

Pensions Committee

2.00pm, Tuesday, 22 March 2022

Risk Management Summary

1. Recommendations

The Pensions Committee (Committee) is requested to:

- 1.1 note the Quarterly Risk Overview as at 15 February 2022; and
- 1.2 note the ongoing strategy and development around the group's risk management framework.

Struan Fairbairn

Chief Risk Officer, Lothian Pension Fund

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

E-mail: 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 15 February 2022.
- 2.2 The paper also highlights certain ongoing development initiatives around the risk management framework and context relevant to its design.

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, 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 15 February 2022 (**Appendix 1**) is included for the Committees consideration.

- 4.2 As reported last quarter, the LPF group's risk management framework has been reviewed by a third party (Mercer) as part of a wider Systems and Controls assurance review for LPFI, having also been the subject of a dedicated separate audit by BDO in 2020. The draft report has now been finalised and, regarding risk, concludes that the LPF group has *developed a robust operational risk management framework*. One of the key findings in relation to risk relates to the extent to which the LPF group requires to put in place dedicated 'investment risk' resource to support the investment team around its underlying investment process. LPF's senior management understand the merits of this finding but has taken the view that this is not yet required (on the basis of proportionality and LPF's existing controls and governance in this area) for the LPF group. However, management has recognised that it may well be something that the LPF group, including LPFI, wishes to introduce as its business plan further develops and the scale of FCA regulatory activity grows. The finding will therefore remain under review as part of LPF's ongoing strategic considerations.

The Committee should note that one of the main purposes of this triennial external systems and controls review is, in addition to providing assurance on the current platform, to provide a steer on a forward-looking basis to ensure the group's systems and controls remain aligned, and are in place ahead of, its strategic initiatives.

- 4.3 The group is also currently subject to an internal audit of its risk management framework as part of this year's annual audit plan. This is being carried out by PwC under direction of the City of Edinburgh Council's internal audit team. The fund will report back to the Committee on any relevant findings and, at the time of writing, is involved in engaging with PwC on the fieldwork. The fund has prepared a management update on the development of its risk management function, to support PwC with background and context, and is included here as **Appendix 2** by way of a general update for Committee.

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 15 February 2022

Appendix 2 – Management Overview of LPF Group Risk Framework: Context and Initiatives



Quarterly Risk Overview

15 February 2022

Executive Summary

This document provides a summary of the assessment of the LPF group's risks by the Risk Management Group (RMG) on 15 February 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 wider background and organisational changes:

Project Forth

- The potential impact of Project Forth is being reflected in current risk scoring – particularly, the risk of resource drain on existing staff. This remains under close review as decisions are made and the group's strategy develops.
- A dedicated Programme Director started in January 2022 and formal project governance is being created, with a number of individual workstreams. Project specific risks will be tracked and managed within workstreams as that detailed analysis develops, with an information flow to ensure material risks are taken into account on LPF-group risk register where necessary.
- As part of Project Forth the LPF group is looking to put in place additional stand-alone service reliance in certain key areas (financial ledger/systems, information compliance and governance services). That will provide the group with greater resilience, but the transition to those stand-alone functions in tandem with the merger implementation will present a short term resourcing challenge.

COVID-19 and move to blended model

- The group began operating on a fully remote basis in March 2020, with a number of risks elevated or requiring increased focus due to the pandemic – including operational resilience and business continuity, staff morale, supplier management, fraud and cyber attack.
- In September 2021, a phased return to a 'blended' model commenced, combining in office and remote working. This was suspended in December 2021 in line with government guidance, and recommenced February 2022.
- We expect to move to the next phase – two days physically in office and remainder remote - in March 2022, which will allow for further detailed 'live' operational risk assessments around the new blended model.
- We continue to closely monitor the post-pandemic trend of staff either looking to change jobs or exit the labour market (following a life reassessment) and prioritise the need to reinforce and build LPF group's culture and values to mitigate the potential adverse impact that fully remote working may have had in this area. Additional flexibilities being introduced across the board also broaden the geographical opportunities for staff and to some degree (perhaps only in the short term) potentially negate the competitive advantage of being located in Edinburgh. LPF's turnover currently remains low by comparison to the wider market, but it is perhaps unlikely this can be sustained in light of the current market forces.

