to be corrected, or completed, having been missed has been observed over the second half of the year, although these are all relatively immaterial in nature. We do not expect this trend to continue, and in fact, most of these were self-identified and reflect the positive risk culture within the organisation with staff identifying, escalating and remediating errors themselves.
- 4.11 There are currently 65 open issues. 51 of these have a completion date of 31 December and we are confident that business owners are on track to complete these actions by their due dates. Of these 51, 9 are with regard to Internal Audit findings which have either been completed but awaiting CEC review, or are in train to complete; 14 relate to information security matters identified by Bridewell; and 11 are regarding CEC IGU findings, which are completed but awaiting on confirmation of closure from CEC. 5 issues are overdue and revised action dates have been agreed with owners as appropriate, having considered rationale for any delay to close.

## **5. Financial impact**

---

- 5.1 There are no direct financial implications as a result of this report.

## **6. Stakeholder/Regulatory Impact**

---

- 6.1 The Pension Board, comprising employer and member representatives, is integral to the governance of the fund and they are invited to comment on the relevant matters at Committee meetings.
- 6.2 Except as otherwise stated in the report itself, there are no adverse health and safety, governance, compliance or regulatory implications as a result of this report.

## **7. Background reading/external references**

---

- 7.1 None.

## **8. Appendices**

---

Appendix 1 – Quarterly Risk Summary as at 9 November 2022





# **Quarterly Risk Overview**

**07 Nov 2022**

## Executive Summary

This document provides a summary of the assessment of the LPF group's risks by the Risk Management Group (RMG) on 07 Nov 2022. The RMG reviews the LPF group risk register on at least a quarterly basis.

Changes to risk register since 22 Aug 22:

- **Risk 9 – Pension Committee decisions.** Risk score improved from 30 to 24, moderate to low. Onboarding and training completed for all new committee members, to ensure sufficient knowledge and understanding of the pension scheme.
- **Risk 39 – Power outages.** New risk added. Risk of energy outages caused by planned or unforeseen blackouts, leading to operational disruption. Risk impact and probability currently assessed as low, as LPF's blended model and existing business continuity processes are judged sufficient to mitigate at the moment. Developments will remain under review.

No risks have been closed, and no risk scores have deteriorated.

### Risk Register at 07 Nov 2022

Total risks	High	Moderate	Low
39	0	13	26

See Appendix 2 for full list of risks.

### Summary of Changes since last review :


New	Closed	Improved	Deteriorated	Unchanged
1	0	1	0	37





## Risk Register Update

Update on all 'High' or 'Moderate' risks, detailing the risk score (0-100), any score changes since last report, and a narrative explanation on the current score and mitigating plans.











New risks added:













Risk	Score	Movement	Update
<b>39. Power outages</b>  Risk of energy outages caused by planned or unforeseen blackouts, leading to operational disruption.	  16	N/A - new	Emerging risk raised at RMG Nov 22, regarding potential for national or local power outages. Potential impact on office availability or ability for staff to work remotely. Blended model helps to mitigate. All key systems and applications are cloud-based rather than servers. Existing business continuity measures judged sufficient at present, no further mitigating actions planned at present. Will remain under review.





Scoring changes:

Risk	Score	Movement	Update
<b>9. Pension committee decision-making</b>  Pension committee (or other) members take decisions against sound advice, on political grounds or due to lack of knowledge	  25	  Improved	Reduced following completion of onboarding and induction for new committee members. Previously elevated due to elections in May 22 resulting in new pension committee members and requirement for training. LPF have taken steps to mitigate i.e. onboarding and engagement plans for new committee members to ensure knowledge and understanding of fund activities.

