



# **Pensions Audit Sub Committee**

2.00pm, Tuesday, 27 September 2022

## **Risk Management Summary**

### **1. Recommendations**

---

The Pensions Audit Sub Committee (Committee) is requested to:

- 1.1 note the Quarterly Risk Overview as at 22 August 2022.

**Kerry Thirkell**

Chief Risk Officer, Lothian Pension Fund

Contact: Sean Reid, Compliance and Risk Manager, Lothian Pension Fund

E-mail: [Rei97S22@lpf.org.uk](mailto:Rei97S22@lpf.org.uk) | Tel: 0333 996 1964

# Risk Management Summary

## 2. Executive Summary

---

- 2.1 In line with the Lothian Pension Fund's (**LPF**) ongoing risk management procedures, this paper provides an overview of LPF's risk analysis arising from the meeting of the Risk Management Group on 22 August 2022.
- 2.2 LPF's Senior Leadership Team (**SLT**) have reviewed the Quarterly Risk Overview.
- 2.3 LPF's current Chief Risk Officer, Struan Fairbairn, finishes on 14 September. Kerry Thirkell started on 22 August and, following a handover process, will take over CRO responsibilities from 15 September. FCA approval for LPFI specific responsibilities is pending.
- 2.4 The CRO role has altered and is now a focussed risk and compliance role, with governance and legal moving to the responsibility of the CEO.
- 2.5 This paper has been prepared under oversight of outgoing CRO.

## 3. Background

---

- 3.1 LPF's risk management procedures require it to:
  - 3.1.1 maintain a detailed operational risk register which sets out all the risks identified and assessed by the officers on an ongoing basis against the group's risk appetite, the degree of risk associated in each case and the action taken to mitigate those risks (the **Operational Risk Register**); and
  - 3.1.2 produce a summary report of the risk register for the Committee and the Pensions Committee which highlights the material risks facing the group and identifies any new risks/concerns and the progress being made over time by the officers in mitigating the relevant risks (the **Quarterly Risk Overview**).
- 3.2 The Conveners and Independent Professional Observer receive a copy of the full risk register every quarter.
- 3.3 The Audit Sub Committee reviews the full risk register on an annual basis as part of its in-depth review in December, which also includes a review of the group's overall risk assurance analysis and risk appetite statement.
- 3.4 The LPFI Limited (**LPFI**) and LPFE Limited (**LPFE**) boards consider their own risks separately and, in the case of LPFI, in line with the regulatory requirements of the Financial Conduct Authority. However, material risks relating to these operational subsidiaries do feed into the overarching group risk management process to the

extent appropriate. The Committee also receives a separate update on the operations of those underlying operational subsidiary companies.

#### **4. Main Report**

---

- 4.1 The Quarterly Risk Overview as at 22 August 2022 (**Appendix 1**) is included for the Committee's consideration.
- 4.2 There is largely no change in risk exposure across the group with two risks (governance and data protection) improving over the period and no risks worsening.
- 4.3 With the introduction from 1 January 2022 of a revised investment firm prudential regime that applies to LPFI, we have prepared the first ICARA report and subject to final checking this confirms that LPFI remains adequately capitalised. The report is expected to be submitted to the regulatory authority by 30 September 2022.
- 4.4 The audit of LPF's risk management framework has been completed - see separate Internal Audit Update paper - and concluded that the framework *"is proportionate and adequately designed for the size and structure of LPF and is operating effectively across the organisation"*. Three findings have been raised and will be reviewed and implemented in due course.

#### **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 Overview, as at 22 August 2022



## **Quarterly Risk Overview**

**22 Aug 2022**

## Executive Summary

---

This document provides a summary of the assessment of the LPF group's risks by the Risk Management Group (RMG) on 22 August 2022. The RMG oversees the LPF group risk register, which is reviewed on an ongoing basis by the risk function and at least quarterly by RMG itself.

Risks are managed across the group by existing controls – activities and measures put in place to prevent and detect risks. These controls are subject to ongoing monitoring and assurance. Where further one-off actions are needed to mitigate risks, these actions are managed at an operational level with reporting to, and oversight by, the RMG. This report provides a narrative update on relevant key risks, rather than lists of actions and controls.