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 broadly in ongoing business-as-usual - with systems and day-to-day operations more stable and resilient than previously, and greater control and visibility over systems.

- 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 all recommendations arising from these activities.
- Risk scores on data protection, information rights, IT systems, and cyber security are elevated while these actions are underway, and will be re-assessed as they progress.
- The group is aware that the rising tensions in Eastern Europe, and globally, present a potential risk not just to the fund's investments, but also in other areas of its supply chain and around cyber security. The risk function has been liaising with the Head of IT to ensure that our ongoing activities and engagement with key suppliers takes this into account and our existing security approach (and those of key suppliers) are fully informed.

Investment management services

- FCA-regulated investment management services were launched in December 2020 for collaborative partners.
- Two new portfolios were onboarding during December 2021, bringing the total to three portfolios. Assets under management 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. It is therefore a current priority for the group to ensure the client facing (reporting), back office and compliance processes are fully bedded in for these new services.

Risk register at 15 Feb 2022

Total risks	High	Moderate	Low
38	1	15	22

See Appendix 2 for full list of risks.

Changes since last review 03 Nov 2021

New	Closed	Improved	Deteriorated	Unchanged
1	0	5	3	29

One new risk added:

- **Risk 38 – Project and change risks.** Currently rated Moderate. Added to reflect specific risks arising from Project Forth and other change initiatives and projects, that are not already captured by other risks (e.g. failure to deliver projects on time, staff change “fatigue” etc.). Over the next 12 months this will be primarily driven by Project Forth, but in time will reflect the ongoing suite of project and change activities.

Five risk scores improved since last review:

- **Risk 8 – Culture.** Improved from 30 to 20, Moderate to Low. Line manager training has been completed. Timing of internal colleague communications have been reviewed to take into account staff survey feedback.
- **Risk 9 – Pension committee.** from 30 to 20, Moderate to Low. Previously raised score reflected issue with matters referred outside the Fund’s existing governance structure.
- **Risk 15 – Late payment of pensions.** Improved from 27 to 21, Moderate to Low. Score has been elevated due to AVC delays for a small number of members. Gradually improved, and though it remains slower than 2020, mitigants are in place - such as informing members in retiral packs of possible AVC delays.
- **Risk 16 – Market Abuse.** Improved from 20 to 15, remains Low. Training carried out during Q4 2021, and added to ongoing learning plan. This should ensure relevant colleagues understand legal obligations relating to Market Abuse, and avoid activities that may constitute it.
- **Risk 34 – Health & Safety breach.** Improved from 20 to 16, remains Low. All H&S checks, policies and procedures completed and refreshed ahead of RTO and start of blended model.

Three risk scores deteriorated since last risk review:

- **Risk 4 – Failure to recruit or retain talent.** Deteriorated from 24 to 28, Low to Moderate, to reflect risk identified during remuneration benchmarking process. Recruitment process itself is functioning well, successful recruitment in a number of recent roles.
- **Risk 13 – Failure to comply with Responsible Investment Principles.** Deteriorated from 16 to 20, remains Low. to reflect period of increased focus and potential regulatory change. A project is underway to review climate reporting requirements.
- **Risk 37 – Climate change related risks.** Deteriorated from 9 to 15, remains Low. In addition to climate reporting project, LPF are reviewing feasibility of committing to Edinburgh Climate Compact.

