



## **Pensions Committee**

2.00pm, Wednesday, 23 June 2021

### **Risk Management Summary**

#### **1. Recommendations**

---

The Pensions Committee (Committee) is requested to:

- 1.1 note the Quarterly Risk Overview as at 06 May 2021

#### **Struan Fairbairn**

Chief Risk Officer, Lothian Pension Fund

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

E-mail: [sean.reid@edinburgh.gov.uk](mailto:sean.reid@edinburgh.gov.uk) | Tel: 0131 529 7259

# 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 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); 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 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 06 May 2021 (Appendix 1) is included for the Committees consideration.
- 4.2 The risk management process for the LPF group is integrated throughout the group's governance and controls. In particular, the Committee should be aware of the following:

- 4.2.1 *Risk appetite*: considered and set by the Senior Leadership Team (SLT) in conjunction with the Risk Management Group.
- 4.2.2 *Risk management group (RMG)*: routine meetings held quarterly and otherwise on an as required basis to consider and assess all elements of the LPF group's risk framework, including the risk appetite, register, overall assurance position and any more granular risks escalated from other sub-groups. The group comprises representation across all functions and includes the SLT.
- 4.2.3 *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 SLT, with key actions being tracked by the risk function and relevant business units.
- 4.2.4 *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 from RMG and SLT, and presented to the Committee annually.
- 4.2.5 *LPF group systems and controls assessment*: managed by SLT and the LPFI and LPFE boards and reported to Committee and JISP annually.
- 4.2.6 *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. This framework continues to be developed and enhanced in conjunction with other developments within the group.
- 4.2.7 *Internal Capital Adequacy Assessment Process (ICAAP)*: which is managed on an ongoing basis by SLT and RMG. 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. This process will be the subject of regulatory change from January 2022 and the group are currently involved in a programme to comply by that date.
- 4.2.8 *ICT oversight and governance procedures*: which are managed by the ICT Oversight Group on an ongoing basis and overseen by the SLT.
- 4.2.9 *People and HR Procedures*: which are managed by the People Group on an ongoing basis and overseen by the SLT and the LPFE board.
- 4.2.10 *Investment Controls and Parameters (LPF Group Controls and Compliance report)*: which are now mostly automated on the CRIMS order management system, managed by the compliance, front and back office functions and

overseen by SLT, the LPFI board and JISP (with annual reporting to Committee).

4.2.11 *Overall review of governance and the LPF group structure:* managed by SLT and overseen annually by the Committee and Pensions Committee.

4.2.12 *COVID-19:* as above, managed by SLT on an ongoing basis, in conjunction with the Risk Management Group and other dedicated sub-groups as required.

## **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 06 May 2021



# **Quarterly Risk Overview**

**6 May 2021**

## Executive Summary

---

This document provides a summary of the assessment of the LPF group's risks by the Risk Management Group (RMG) on 6 May 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 continues to carry a higher than normal level of operational risk as it transitions its model to an increasingly arms-length structure, but in doing so it is significantly mitigating other fundamental structural and operational risks. This period of organisational transformation is now (excluding consideration of Project Forth) giving way to a more settled stage of 'bedding-in' and reflective assurance work, with the ongoing project to implement a separate managed service provider for core ICT being the only significant non-BAU initiative.

The group began supporting its collaborative partners with portfolio management services from December 2020. That brought heightened client servicing and regulatory risks, but improved business resilience, sustainability and enhanced cost sharing. The service is expected to build throughout the next 12 months, subject to JISP and partner fund take-up, but then level off thereafter. That AUM build is progressing slower than originally reported, simply due to competing demands on resource both within LPF and amongst our collaborative partners. That is important to note in terms of assessing the current and projected risk environment, but is not of itself a concern.

The group continues to operate on a fully remote basis and its business continuity plan is still operating effectively. Good progress has also been made in anticipating medium term adjustments (such as its office refit) to further mitigate the position as soon as that becomes possible. Shorter-term mitigation strategies remain under review, as in some cases these were required to be put in place quickly and on an agile basis. Business continuity in all its facets therefore continues to be a key focus, including around heightened risk of cyber security, fraud, group resilience, culture and staff conduct.

## Risk register at 6 May 2021

Total risks	High	Moderate	Low
35	3	13	19

See Appendix 2 for full overview of risks.

## Changes since last review 8 Feb 2021

New	Closed	Improved	Deteriorated	Unchanged
0*	1	7	4	24

\*1 new risk will be added to the risk register next quarter, on Climate-related issues.

1 risk has been closed and removed from the register:

- **Risk 13 – Loss due to stock lending.** This risk has been closed. It is no longer deemed useful to monitor as a separate risk. Any stock lending issues arising in future can be captured and monitored as part of Risk 1, on investment performance.

