



Pensions Committee

2.00pm, Wednesday, 8 December 2021

Risk Management Summary

1. Recommendations

The Pensions Committee (Committee) is requested to:

- 1.1 note the Quarterly Risk Overview as at 3 November 2021 and Statement of Risk Appetite

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 and the group's Statement of Risk Appetite for consideration by the Committee.

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).
 - 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); and
 - 3.1.3 consider and refresh a Statement of Risk Appetite on at least an annual basis, setting out the level and type of risks the group is willing to accept to pursue its strategy
- 3.2 The Conveners and Independent Professional Observer receive a copy of the full risk register every quarter.
- 3.3 The Audit Sub Committee routinely 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 and risk appetite.
- 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.

4. Main Report

- 4.1 The Quarterly Risk Overview as at 3 November 2021 (Appendix 1) is included for the Committees consideration.

- 4.2 The group's Statement of Risk Appetite is set out in Appendix 2 for consideration.
- 4.3 The risk management process for the LPF group is integrated within all of the group's governance and controls. In particular, the Committee should be aware of the following:
- 4.3.1 *Risk appetite*: considered and set by the Senior Leadership Team (SLT) in conjunction with the Risk Management Group.
 - 4.3.2 *Risk management group*: routine meetings held quarterly and otherwise on an as required basis to consider and assess the LPF group's risk register and wider risk environment and track relevant actions. The group comprises representation across all functions and includes the SLT.
 - 4.3.3 *Compliance checklist*: listing critical points of compliance for monitoring and as a reference point for breach reporting. Reviewed and signed off on a quarterly basis by the senior management of the LPF group, which includes SLT, with key actions being tracked by the compliance and risk function and relevant business units.
 - 4.3.4 *Assurance overview and mapping*: providing analysis and oversight of the group's overarching risk assurance framework across the 'four lines of defence', and mapping those points of assurance to relevant risks. This is managed by the risk function, with oversight by SLT, and presented to the Committee annually.
 - 4.3.5 *LPF group systems and controls assessment*: managed by SLT and the LPFI and LPFE boards and reported to Committee annually, with a copy sent to JISP for background information.
 - 4.3.6 *Third party supplier management*: a supplier management framework is managed on an ongoing basis by the risk function in conjunction with the wider business and overseen by SLT. We are continuing to enhance this framework in line with industry best practice and the group's strategic development. Specific representation on the Risk Management Group with accountability for supplier management will be one of the proposed enhancements, together with more detailed and standardised requirement criteria for ongoing management of the various tiers (by risk) of suppliers.
 - 4.3.7 *Internal Capital Adequacy Process (ICAAP)*: which is managed on an ongoing basis by the SLT. The ICAAP itself is reviewed and approved at least annually by the LPFI board, with various aspects considered separately and, in more detail, routinely throughout the year. The ICAAP contains the Risk Appetite Statement and analysis for LPFI, and is due to be updated in 2022 to meet new regulatory requirements coming into force then.

- 4.3.8 *LPFE and LPFI boards*: each receive bespoke risk reporting, with risk management being a standing item on their respective agendas.
- 4.3.9 *Functional sub-group linkage*: there are a number of sub-groups which consider risk at a more operational level (e.g. for People, ICT, Employer, Pensions Administration and Investment related matters) which escalate material issues to the risk function for consideration by the Risk Management Group. This area of the framework remains under continual review and adaptation to ensure it remains both effective and proportionate to the requirements of the group and aligned to the resources available within the group. Consideration of risk at this level is purposefully more agile to retain a 'live' risk culture within the organisation and not stifle a focus and escalation of critical risks.
- 4.4 The risk management processes of LPFI, also covering indirectly the wider group's approach, were reviewed by BDO in March of 2021. The report confirmed that LPF's risk management framework is broadly satisfactory given the size and nature of business activities; that there is an open risk culture at the Firm; that documentation is improving; and that staff are comfortable raising and escalating issues. No material or high priority findings were identified. Low priority recommendations were given on strengthening internal risk MI and documentation.
- 4.5 Those processes are also currently being reviewed by Mercer as part of the wider Systems and Controls review of the LPF group/LPFI and the fund will report back to the Committee any relevant findings.
- 4.6 The group will also be subject to an internal audit of its risk management framework as part of this year's annual audit plan. This will be carried out by PwC under direction of the City of Edinburgh Council's internal audit team, and likely take place in January/February 2022.
- 4.7 The group's assurance overview and mapping document will be updated to acknowledge the assurance provided by these external and internal audit reviews.