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 narrative:

Risk & reference number	Update
33 - Staff Resource within the Fund not sufficient to carry out core tasks	Score: 36. Unchanged. Score remains high to reflect the increasing burden on existing staff, particularly senior management, from Project Forth, assurance activities, and other organisational development projects and change initiatives. An organisational review was completed and additional recruitment underway in a number of areas. Project design for Forth is also in process.
38 – Project and change risks	Score: 32. New risk. New risk added. The risk that project / change activities lead to delays or failure to deliver on time; change fatigue amongst colleagues; or a detrimental impact on day-to-day operations. Over the next 12 months this will be primarily driven by Project Forth, but in time will reflect the ongoing suite of project and change activities. It is currently rated Amber but will be kept under review as project governance is finalised and clearer timelines and resource requirements emerge.
36 - Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	Score: 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. Escalating global tensions and potential for heightened cyber threat being kept under review. Not impacting our risk scores – existing controls will remain in place regardless of threat.
7 - Failure of IT systems	Score: 30. Unchanged Score unchanged. IT move complete in Aug 21 and score has gradually been reducing. Now in BAU with stable systems and ongoing controls/reports/supplier monitoring to monitor position. This would reduce risks scores from last quarter, but kept as amber until plan created for cyber security review: including internal IT procedures and control framework.
11 - Business continuity issues	Score: 30. Unchanged Remains elevated due to COVID-19 and remote working. Will be reassessed next quarter following full period of hybrid working, and refresh of Business Continuity Plans post ICT migration.
12 - Members' confidential data is lost or made public. Breach of Data Protection Act	Score: 30. Unchanged The Information Governance project is underway to review and address our data protection systems and controls, and this score will be reviewed on completion – expected by end Q1 2022. The Fund is comfortable our systems and controls to protect member data and identify and report breaches are robust. Enhancements are required to fully document existing processes, and to refresh training and awareness amongst colleagues.
	Score: 30. Unchanged

Risk & reference number	Update
21 - Information Rights processes not in accordance with regulations	Score is elevated while an Information Governance project is underway to review and improve processes around records management and retention i.e. not keeping information for longer than is necessary. In particular, we are analysing the control environment around new technology, driven by pandemic innovation and greater use of Teams video calls/hybrid working - as opposed to the traditional call or meeting distinction. A primary focus here is how best to manage and retain data around our call recording systems and regulatory requirements.
23 - Acting beyond proper authority/delegations	<p>Score: 30. Unchanged</p> <p>Score unchanged while mitigating actions are in process - the risk remains amber, although there has been no breach in existing delegations.</p> <p>A review and refresh of the Scheme of Delegations is underway, to clearly map them to the functions within the LPF group.</p>
20 - Regulatory breach	<p>Score: 30. Unchanged</p> <p>Risk remains higher to reflect the increased regulatory burden from FCA-regulated investment services. LPFI compliance monitoring has been enhanced and is picking up minor findings and recommendations, which shows it is working effectively.</p> <p>Score expected to be reviewed after a full annual cycle of LPFI's improved monitoring (Q1-Q2 2022).</p>
25 - Procurement/framework breach	<p>Score: 30. Unchanged</p> <p>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 18 months.</p> <p>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.</p>
27 - Group structure and governance fully compliant and up-to-date	<p>Score: 30. Unchanged</p> <p>Resourcing of committee services under review as part of the Governance Review process. Transitional arrangements are in process to migrate committee administrative support to LPF, but also mindful of the need to establish a stand alone LPF governance unit to support the post-merger environment.</p>
4 - Failure to recruit, engage and retain talent	<p>Score: 28. Deteriorated</p> <p>Deteriorated to reflect risk raised during benchmarking process that some senior remuneration is below market rate. Succession plans have been approved as interim mitigant.</p> <p>Annual performance processes for 2021 have been completed for all colleagues, and 2022 plan has commenced without material change.</p>
3 - Failure of an employer to pay contributions	<p>Score: 28. Unchanged</p> <p>Employers continue to be under increasing financial pressure due to the global pandemic and resulting economic implications. The fund continues to monitor this on an ongoing basis with regular employer contact and existing controls. Admission agreements are subject to review and update following employer covenants review.</p>
1 - Investment Performance pressure on employer contributions	<p>Score: 25. Unchanged</p> <p>A number of actions have been taken to reflect recent JISP investment strategy review, including adjustments to allocations, and strategy/unitisation reporting to JISP.</p>
	Score: 25. Unchanged




Risk & reference number	Update
2 - Adverse Movement - pressure on employer contributions	The employer contribution rates approach has changed from deterministic to risk-based, with Funding Strategy Statement updated and employers consulted and informed.
35 - Inadequate, or failure of, supplier and other third-party systems (including IT and data security).	Score: 25. Unchanged
	We monitor availability for key suppliers, reported to relevant groups. Our supplier management processes are being reviewed, and a risk-based framework will be implemented to ensure greater consistency across providers.