Commentary on all remaining high or moderate risks:

Risk	Score	Movement	Update
<b>36. Cybersecurity</b> Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	 32	 Unchanged	<p>Independent cyber security maturity assessment completed in Dec 2021. Concluded that current state has “features of higher-level maturity” but recommended enhancements on defined processes, such as incident response plans. These are being addressed by an action plan, expected to completed Dec 2022.</p> <p>External phishing testing carried out in Oct 22. Results that technical security controls work well; but staff ability to identify and report suspicious emails could be improved. Training and communications will be carried out to increase awareness. Once done, further phishing tests will be carried out and score reconsidered.</p>
<b>38. Project and change</b> Project and change activities not effectively managed	 32	 Unchanged	<p>It is currently rated Amber due to Project Forth timeline but will be kept under review as project progresses.</p>
<b>27. Governance</b> Group structure and governance not fully compliant and up-to-date or working effectively	 30	 Unchanged	<p>Recent elections increased probability of disruption to the schedule of committee meetings, and timing of decisions. The score has improved as committee membership has been confirmed, dates scheduled, and induction training for new members complete. LPF governance structure is in process of further improvement in order to work effectively – including a new governance portal, and transfer of committee services from CEC to LPF. Risk will remain elevated until portal and SLA are in place.</p>
<b>20. Regulatory Breach</b> Failure to comply with applicable laws and regulations	 30	 Unchanged	<p>Risk remains higher to reflect the increased regulatory burden from FCA-regulated investment services, including new processes required by IFPR requirements. New compliance monitoring processes will improve assurance activities.</p>
<b>21. Information Rights</b> FOI and subject rights processes not in accordance with laws and regulations	 30	 Unchanged	<p>Score is elevated while an Information Governance project is underway. This will review and improve processes around information rights, records management, and retention.</p>

Risk	Score	Movement	Update
<b>23. Delegations</b> Acting beyond proper authority / delegations.	 30	 Unchanged	<p>A review and refresh of the Scheme of Delegations is underway, to clearly map them to the functions within the LPF group.</p> <p>Score unchanged while mitigating actions are in process - the risk remains amber, although there has been no breach in existing delegations.</p>
<b>25. Procurement</b> Breach of procurement/framework regulations	 30	 Unchanged	<p>LPF is continuing to work with CEC to align procurement processes to the needs of LPF group business while also satisfying CEC's oversight requirements.</p> <p>Score will be reviewed and likely reduce Q1 2023 once an updated Contracts Standing Order (CSO) confirmed in place. This will ensure appropriate actions including procurement compliance in respect of LPF's contract letting.</p>
<b>33. Staff Resource</b> Staff Resource within the Fund not sufficient to carry out core tasks	 30	 Unchanged	<p>Score is Amber to reflect the increasing burden on existing staff from Project Forth, assurance activities, and other organisational development projects and change initiatives. Successful recruitment has taken place in a number of areas.</p>
<b>3. Employer contributions</b> Failure of an employer to pay contributions causes either a significant fall in funding level or requires higher contributions from other employers	 28	 Unchanged	<p>Employers continue to be under increasing financial pressure due to the current economic situation. The fund continues to monitor this on an ongoing basis with regular employer contact and existing controls.</p>
<b>4. Recruitment</b> Failure to recruit, engage and retain talent leads to workforce capability gaps with implications for oversight, control, administration and achievement of service plan goals	 28	 Unchanged	<p>Unchanged. There has been successful recruitment in a number of areas however it is a candidate market, particularly in more technical roles, leading to the fund incurring more recruitment related costs.</p>
<b>1. Investment performance</b> Adverse investment performance causes funding levels to fall requiring higher employer contributions	 25	 Unchanged	<p>JISP advisers and asset allocation and policy group investment committees have been meeting frequently to ensure the Pension Committee's investment strategy is implemented within prescribed constraints, and to respond to material market changes, such as the September 2022 dislocation in the gilts market.</p>

Risk	Score	Movement	Update
<b>2. Adverse Movement - pressure on employer contributions</b> Adverse change in non-investment actuarial assumptions causes either funding levels to fall or requiring higher employer contributions	 25	 Unchanged	The employer contribution rates approach has changed from deterministic to risk-based, with Funding Strategy Statement updated and employers consulted and informed.
<b>35. Supplier and third-party systems</b> Inadequate, or failure of, supplier and other third-party systems (including IT and Data security).	 25	 Unchanged	Our supplier management processes have been reviewed, and a risk-based framework implemented to ensure greater consistency across providers. Score will remain Amber until we have carried out assurance that processes are working as expected.