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 An initial assessment of the anticipated risks associated with Project Forth are included in the separate report provided to Committee this cycle on that project. That paper contemplates more detailed risk analysis once the Committee has considered and approved the basis and principles on which that project may proceed, which will then be taken into account by LPF's Risk Management Group in the usual way.

8. Appendices

Appendix 1 – Quarterly Risk Overview, as at 3 November 2021



Quarterly Risk Overview

03 November 2021

Executive Summary

This document provides a summary of the assessment of the LPF group's risks by the Risk Management Group (RMG) on 03 November 2021. 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.

Prevailing risk climate

The LPF group risks should be viewed in the context of the following wider background and organisational changes:

COVID-19 and move to blended model

The group has been operating on a fully remote basis since 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. The initial phase for all colleagues is one day physically in office and the remainder remote. This will remain under close review and will be re-assessed in early 2022, when the current phasing anticipates moving to two days per week for most staff. The risks associated with this gradual return and evolving operating model remain under close review, whether relating to use of the office, systems and/or team continuity. Similarly, certain agile decisions and systems deployments made during the pandemic are the subject of re-review, such as our print and post service from CEC's Clocktower – where we are looking to finalise a more detailed SLA.

ICT provider change

The long-planned move to a new ICT provider was substantially completed in August 2021. Following a period of bedding in and independent review, this is delivering meaningful reduction in risks around cyber security, data protection, business continuity, and day-to-day operations.

Assurance work during migration identified potential risks around data protection and information rights. A short-term project is underway to review the group's Information Governance framework against Information Commissioner Office standards, and address any gaps. Equally, the group is now moving to further make use of certain additional capabilities and software anticipated as part of the migration, such as an enhanced document management system/Sharepoint, and is currently in the process of analysing best use of those systems and designing policies and controls that align to its culture and operating model.

Investment management services

FCA-regulated investment management services were launched in December 2020 for collaborative partners, and to date have been provided on a single portfolio of fixed income assets to the Falkirk Council Pension Fund (c.£61m) (FCPF). Assets under management are expected to increase considerably over the next 6-12 months (to c.£1 billion) as a number of new sovereign debt and equity portfolios finish onboarding for both FCPF and the Fife Council Pension Fund. This expansion of services will increase both client exposure and associated service delivery operational risks – i.e. day to day operations, resourcing, increased regulatory obligations and monitoring. However, the LPF group's systems and controls have been enhanced in anticipation of this level of collaborative client support.

Project Forth

The potential impact of Project Forth is being reflected in current risk scoring – particularly in the risk of resource drain on existing staff. This remains under close review as decisions are made and the group’s strategy develops. Project Forth is anticipated to proceed towards implementation in early 2022, at which point other associated risks will track through from the strategic risk analysis presented to the Committee as part of the relevant papers for that project.

Risk register at 03 Nov 2021

Total risks	High	Moderate	Low
37	1	16	20

See Appendix 2 for full overview of risks.

Changes since last review 18 Aug 2021

New	Closed	Improved	Deteriorated	Unchanged
0	0	1	2	34

Scoring changes since the last risk review:

- **Risk 4 – Staff recruitment.** Improved from 30 to 24, Moderate to Low. Previous recruitment issues, such as large number of unskilled applicants, now mitigated with improved processes. Successfully recruited in a number of recent roles, including pensions administrators.
- **Risk 33 – Staff resource.** Deteriorated from 30 to 36, Moderate to High. Resource requirements in a number of active or anticipated projects is increasing the probability of issues in this area. Proposals are being developed for resource augmentation, and will be progressed alongside Project Forth decision papers.
- **Risk 9 – Pension committee decisions.** Deteriorated from 24 to 30, Low to Moderate. Score adjusted to reflect recent issue with matters relating to investment strategy and divestment being considered out-with the Fund’s existing governance structure.