Appendix 1 – Risk Scoring & Distribution Chart

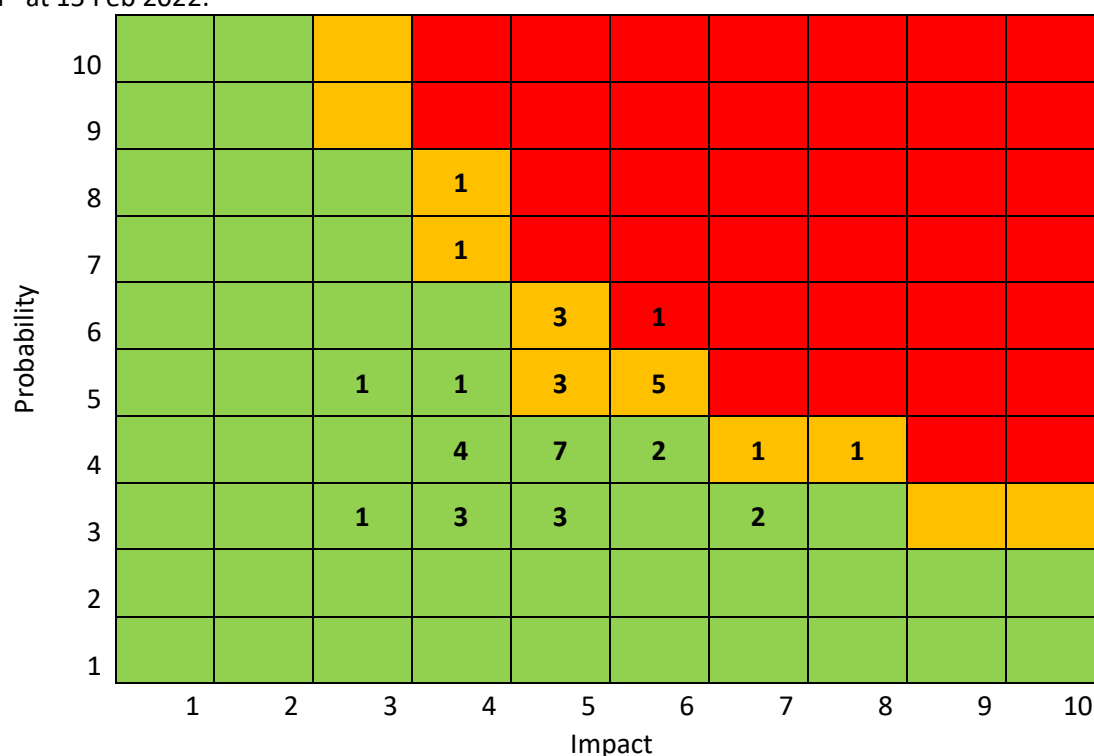
Risk scoring:

	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	
	High: resolve urgently where possible (probability and impact total 35 and above)
	Moderate: resolve where possible (probability and impact total 25 to 34)
	Low: monitor (probability and impact total 24 and below)

Risk Distribution - at 15 Feb 2022:



Appendix 2 – Full Risk Key

Full risk register Red Amber Green (RAG) status at 15 February 2022:

Ref	Risk	RAG
1	Investment Performance pressure on employer contributions	
2	Adverse Movement - 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 (or other) 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 PensionsWEB	
30	Incorrect data from Employers leading to fines	
31	Inadequate contractual protection for services	
32	Over reliance on single core 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 (including IT and data security).	
36	Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	
37	Climate related risks	
38	Project and change risks	