Scoring changes since the last risk review:

- **Risk 4 – Recruitment & retention of staff.** Deteriorated from 24 to 30. Potential for recruitment issues due to flooded market and we're seeing an increased number of unskilled applicants to advertised vacancies.
- **Risk 7 – Failure of IT systems.** Deteriorated from 48 to 54. Temporary increase due to upcoming ICT transition, and risk of disruption during migration.
- **Risk 12 – Data loss or breach.** Deteriorated from 36 to 42. Also a temporary increase from potential data related risks arising from forthcoming ICT migration.
- **Risk 17 – Portfolio Transition Issues.** Deteriorated from 8 to 12, due to proposed collaborative partner transitions.
- **Risk 5 – Fraud relating to members.** Improved from 24 to 16. LPF has signed up to the TPR Pledge to combat pension scams, and implemented new processes to identify potential fraud and ensure members are aware of potential scams. There is nevertheless no complacency around the heightened risk around cyber and other fraud arising from the pandemic driven remote working.
- **Risk 9 – Pension Committee (or other) members take decisions against sound advice.** Improved from 30 to 24. LPF liaised with Democracy, Governance and Resilience team and Azets, it was agreed that the annual report for LPF will only be considered and approved by the Pension Committee.
- **Risk 10 - Pension Board not operating effectively.** Improved from 28 to 20. The Chair has agreed to extend their tenure for another year. Two of three vacancies have now been filled.
- **Risk 14 – Risk of incorrect pension payments.** Improved from 16 to 9. All recommendations from previous audits have been implemented, with mitigating controls in place and working as expected.
- **Risk 15 – Failure to pay pensions as they fall due.** Improved from 36 to 27. Some progress made with AVC issues, although not fully resolved.
- **Risk 22 – Incorrect communications with members.** Improved from 20 to 16. Work underway on hosting service and review of communications channels.
- **Risk 30 – Limited or incorrect data from Employers.** Improved from 20 to 16. Progress made on ensuring Employers are using data validation when submitting information.

The scoring for one remaining material risk – **11 Business Continuity Issues** - remains unchanged. Elevated score is partly due to COVID-19 and continuing remote arrangements. This risk will improve meaningfully once a partial return to office occurs, and the move to the new ICT provider is complete and related enhancements are delivered.

## Other relevant updates

Material litigation – none

## Detailed Update

Update on all 'High' or 'Moderate' risks:

Risk & reference number	Update	Score & movement
7 - Failure of IT systems	<p>COVID-19 remote working remains in place. Resilience is good and stable, but impact and probability remain increased to reflect these circumstances.</p> <p>Score temporarily elevated due to upcoming ICT provider change, and risk of disruption during migration. A migration project group meets weekly to manage the transition.</p>	<p><b>54</b> <b>Deteriorated</b></p>
11 - Business continuity issues	<p>Remains high due to the prevailing COVID-19 situation. All staff continue to work remotely. Move to IT provider expected to improve system robustness.</p> <p>Office refit completed within timescales – some adjustments and snagging to be finished. Expected to be fully ready by end May.</p>	<p><b>42</b> <b>Unchanged</b></p>
12 - Members' confidential data is lost or made public. Breach of Data Protection Act	<p>There continues to be a potential increased risk of cyber attacks as a result of COVID-19 and LPF, as with the wider business community, has experienced targeted phishing attempts.</p> <p>This risk has been elevated due to upcoming ICT provider change, and related risks on data loss / corruption during migration. A migration project group meets weekly to manage the transition.</p>	<p><b>42</b> <b>Deteriorated</b></p>
36 - Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	<p>As above, risk raised due to COVID and remote working. Formal training and awareness programmes are in place for staff.</p> <p>An independent security consultant has been appointed and will carry out penetration testing and information security reviews pre and post migration.</p>	<p><b>32</b> <b>Unchanged</b></p>
4 - Recruitment & retention of staff	<p>Score increased - potential recruitment issues on getting appropriate calibre of talent due to flooded market, and an increased number of unskilled applicants.</p>	<p><b>30</b> <b>Deteriorated</b></p>
8 - Staff culture & engagement issues	<p>A refreshed annual performance process has been embedded, with 2021 plans and objective for all colleagues in place.</p> <p>A People &amp; Communications review by an external consultant was carried out in Mar/Apr with no material adverse findings. Recommendations are being reviewed and implemented.</p>	<p><b>30</b> <b>Unchanged</b></p>
20 – Regulatory breach	<p>Continuing to implement operational changes required for compliance following the extensions of LPF's regulatory permissions and new investment management services.</p>	<p><b>30</b> <b>Unchanged</b></p>
23 - Acting beyond proper authority/delegations	<p>Due to the prevailing circumstances and outstanding actions the risk remains on amber, although there has been no breach in existing delegations.</p> <p>LPF has paid close attention to the operation of its delegations under the present circumstances, with all the team remote working and with key person dependencies in mind. The group</p>	<p><b>30</b> <b>Unchanged</b></p>