Other relevant updates

- **Risk 13 – Statement of Responsible Investment Principles.** Score remains unchanged, although a new cross-functional group – Responsible Investment Group – has been created to manage and monitor risks in this area.
- **Risk 7 – Failure of IT Systems, Risk 36 – Cyber Security.** Both IT systems and cyber security risk scores remain unchanged for the moment, while new systems are bedded-in and a cyber-security consultant carries out a review of our post-migration processes.

Material litigation – none.

Detailed Update

Update on all 'High' or 'Moderate' risks, detailing risk score, any score change since last report, and narrative:

Risk & reference number	Update
33 - Staff Resource within the Fund not sufficient to carry out core tasks	<p>Score: 36. Deteriorated</p> <p>Score deteriorated to reflect the increasing burden on existing staff, particularly senior management, from Project Forth, investment service expansion, assurance activities, and other organisational development projects. An organisational review is in progress in tandem with a design for Project Forth. With the exception of Project Forth, many of these initiatives are expected to fall away in 2022 and with the McCloud remedy having been delayed.</p>
36 - Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	<p>Score: 32. Unchanged</p> <p>Risk has been elevated since Mar 2020 due to COVID and remote working, and the increased risk of targeted phishing attempts. A third-party review of our post-IT migration information security arrangements is underway, and the risk score will be reviewed on completion.</p>
21 - Information Rights in accordance with regulations	<p>Score: 30. Unchanged</p> <p>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. No issues have been identified with Freedom of Information or Subject Access processes.</p>
12 - Members' confidential data is lost or made public. Breach of Data Protection Act	<p>Score: 30. Unchanged</p> <p>The Information Governance project will also review and address our data protection systems and controls, and this score will be reviewed on completion. The Fund is comfortable our systems and controls protect member data and identify and report that breaches are robust. Enhancements are required to fully document existing processes, and to refresh training and awareness amongst colleagues.</p>
7 - Failure of IT systems	<p>Score: 30. Unchanged</p> <p>IT migration completed in Aug 2021 without material issue. Score will remain elevated while new systems bedded in, new controls are implemented, and external consultant review is carried out.</p>
11 - Business continuity issues	<p>Score: 30. Unchanged</p> <p>Remains elevated due to COVID-19 and remote working. First phase of return to office / longer-term blended model began in Sep 2021: colleagues are in office one day per week and remainder remote.</p> <p>Work underway to refresh and test Business Continuity Plans post ICT migration.</p>
8 - Staff culture & engagement issues	<p>Score: 30. Unchanged</p> <p>Annual YourVoice survey was carried out for all colleagues in October 2021. Results will be collated and reviewed in due course.</p> <p>All end year annual performance reviews are expected to be completed by end November 2021. Performance Management Development training is being provided to all LPF line managers during Q4 2021.</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>Risk score expected to be reviewed after a full annual cycle of LPFI's improved monitoring (Q1-Q2 2022).</p>

Risk & reference number	Update
23 - Acting beyond proper authority/delegations	<p>Score: 30. Unchanged</p> <p>Due to the prevailing circumstances and outstanding actions 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 more broadly map them to the functions within the LPF group and reflect the wider corporate structure and delegations.</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 across 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 otherwise continuing to work closely and well with CEC's procurement team 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 generally, with enhanced recent engagement, and as part of the Governance Review process. Transitional arrangements are in process to migrate committee administrative support to LPF by December 2021.</p>
9 - Pension committee (or other) members take decisions against sound advice, on political grounds or due to lack of knowledge	<p>Score: 30. Deteriorated</p> <p>In Oct 2021, matters were referred and discussed at CEC committees outwith Fund's existing governance structure. Action required to ensure awareness of governance processes and the fund's separate code of conduct.</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>
15 - Late payment of pensions	<p>Score: 27. Unchanged</p> <p>Elevated risk score due to AVC provider issues and delays to member payments. Has improved somewhat from initial problems in early 2021, but not fully resolved – remains under review. Our annual service review with the provider is due in November 2021.</p>
1 - Investment Performance pressure on employer contributions	<p>Score: 25. Unchanged</p> <p>Investment strategy was recently reviewed by JISP, and a number of actions taken, including adjustments to allocations, and strategy/unitisation reporting to JISP.</p>
2 - Adverse Movement - pressure on employer contributions	<p>Score: 25. Unchanged</p> <p>The employer contribution rates approach has changed from deterministic to risk-based, with Funding Strategy Statement updated and employers consulted and informed.</p>
35 - Inadequate, or failure of, supplier and other third-party systems (including IT and data security).	<p>Score: 25. Unchanged</p> <p>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.</p>