Appendix 3 – Three-year risk trends

Ref	Risk	Q1 2019/20	Q2 2019/20	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
1	Investment Performance pressure on employer contributions	●	●	●	●	●	●	●	●	●	●	●	●
2	Adverse Movement - 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 (or other) 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	Unauthorise access to PensionsWEB	●	●	●	●	●	●	●	●	●	●	●	●
30	Incorrect data from Employers leading to fines	●	●	●	●	●	●	●	●	●	●	●	●
31	Inadequate contractual protection for services	●	●	●	●	●	●	●	●	●	●	●	●
32	Over reliance on single core 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 (including IT and data security).	●	●	●	●	●	●	●	●	●	●	●	●
36	Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.		●	●	●	●	●	●	●	●	●	●	●
37	Climate related risks										●	●	●
38	Project and change risks												●

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'**.*

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Overview and approach

The LPF group operates a risk management framework which seeks to align to the nature and extent of its business activities and regulatory environment. Businesses are fluid and evolving and LPF's risk management framework likewise seeks to regularly adapt to the group's needs on an ongoing basis, and with due awareness of external factors. This appendix sets out some context around the current risk management framework and highlights areas under ongoing consideration.

Strategic context and proportionality

Area	Context
Strategic, operational and investment risk	<p>The LPF group risk register purposefully includes an element of both strategic and operational risks, which is determined to be appropriate for a pension fund with long term horizons and, in operational areas, proportionate to the size and nature of our business. Strategic and operational risk analysis is also separately addressed when required for very critical strategic shifts; such as in 2015 when the new delegated corporate structure was introduced and most recently for the ICT migration and Project Forth.</p> <p>As set out below, because the fund is an occupational pension fund and asset owner (c.£9 bn) it does not require to take the same approach as required by the FCA to elements such as market and credit risk. Solvency of the fund is routinely managed and monitored through associated occupational pension fund regulations and oversight - triennial valuation etc. Similarly, liquidity risk is not a current concern for the fund as it remains open to new participants and >50% of the assets are publicly listed or readily realisable.</p> <p>The risks associated with the investments themselves and third-party external managers is managed by our team of investment professionals and purposely not as part of (or with support from) a separate investment risk function. See below for further details on this.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
Risk appetite and tolerances	<p>We are aware that the majority of non-FCA regulated businesses within the UK do not have a risk appetite statement, but took the decision several years ago to deploy this for the LPF group as a best practice enhancement. This statement purposefully does not deploy a detailed quantitative approach but does have a separate guidance document with some supporting detail. The risk appetite statement and tolerance document are added to on an ongoing basis and reviewed/endorsed annually by the Pensions Committee. Where helpful and meaningful, quantitative guidance is added but we have taken the approach that additional layers of quantitative tolerances are not necessary for an organisation of our size and nature. We have taken advice and analysed what a step-up in this area would look like, to ensure we are fully aware, and will continue to keep it under review as part of the development of the organisation.</p> <p>Our risk management policy and philosophy requires us not to over-develop frameworks at the expense of maintaining a 'live' risk culture and beyond the resources and capabilities of the business. In our experience that approach leads to 'risk indifference' and achieves the very opposite of what is intended.</p> <p>LPFI has maintained a risk appetite statement (as an FCA regulatory requirement) since inception.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
Business transformation and maturity of the model	<p>The LPF group has for the last eight years been undergoing significant business transformation, putting in place its own systems and controls to reinforce the necessarily arms-length nature of the pension fund, as distinct from the City of Edinburgh Council (as employer in the fund). Aspects of that transition have moved at different paces and with different governance and other dependencies. The group therefore continues to manage this transition and is currently in the middle of potentially the final structural phase (in Project Forth) which will result in it moving to a separate structure. The group is therefore looking to re-align its systems, controls, policies etc. in line with that new model and is presently analysing that in all key areas. Strategic and project risk methodologies are being reviewed by PwC as part of a separate assurance engagement.</p> <p>The business is therefore continuing to go through a period of meaningful transition, with the risk management framework's operation and design requiring it to accommodate that change and adapt to short term changes to resourcing levels and priorities across the business. We are therefore looking to maintain the existing framework with minimal change to ensure stability for the business during this period.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
Regulatory environments	<p>The LPF group's risk management function requires to take account of two distinct regulatory environments:</p> <ol style="list-style-type: none">1. LPF as a local government pension fund and asset owner (TPR and ICO); and2. LPFI as a regulated investment advisory and management business - albeit with a limited and captive professional client base (FCA). <p>The risk framework operates on an overarching group basis to capture specific LPF-parent risks relating to all the activities within the group and to ensure risks around critical systems and controls shared across its group entities (such as ICT, People etc.) align to the highest applicable standard where necessary. This is to the substantial benefit of LPF in terms of resilience etc., albeit is not a formal requirement nor standard within the LGPS sector. LPF separately needs to be mindful of its statutory obligation to make best use of pension fund monies and so is required to adopt a prudent approach to systems and resource deployment along with the rest of the LGPS sector.</p> <p>LPF's group level risk assessments seek to adopt best practice in the pension sector, but does not require to adopt methodologies specific to those required by the FCA. Those are adequately dealt with at subsidiary level by LPFI and monitored by its board through a purposeful strategy of group delegation.</p>