## Background

The LPF group risks should be viewed in the context of the following background:

### Project Forth and potential merger

- Project Forth – a potential merger with Falkirk Council Pension Fund – was publicly announced on 24 May 2022.
- Project specific risks are tracked and managed within the project, with an information flow to ensure material risks are taken into account on LPF-group risk register where necessary. The potential impact of Project Forth is therefore being reflected in current risk register scoring and mitigations.

### IT provider and information security

- The group moved to a new IT provider in August 2021. Previously, services were provided as part of CEC's wider IT service. Following a period of bedding in, this is now in ongoing business-as-usual - with systems and day-to-day operations more stable and resilient than previously, and greater control and visibility over any issues.
- A number of assurance activities have been carried out during and post-migration - including penetration testing, data protection impact assessments, an internal audit on LPF's technology model, and a cyber security maturity assessment. Action plans are underway to address recommendations arising from these activities.
- Risk scores on information rights and cyber security are elevated while these actions are underway, and will be re-assessed as they progress.

### Investment management services

- FCA-regulated investment management services were launched in December 2020 for collaborative partners.
- Assets under management have been steadily increasing since, and are expected to increase further over the next 6-12 months as other new portfolios are taken on. This expansion of services may increase operational risks – i.e. day to day operations, resourcing, increased regulatory obligations and monitoring.

## Risk register at 22 Aug 2022

Total risks	High	Moderate	Low
38	0	14	24

See Appendix 2 for full list of risks.

## Changes since last review 23 May 2022

New	Closed	Improved	Deteriorated	Unchanged
0	0	2	0	36

### No new risks added or removed

### 2 risk scores improved since last review:

- **Risk 27 – Governance.** Improved from 35 to 30, High to Moderate. Committee membership has now been confirmed, dates in place, and induction training for new members is underway.
- **Risk 12 – Data Protection.** Improved from 30 to 24, Moderate to Low. Data protection policies refreshed and training carried out for all colleagues.

### No risk scores have deteriorated since last risk review.



















### Other relevant updates

- Material litigation – none











## Detailed 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.

For full list of risks, see Appendix 2.

Risk	Score	Movement	Update
<b>36. Cybersecurity</b> Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	 32	 Unchanged	Independent cyber security maturity assessment completed in Dec 2021. Concluded that current state has "features of higher-level maturity" but highlighted risks on defined processes, incident response, and supply chain management. These are being addressed by an action plan.
<b>38. Project and change</b> Project and change activities not effectively managed	 32	 Unchanged	It is currently rated Amber due to Project Forth but will be kept under review as project deliverables, timelines and resource requirements are clarified.
<b>27. Governance</b> Group structure and governance not fully compliant and up-to-date or working effectively	 30	 Improved	Recent elections had increased probability of disruption to schedule of committee meetings, and timing of decisions. Score improving as committee membership has been confirmed, dates scheduled, and training for new members underway.
<b>9. Pension committee</b> Pension committee (or other) members take decisions against sound advice, on political grounds or due to lack of knowledge	 30	 Unchanged	Elevated due to requirement for training and onboarding of new committee members following recent council elections.  Induction training has begun, and due to complete in September. Score will be reassessed once training finished.
<b>20. Regulatory Breach</b> Failure to comply with applicable laws and regulations	 30	 Unchanged	Risk remains higher to reflect the increased regulatory burden from FCA-regulated investment services, including new processes required by IFPR requirements.
<b>21. Information Rights</b> FOI and subject rights processes not in accordance with laws and regulations	 30	 Unchanged	Score is elevated while an Information Governance project is underway. This will review and improve processes around records management and retention.
<b>23. Delegations</b> Acting beyond proper authority / delegations.	 30	 Unchanged	Score unchanged while mitigating actions are in process - the risk remains amber, although there has been no breach in existing delegations.  A review and refresh of the Scheme of Delegations is underway, to clearly map them to the functions within the LPF group.
<b>25. Procurement</b> Breach of procurement/framework regulations	 30	 Unchanged	The risk is static due to the enhanced impact the procurement regime has on LPF's developing business model (sitting within all of the financial services, pensions and public sector regimes) and the fact that progress on developing new systems, controls and procedures in this area has been hampered by the prevailing circumstance of the last 24 months.  LPF is continuing to work closely with CEC to align procurement processes to the specific needs of the LPF group business and also satisfy CEC's oversight requirements.
<b>33. Resource</b> Staff Resource within the Fund not sufficient to carry out core tasks	 30	 Unchanged	Score is Amber to reflect the increasing burden on existing staff from Project Forth, assurance activities, and other organisational development projects and change initiatives.  An organisational review and additional recruitment has been completed. Governance for Project Forth has been agreed and project is underway, with resource risks tracked within project.