## Appendix 1 – Risk Scoring & Distribution Chart

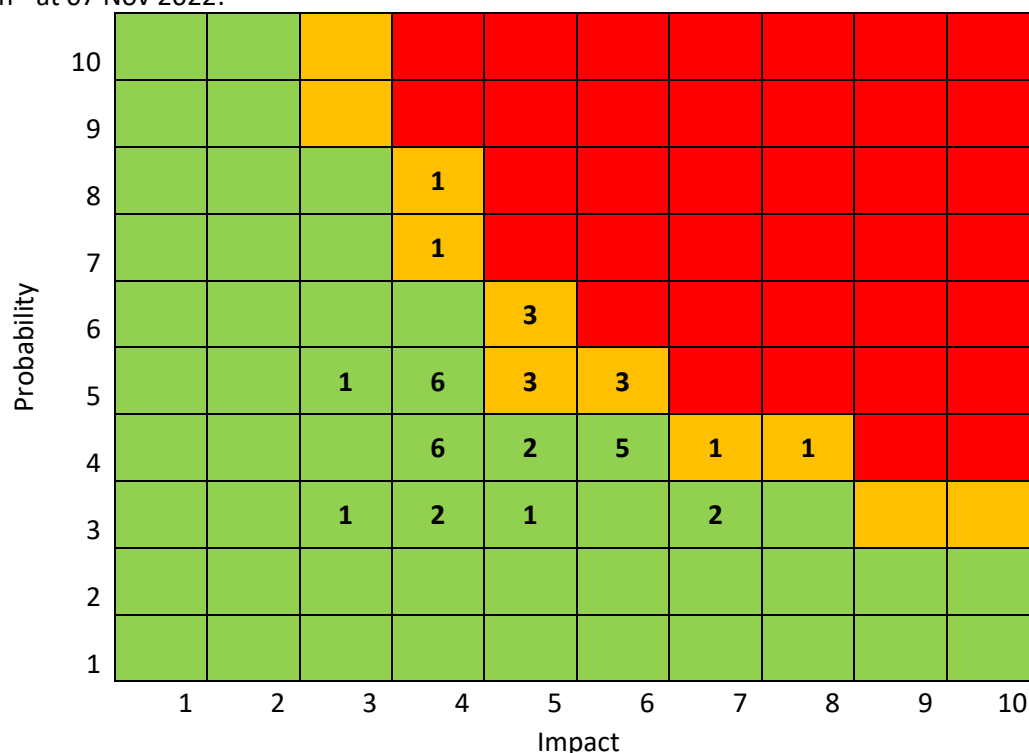
Risk scoring:

	Impact	Probability
1	No discernible effect	Virtually impossible
2	Little discernible effect	Extremely unlikely
3	Some effect noticeable	Remotely possible
4	Some effect on service provision	May occur
5	Noticeable effect on service provision	Fairly likely to occur
6	Some disruption of service	More likely to occur than not
7	Significant service disruption	Likely to happen
8	Material disruption to services	Probably will happen
9	Major service disruption	Almost certainly will happen
10	Catastrophic	Already happening

RAG (Red Amber Green) status:

Risk Status	
<span style="background-color: red; color: black;"> </span>	High: resolve urgently where possible (probability and impact total 35 and above)
<span style="background-color: orange; color: black;"> </span>	Moderate: resolve where possible (probability and impact total 25 to 34)
<span style="background-color: green; color: black;"> </span>	Low: monitor (probability and impact total 24 and below)

Risk Distribution - at 07 Nov 2022:



## Appendix 2 – Risk Register

Full risk register Red Amber Green (RAG) status at 07 Nov 2022:

Ref	Risk	RAG
1	Investment Performance	
2	Adverse Movement - pressure on employer contributions	
3	Failure of an employer to pay contributions	
4	Recruitment & retention	
5	Fraud by LPF staff or relating to members	
6	Staff competence	
7	IT systems	
8	Culture & engagement	
9	Pension Committee decisions	
10	Pension Board effectiveness	
11	Business continuity	
12	Data protection	
13	Responsible Investment	
14	Incorrect pension payments	
15	Late payment of pension	
16	Market abuse	
17	Investment operations	
18	Disclosure of confidential information	
19	Material breach of contract	
20	Regulatory breach	
21	Information Rights	
22	Member communications	
23	Acting beyond proper authority/delegations	
24	Inappropriate use of pension fund monies	
25	Procurement/framework breach	
26	Procurement process	
27	Group structure and governance	
28	Claim or liability arising from shared services	
29	Employer systems access	
30	Incorrect member data	
31	Inadequate contractual protection	
32	Over reliance on single core service provider	
33	Staff Resource	
34	Health and safety	
35	Supplier and third-party systems	
36	Cybersecurity	
37	Climate change	
38	Project and change activities	
39	Power outages	