Governance	<p>The group has a, perhaps overly, complex governance structure arising from its present statutory and legal basis, and it is in the process of reviewing that with a view to rationalisation. Most of that will flow from the outcomes of Project Forth, however the group continues to seek efficiencies and simplification where possible within the constraints of its existing structure.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
Scale and staff resource	<p>The LPF group has c.80 employees and its medium-term business plan does not anticipate it rising beyond 120. In that regard it is a small business and so its culture, systems, controls and practices align to that scale and resource.</p> <p>Whilst operating a 4LOD model, the 2nd line is deliberately 1 FTE employee supplemented by a structured and approved use of external assurance (see below). 3rd line is currently provided by CEC IA, and provides a limited, but adequate volume of audit assurance, within a consciously restricted scope (LPF as a Fund and entity, excl LPFI).</p>
Captive regulated investment services	<p>LPFI only provides services to a limited and captive group of four LGPS (professional not retail) clients and its regulated business plan does not contemplate wider marketing of those services. It (as with LPF) only participates in very low-volume and infrequent trading by comparison to the wider investment management sector. LPFI, and therefore the group where appropriate on shared systems and controls, is therefore only required to satisfy systems and controls and other regulatory standards proportionate to that business plan and level of activity.</p>
Front line services	<p>The LPF group provides front line administrative (including an element of internal asset stewardship) services to the members and the employers in the pension fund and, as above, delivers (through LPFI) limited investment management services to four other LGPS pension funds.</p> <p>There are no other front-line services and all the services are mostly 'desk and systems based' financial services and so do not require staff participating in high risk external or other physical environments with associated risks and operational risk methodologies.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
<p>Physical space/office and 'blended model'</p>	<p>The fund operates a small unit in a grade A commercial building in Edinburgh's city centre. The space was recently re-fitted to allow for a 'blended' model of office and remote working and continues to be under close review as that 'blended model' is being slowly introduced in line with Scottish pandemic regulations.</p> <p>As with most businesses, the group deployed agile solutions effectively to mitigate risk during the global pandemic and is now in the process of reassessing elements of those arrangements to ensure they are fit for purpose for the medium to long term and the new 'blended model'. The organisation remains under pandemic restrictions as of this date.</p> <p>Due to the nature of its business the group considered but rejected the need for a specific pandemic risk register, but did set up a special 'Recovery Group' to manage and monitor specific operational and other business continuity risks associated with it. That group has now been wound-down and the relevant other Tier Two groups monitor pandemic related risks – e.g. People Group, ICT Oversight Group, Risk Management Group etc.</p> <p>In terms of wider context, the LPF group moved to its own office in 2016 and is gradually establishing non-parent reliance on core support functions (<i>see also transition below</i>). It is anticipated that Project Forth will be the focus for the deployment of any remaining independent support functions around office management, health and safety etc.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
Suppliers	<p>The group has a number (4-6) of critical core suppliers, a group of suppliers (2-3) with a particular sensitivity or risk that needs closely managed (e.g. data security/cyber risk etc.) and thereafter a more routine array of business suppliers.</p> <p>A third-party supplier framework is in the process of being reviewed and (where necessary and proportionate) enhanced. Along with associated policies and procedures, this will bring increased rigour to the management of suppliers, with a focus on vesting accountability with relevant business units and retaining an appropriate level of second line oversight.</p> <p>Currently certain aspects of supplier management, including procurement and contract management, are shared between LPF and relevant functions within CEC. This essential element of governance is being looked at with a view to making it more aligned to the accountability within the LPF group. This is being reviewed generally but also as part of Project Forth.</p> <p>In addition, the group has investment management arrangements in place with external managers and counterparties, where separate operational due diligence takes place as part of the investment process. <i>See also below re investment risk.</i></p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Data protection and information security	<p>As an occupational pension fund providing administration services the group processes personal data of some c.85,000 members in the pension funds, from c.80 different employers. The vast majority of this data is held on third party systems and the fund has now recruited a Head of ICT and other specialist staff to, amongst other things, support it with direct ICT and systems supplier oversight and diligence.</p> <p>The business has also recently deployed its own core ICT platform with a view to ensuring the group is best placed to have in place appropriate standards of governance, accountability and security around the data it holds itself. That system was deployed in August 2021 and the business is currently in the process of designing and enhancing its control environment, in conjunction with a project with CEC's IGU unit, to accommodate its new independent supplier and information compliance governance. The results of an external security review are also being reviewed and acted upon.</p> <p>Separately, the group also participates in high value commercial transactions which are highly commercially sensitive. Whilst not a personal data or regulatory issue, the group requires to maintain high standards of information security for this reason also.</p> <p>The only personal data processed by LPFI as part of the delivery of regulated services is a very small amount of information provided by its four clients relating to KYC verification of their key officers for onboarding purposes.</p> <p>Like all businesses, the LPF group manages its own HR information primarily through a third party hosted system, already the subject of a DPIA review and ongoing ICT supplier dd.</p> <p>LPF is a data controller in its own right to reinforce its separate statutory duties around ringfencing its members and employers personal data away from CEC (as an employer in the fund). CEC is also a data controller as a local authority and administering authority of the fund. LPF does not currently require a separate DPO, as the CEC DPO acts as DPO for LPF within the context of CEC as data controller.</p>
---	--