Risk	Score	Movement	Update
<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	Employers continue to be under increasing financial pressure due to the global pandemic and current economic situation. The fund continues to monitor this on an ongoing basis with regular employer contact and existing controls.
<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	Unchanged. There has been successful recruitment in a number of areas however it is a candidate market, particularly in more technical roles. We are incurring more recruitment related costs.
<b>1. Investment performance</b> Adverse investment performance causes funding levels to fall requiring higher employer contributions	 25	 Unchanged	A number of actions have been taken to reflect recent JISP investment strategy review, including adjustments to allocations, and strategy/unitisation reporting to JISP.
<b>2. Actuarial assumptions</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 failure</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

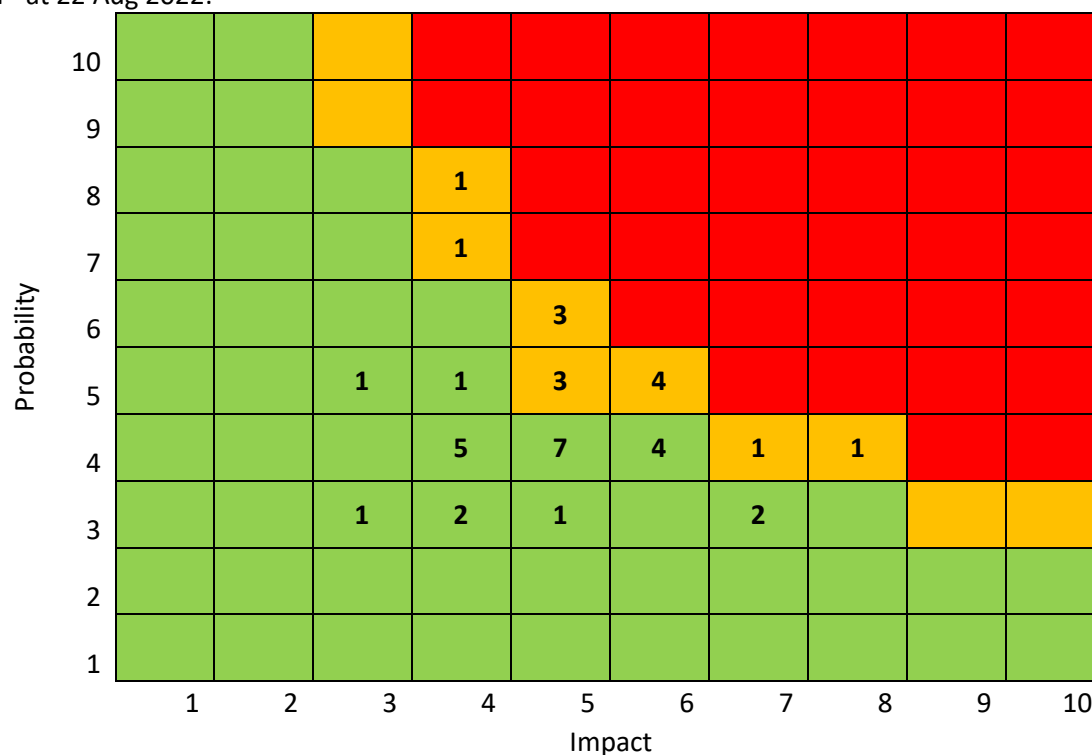
Risk scoring:

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

Risk Distribution - at 22 Aug 2022:



## Appendix 2 – Risk Register

Full risk register Red Amber Green (RAG) status at 22 Aug 2022:

Ref	Risk	RAG
1	Investment Performance causes higher employer contributions	
2	Adverse change in assumptions - pressure on employer contributions	
3	Failure of an employer to pay contributions	
4	Recruitment & retention of staff	
5	Fraud by LPF staff or relating to members (including pension liberation fraud)	
6	Staff negligence, maladministration or lack of specialist knowledge	
7	Failure of IT systems	
8	Staff culture & engagement issues	
9	Pension Committee members take decisions against sound advice	
10	Pension Board not operating effectively	
11	Business continuity issues	
12	Members' confidential data is lost or made public. Breach of Data Protection Act	
13	Compliance with Statement of Responsible Investment Principles	
14	Risk of incorrect pension payments	
15	Late payment of pension	
16	Market abuse by investment team	
17	Portfolio transition issues	
18	Disclosure of confidential information	
19	Material breach of contract	
20	Regulatory breach	
21	Information Rights in accordance with regulations	
22	Incorrect communication with members	
23	Acting beyond proper authority/delegations	
24	Inappropriate use of pension fund monies	
25	Procurement/framework breach	
26	Procurement process compromising ability to secure required resource.	
27	Group structure and governance fully compliant and up-to-date.	
28	Claim or liability arising from shared services	
29	Unauthorised access to employer online system	
30	Incorrect data from Employers leading to fines	
31	Inadequate contractual protection for services	
32	Over reliance on dominant service provider	
33	Staff Resource within the Fund not sufficient to carry out core tasks	
34	Breach of Health and safety regulations	
35	Inadequate, or failure of, supplier and other third-party systems	
36	Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	
37	Climate related operational risks	
38	Project and change activities not effectively managed	

## Appendix 3 – Three-year risk trends

Ref	Risk	Q3 2019/20	Q4 2019/20	Q1 2020/21	Q2 2020/21	Q3 2020/21	Q4 2020/21	Q1 2021/22	Q2 2021/22	Q3 2021/22	Q4 2021/22	Q1 2022/23	Q2 2022/23
1	Investment Performance causes higher employer contributions	●	●	●	●	●	●	●	●	●	●	●	●
2	Adverse change in assumptions - pressure on employer contributions	●	●	●	●	●	●	●	●	●	●	●	●
3	Failure of an employer to pay contributions	●	●	●	●	●	●	●	●	●	●	●	●
4	Recruitment & retention of staff	●	●	●	●	●	●	●	●	●	●	●	●
5	Fraud by LPF staff or relating to members (including pension liberation fraud)	●	●	●	●	●	●	●	●	●	●	●	●
6	Staff negligence, maladministration or lack of specialist knowledge	●	●	●	●	●	●	●	●	●	●	●	●
7	Failure of IT systems	●	●	●	●	●	●	●	●	●	●	●	●
8	Staff culture & engagement issues	●	●	●	●	●	●	●	●	●	●	●	●
9	Pension Committee members take decisions against sound advice	●	●	●	●	●	●	●	●	●	●	●	●
10	Pension Board not operating effectively	●	●	●	●	●	●	●	●	●	●	●	●
11	Business continuity issues	●	●	●	●	●	●	●	●	●	●	●	●
12	Members' confidential data is lost or made public. Breach of Data Protection Act	●	●	●	●	●	●	●	●	●	●	●	●
13	Compliance with Statement of Responsible Investment Principles	●	●	●	●	●	●	●	●	●	●	●	●
14	Risk of incorrect pension payments	●	●	●	●	●	●	●	●	●	●	●	●
15	Late payment of pension	●	●	●	●	●	●	●	●	●	●	●	●
16	Market abuse by investment team	●	●	●	●	●	●	●	●	●	●	●	●
17	Portfolio transition issues	●	●	●	●	●	●	●	●	●	●	●	●
18	Disclosure of confidential information	●	●	●	●	●	●	●	●	●	●	●	●
19	Material breach of contract	●	●	●	●	●	●	●	●	●	●	●	●
20	Regulatory breach	●	●	●	●	●	●	●	●	●	●	●	●
21	Information Rights in accordance with regulations	●	●	●	●	●	●	●	●	●	●	●	●
22	Incorrect communication with members	●	●	●	●	●	●	●	●	●	●	●	●
23	Acting beyond proper authority/delegations	●	●	●	●	●	●	●	●	●	●	●	●
24	Inappropriate use of pension fund monies	●	●	●	●	●	●	●	●	●	●	●	●
25	Procurement/framework breach	●	●	●	●	●	●	●	●	●	●	●	●
26	Procurement process compromising ability to secure required resource.	●	●	●	●	●	●	●	●	●	●	●	●
27	Group structure and governance fully compliant and up-to-date.	●	●	●	●	●	●	●	●	●	●	●	●
28	Claim or liability arising from shared services	●	●	●	●	●	●	●	●	●	●	●	●
29	Unauthorised access to employer online system	●	●	●	●	●	●	●	●	●	●	●	●
30	Incorrect data from Employers leading to fines	●	●	●	●	●	●	●	●	●	●	●	●
31	Inadequate contractual protection for services	●	●	●	●	●	●	●	●	●	●	●	●
32	Over reliance on dominant service provider	●	●	●	●	●	●	●	●	●	●	●	●
33	Staff Resource within the Fund not sufficient to carry out core tasks	●	●	●	●	●	●	●	●	●	●	●	●
34	Breach of Health and safety regulations	●	●	●	●	●	●	●	●	●	●	●	●
35	Inadequate, or failure of, supplier and other third-party systems	●	●	●	●	●	●	●	●	●	●	●	●
36	Cybersecurity protections and/or back-up not sufficient	●	●	●	●	●	●	●	●	●	●	●	●
37	Climate related operational risks	●	●	●	●	●	●	●	●	●	●	●	●
38	Project and change activities not effectively managed	●	●	●	●	●	●	●	●	●	●	●	●