Appendix 1 – Risk Scoring & Distribution Chart

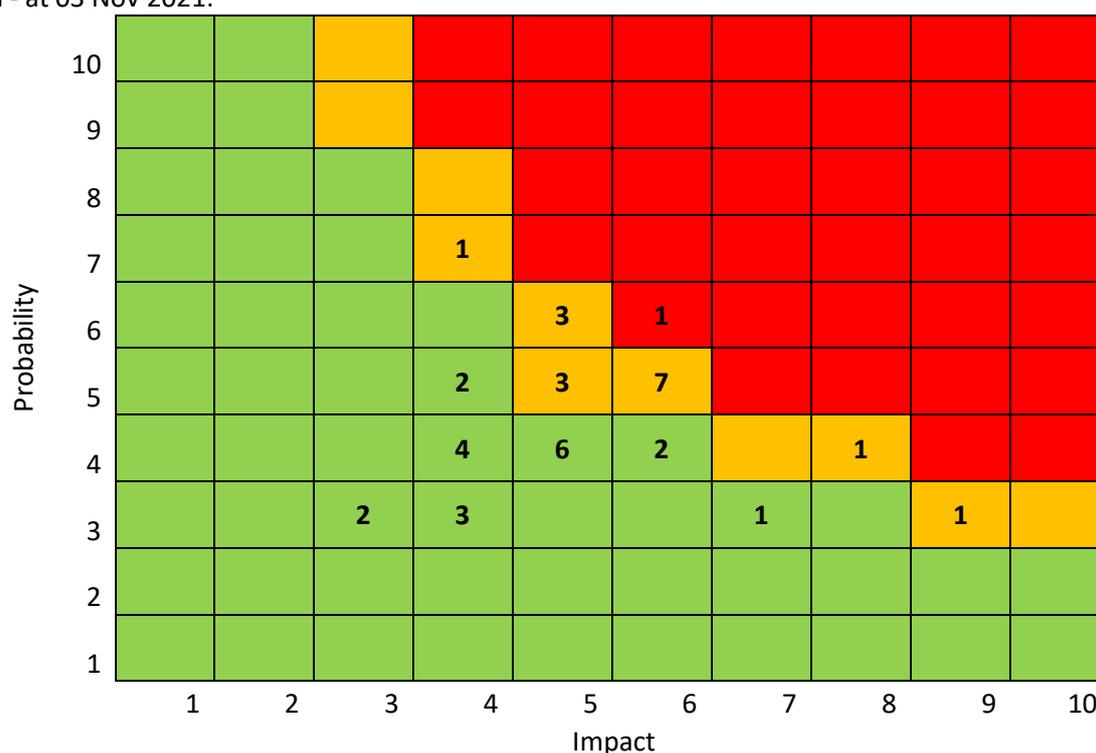
Risk scoring:

	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 03 Nov 2021:



Appendix 2 – Full Risk Key

Full risk register Red Amber Green (RAG) status at 03 Nov 2021:

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

Appendix 3 – Three-year risk trends

Ref	Risk	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
		2018/19	2019/20	2019/20	2019/20	2019/20	2020/21	2020/21	2020/21	2020/21	2020/21	2021/22	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												

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’**.*