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Area	Context
	This twin data controller position introduces ambiguity and complexity. It is anticipated that CEC ceases the DC role for LPF. LPF is working with CEC to develop a stand-alone data protection framework generally and as part of Project Forth.
Information rights and public transparency	The group is subject to the freedom of information and subject access request obligations and so has relevant procedures in place to accommodate that. As part of a wider Information Compliance project, the group is looking to realign its governance and procedures in this area towards an entirely stand-alone model without reliance on parent services.
Procurement	The group is subject to the procurement regulations. As above, the group is looking to realign its governance and procedures in this area towards an entirely stand-alone model.
External fourth line assurance	<p>The LPF group has a significant amount of routine external fourth line assurance across its different business areas, which has been further supplemented over the last several years to provide assurance on various aspects of its business transformation. In addition to that, it is required to comply with multiple levels of sector transparency (regulatory reporting, industry cost transparency etc.).</p> <p>The group continues to review its overall assurance coverage to ensure that it remains proportionate to its business and anticipates rationalising this once it moves beyond this period of immediate transformation. The LPFI board continue to review their own requirement for 3rd line (internal audit) assurance with specialist asset management expertise, as its business grows and develops, but has significant external assurance in place in the meantime. The group's assurance mapping overview services to monitor this balance on an ongoing basis and is reviewed annually by the pensions committee.</p>

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

Ongoing areas of development

The current development initiatives for the risk management function are:

- **Risk policy and overarching document:** an overview of the risk policy has previously been contained within the risk management document as a prelude to the risk register. We are currently in the process of splitting that out into a separate document and adding elements of the overarching risk framework (previously used in staff training) to create a single policy and overview. This is expected to be completed and socialised by 31 March 2022.
- **Risk Management Group (RMG) membership:** we have recently reviewed the membership of the RMG to align to our developing 'People' initiatives, ownership and accountability. The intention is to reduce/focus the membership and include designated deputies. The newly appointed Head of Legal is also anticipated to be included to specifically cover Supplier Management in tandem with the enhancements to that part of the business second line.
- **Staffing and resource:** our functional business plan anticipates recruiting a more junior compliance and risk analyst at some point in 2022/23. It is likely the recruitment will be brought forward due to Project Forth, but this remains a matter of ongoing strategic review.
- **Systems:** we have considered and reviewed risk tracking software (to be provided by BDO) which would tie in with our existing Compliance Monitoring Programme (CMP) system. The group understands the potential benefits of such a system, but has determined that at this stage it would not be necessary or proportionate to its needs nor a resource priority. The risk function's business plan nevertheless has this as an ongoing item to track in line with the growth and development of the function and wider business.
- **Strategy and decision making:** the group has had two changes in CEO over the last three years, and accompanying changes in approach to management, with the current CEO joining in August 2021. The Senior Leadership Team are therefore presently in the middle of reassessing the operation, governance and management information that flows to that body.

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

- **Tier Two governance risk administration:** Having extended more formal, but purposefully lighter, risk administration to the next level of governance (Tier Two) the risk management group is currently in its first year of bedding this in and ensuring consistency. However, the risk function requires to ensure that the extent and nature of this governance and administration remains proportionate and does not adversely impact on a focus on key risks and the need to ensure a 'live' risk culture. The risk function is therefore reviewing the operation of the current governance to ensure it is effective and viable and will continue to nuance it over the course of the next 18 months. That will look to retain consistency, but also flex administration overhead **up or down** depending on the capabilities, resources and strategic priorities/competing risks of the business. However, where standards drop below what is deemed acceptable, this will be reported through the usual Tier One channels either from a performance or resourcing perspective. This review will also include an assessment of groups below Tier Two, which the governance function is looking to map into the governance overview this year as a 'next stage' enhancement. It is not currently anticipated that this third tier of governance will have formal risk focused administration (other than by exception) beyond managing and escalating their own operational issues in the usual way.
- **Escalation and documentation/minutes:** the group's policy is to have formal minutes as part of its Tier One governance, but only action trackers as part of its Tier Two governance bodies to ensure an effective balance of resource and not distract existing resource from business-critical tasks. The Risk Management Group is currently the only exception to this (at Tier Two level) which, in addition to actions, also seeks to note any challenge or other key points raised/discussed at the meeting – albeit this purposefully does not extend to a full set of formal minutes. All Tier One governance has formal minutes, though the group is looking to enhance the Pensions Committee minuting process once this function migrates across to LPF.
- As a smaller organisation the group uses multiple channels to escalate and disseminate risk information across its governance and staffing structures, proportionate to the nature of that information at any given time. It nevertheless does seek to retain written record via email and logging of key intra-group escalations or decisions. Incident reports are of-course logged and details retained. The group is nevertheless keeping the level and formality of its minuting and communication under ongoing review. Following the implementation of Project Forth, the group expects to have additional dedicated governance resource to further support aspects of the administration at the Tier Two level, but that may not necessarily lead to an escalation in formal administration or procedures.

LPF Risk Management Internal Audit

Management Overview of LPF Group Risk Framework: Context and Initiatives

- **Training:** We have implemented annual staff training on risk management through our ComplianceServe system but are presently reviewing the frequency and detail of that training to ensure it continues to be effective and does not lose impact from being repetitive. Key areas being considered are: (a) the extent to which the broader training module would be better delivered on a twice-yearly basis, and (b) the extent to which shorter and more targeted training and communications should be deployed.
- Staff within the risk function separately receive specialist CPD which they access through a number of channels, including membership of the Institute of Risk Management (IRM). The CRO presently Chairs the IRM's Scottish Group and therefore has access to a significant network and resource to support horizon scanning of emerging issues and best practice in the risk sector.
- **Investment risk:** We have considered the need for separate and independent risk resource to support the investment decision making forums and other processes, but at this stage determined that would not be proportionate to the activities of the business and is adequately covered through existing arrangements. This will nevertheless remain under review as a potential future initiative should the development of the organisation warrant that.

February 2022