## Appendix 3 – Three-year risk trends

Ref	Risk name	Q1 2020	Q2 2020	Q3 2020	Q4 2020	Q1 2021	Q2 2021	Q3 2021	Q4 2021	Q1 2022	Q2 2022	Q3 2022	Q4 2022
1	Investment Performance	●	●	●	●	●	●	●	●	●	●	●	●
2	Adverse Movement - pressure on employer contributions	●	●	●	●	●	●	●	●	●	●	●	●
3	Failure of an employer to pay contributions	●	●	●	●	●	●	●	●	●	●	●	●
4	Recruitment & retention	●	●	●	●	●	●	●	●	●	●	●	●
5	Fraud by LPF staff or relating to members	●	●	●	●	●	●	●	●	●	●	●	●
6	Staff competence	●	●	●	●	●	●	●	●	●	●	●	●
7	IT systems	●	●	●	●	●	●	●	●	●	●	●	●
8	Culture & engagement	●	●	●	●	●	●	●	●	●	●	●	●
9	Pension Committee decisions	●	●	●	●	●	●	●	●	●	●	●	●
10	Pension Board effectiveness	●	●	●	●	●	●	●	●	●	●	●	●
11	Business continuity	●	●	●	●	●	●	●	●	●	●	●	●
12	Data protection	●	●	●	●	●	●	●	●	●	●	●	●
13	Responsible Investment	●	●	●	●	●	●	●	●	●	●	●	●
14	Incorrect pension payments	●	●	●	●	●	●	●	●	●	●	●	●
15	Late payment of pension	●	●	●	●	●	●	●	●	●	●	●	●
16	Market abuse	●	●	●	●	●	●	●	●	●	●	●	●
17	Investment operations	●	●	●	●	●	●	●	●	●	●	●	●
18	Disclosure of confidential information	●	●	●	●	●	●	●	●	●	●	●	●
19	Material breach of contract	●	●	●	●	●	●	●	●	●	●	●	●
20	Regulatory breach	●	●	●	●	●	●	●	●	●	●	●	●
21	Information Rights	●	●	●	●	●	●	●	●	●	●	●	●
22	Member communications	●	●	●	●	●	●	●	●	●	●	●	●
23	Acting beyond proper authority/delegations	●	●	●	●	●	●	●	●	●	●	●	●
24	Inappropriate use of pension fund monies	●	●	●	●	●	●	●	●	●	●	●	●
25	Procurement/framework breach	●	●	●	●	●	●	●	●	●	●	●	●
26	Procurement process	●	●	●	●	●	●	●	●	●	●	●	●
27	Group structure and governance	●	●	●	●	●	●	●	●	●	●	●	●
28	Claim or liability arising from shared services	●	●	●	●	●	●	●	●	●	●	●	●
29	Employer systems access	●	●	●	●	●	●	●	●	●	●	●	●
30	Incorrect member data	●	●	●	●	●	●	●	●	●	●	●	●
31	Inadequate contractual protection	●	●	●	●	●	●	●	●	●	●	●	●
32	Over reliance on single core service provider	●	●	●	●	●	●	●	●	●	●	●	●
33	Staff Resource	●	●	●	●	●	●	●	●	●	●	●	●
34	Health and safety	●	●	●	●	●	●	●	●	●	●	●	●
35	Supplier and third-party systems	●	●	●	●	●	●	●	●	●	●	●	●
36	Cybersecurity	●	●	●	●	●	●	●	●	●	●	●	●
37	Climate change	●	●	●	●	●	●	●	●	●	●	●	●
38	Project and change activities	●	●	●	●	●	●	●	●	●	●	●	●
39	Power outages	●	●	●	●	●	●	●	●	●	●	●	●