Risk & reference number	Update	Score & movement
	<p>has only required minimal adaption to current processes so far and has sought to introduce supporting systems (e.g. e-signing) where necessary to mitigate any associated continuity risks.</p> <p>The group's sub-delegations require to be updated and will need to be refreshed again on the new CEO joining.</p>	
25 - Procurement/framework breach	<p>LPF is 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> <p>The risk is static due to the enhanced impact the procurement regime has on LPF's developing business model (sitting unusually within all of the financial services, pensions and public sector regimes) and the fact that it continues to be in the midst of developing new systems, controls and procedures in this area – with progress having been hampered by the prevailing circumstance of the last 6 months.</p>	<p><b>30</b> <b>Unchanged</b></p>
27 - Group structure and governance fully compliant and up-to-date.	Resourcing of committee services under review generally, with enhanced recent engagement, and as part of the Governance Review process.	<p><b>30</b> <b>Unchanged</b></p>
33 - Staff Resource within the Fund not sufficient to carry out core tasks	This risk remains amber due to the additional resource attributable to significant strategic initiatives such as the implementation of the Digital Strategy, extension of investment management services and Project Forth.	<p><b>30</b> <b>Unchanged</b></p>
3 - Failure of an employer to pay contributions	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 and has established structures and processes to engage with its employers around affordability and potential exit.	<p><b>28</b> <b>Unchanged</b></p>
15 - Late payment of pension	Score improved, moved to amber from red – AVC provider issues and delays to member payments have improved somewhat, but not fully resolved. Remains under close review.	<p><b>27</b> <b>Improved</b></p>

## Appendix 1 – Risk Scoring & Distribution Chart

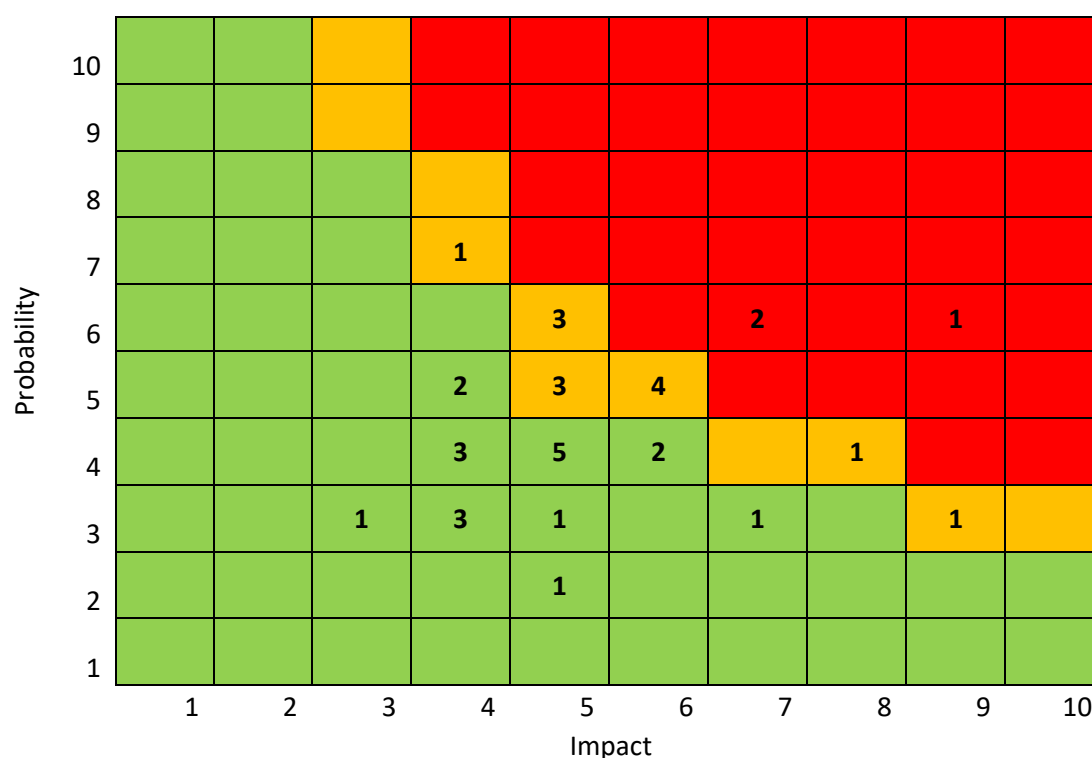
Risk scoring:

	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 6 May 2021:



## Appendix 2 – Full Risk Key

Full risk register scores, including Red Amber Green (RAG) status at 6 May 2021:

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	<i>Loss due to stock lending default (removed – will no longer appear from next quarter)</i>	
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	FOI process in accordance with law	
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 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.	

## Appendix 3 – Three year risk trends

Ref	Risk	Q2 2018/19	Q3 2018/19	Q4 2018/19	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
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	Loss due to stock lending default	●	●	●	●	●	●	●	●	●	●	●	
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	FOI process in accordance with law	●	●	●	●	●	●	●	●	●	●	●	●
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.					●	●	●	●	●	●	●	●

## 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’**.