## Appendix 4 – Background and Parameters (extract from Risk Register)

---

*The Risk Management Group, and risk register, form part of the LPF group's critical assurance framework, covers all entities within the group and should be read in conjunction with the other forms of assurance set out in LPF's assurance overview document.*

*The register is formally considered by the Risk Management Group quarterly but is also updated on an ad hoc basis where required. The register also takes into account material risks identified by the wider business, including arising from (i) the other oversight groups (e.g. SLT, People, ICT Oversight and/or any relevant project groups), (ii) any prior board, committee and stakeholder feedback, and (iii) compliance monitoring and processes (e.g. breach reporting, whistleblowing).*

*The Risk Management Group itself comprises senior officers of each function within the LPF group, as well as the Senior Leadership Team (SLT). All members are accountable for escalating material risks, with a particular focus on their respective areas, for consideration. If relevant and deemed sufficiently material, the risk will be included in the register and monitored by the risk function in conjunction with the relevant business unit.*

*The approved risk register is tabled and considered by SLT following sign-off to ensure additional oversight and ongoing engagement with any resulting actions. Those actions are tracked and followed up by the LR&C team with the business on an ongoing basis. The risk register is also circulated to the conveners of the Pensions Committee and Audit Sub-Committee, Chair of the Pension Board and Independent Professional Observer on a quarterly basis, with summary analysis and reporting provided to those bodies each quarter. In addition, an in-depth risk report is provided to the Audit Sub Committee annually, which includes a review of the full register.*

*The risk register is a continually evolving document and doesn't purport to be a comprehensive list of every risk or potential exposure to which the LPF group entities are subject or involved in managing. It should therefore continue to be read in the context of the LPF group's overall business strategy, risk appetite and assurance map. The risk register may cross-refer to separate operational project management tools or action trackers which monitor relevant items in more granular detail and for which the business units are accountable.*

*Importantly, that risk appetite and assurance structure will flex to ensure that it continues to be proportionate to the size and nature of the business of the LPF group and also adhere to the following industry best practice principles:*

- *Ensure that the LPF group's risk appetite **aligns with its strategy** and is **set by its senior management team without undue influence** either externally or otherwise across its assurance stack.*
- *Integrates risk as **a key component of the group's management and decision-making** processes, and so through the spine of its governance and operations.*
- *Engenders an **open, 'live' and engaged risk culture** which seeks to pro-actively identify current and future risks for the business, simplifying layers of controls to ensure this is not stifled, and so...*
- ***Not establish or perpetuate systems, controls or processes** which are out of line with, or **disproportionate to, the group's risk appetite**. That can be counterproductive in distracting key focus and resource away from delivering the group's strategy, core function and assurance over a manageable number of critical risks.*
- *Remain **aligned to LPF's existing resources** and organisational development.*
- *Ensure an **effective and independent risk and compliance function** is maintained, as a general principle and in line with the standards of the UK regulated financial services sector.*
- *Ensure appropriate levels of **separation and independence** of each of the **'four lines of defence'**, as a general principle and in line with the standards of the UK regulated financial services sector.*
- *Ensure appropriate levels of **co-operation and information sharing** across the **'four lines of defence'**.*