Pensions Audit Sub Committee

2.00pm, Monday, 27 September 2021

Risk Management Summary

1. Recommendations

The Pensions Audit Committee (Committee) is requested to:

1.1 note the Quarterly Risk Overview as at 18 August 2021

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 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 18 August 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.

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 18 August 2021

LOTHIAN
PENSION FUND

Quarterly Risk Overview

18 August 2021

Executive Summary

This document provides a summary of the assessment of the LPF group's risks by the Risk Management Group (RMG) on 18 August 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, governance and strategic risks. This period of organisational transformation is now (excluding consideration of Project Forth) giving way to a more settled stage of 'bedding-in', control design and reflective assurance work.

Investment management services

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 through to May 2022, subject to JISP and partner fund take-up, but then level off thereafter.

Business continuity

The group continues to operate on a fully remote basis and its business continuity plan is still operating effectively. At present there are no pandemic related supply chain issues or supplier problems, but this continues to be monitored on an ongoing basis. The office refit has been finalised and passed all health and safety checks. A phased return to a 'blended' model of both office and remote working will commence in September 2021. Business continuity continues to be a key focus and the new blended model will be closely scrutinised with this in mind. In terms of medium-term pandemic impact, the key focus is on: (I) risk to deliverability of strategy and key objectives, (ii) operational resilience and continuity, (iii) information security, (iv) fraud, (v) key person retention and (vi) integrity, culture and controls.

New ICT provider

The long-planned move to a new ICT provider was substantially completed in August 2021. Following a period of bedding in and review, this will deliver meaningful reduction in risks around cyber security, data protection, business continuity, and day-to-day operations. Assurance work during the migration identified potential risks on data protection and information rights, relating to the existing framework. These are being reviewed and (where necessary) addressed in tandem with other organisational and control design work arising from opportunities presented by the new platform – new document management system, intranet, website update etc.

Risk register at 18 Aug 2021

Total risks	High	Moderate	Low
37	0	17	20

See Appendix 2 for full overview of risks.

Changes since last review 6 May 2021

New	Closed	Improved	Deteriorated	Unchanged
2	0	3	2	30

2 new risks have been added to the register:

- **Risk 13 – Statement of Responsible Investment Principles (SRIP).** Risk that we fail to comply with our Statement of Responsible Investment Principles, leading to adverse investment performance, reputational damage or failure to meet regulatory standards. Currently rated low, due to existing controls and dedicated resource.
- **Risk 37 – Climate change risks.** Risk that operational risks arising from climate change are not managed across LPF group, leading to impact on resilience, failure to meet regulatory standards, reputational damage**.** Currently rated low due to nature of LPF operations, although a full identification and assessment of operational climate risks will be carried out.

Scoring changes since the last risk review:

- **Risk 21 – Information Rights.** Deteriorated from 10 to 30. Partly due to redefining of risk – expanded from Freedom of Information (FOI) to wider Information Rights more broadly – but mostly relating to the anticipated change and redesign of the LPF group's information compliance governance, policies and controls post-ICT migration to better reflect the stand-alone nature of the group. There are also a number of separate and related findings from a Data Protection Impact Assessment (DPIA) carried out by CEC's IGU team as part of the pre-migration assessment process to review and (where appropriate) address.
- **Risk 16 – Market Abuse.** Deteriorated from 15 to 20. Increased training amongst relevant staff required to meet regulatory good practice.
- **Risk 7 – Failure of IT systems.** Improved from 54 to 30. Previously increased score included risk of disruption during migration. Migration now substantially complete. Will remain elevated until new systems and processes bedded in and service is reviewed.
- **Risk 12 – Data loss or breach.** Improved from 42 to 30. IT migration is substantially complete, delivering improvements in security, web controls, access permissions etc. and the significant "point of migration" risks around the transfer of data to the new environment have abated. The risk will be further reduced in the next few quarters as the group finalises its post-migration security assurance review, information governance refresh and DPIA remediation.
- **Risk 14 – Business Continuity.** Improved from 42 to 30. IT migration substantially complete, refit of office complete. Phased RTO / blended model is planned. Full time remote working still currently in place.

Other relevant updates

Risk 36 – Cyber Security. Although there have been meaningful benefits from the new ICT provider and migration penetration testing, the score will be reassessed after our first post-migration cyber security review (by the external consultant) due to conclude in September. We anticipate that this risk will meaningfully reduce following that assurance assessment and our finalising any follow up on any findings.

Material litigation – none.

Detailed Update

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

Risk & reference number	Update	Score & movement
36 - Cybersecurity protections and/or back-up not sufficient to prevent/minimise cyber-attacks.	Risk raised due to COVID and remote working, and increased risk of targeted phishing attempts. IT migration should meaningfully improve once fully embedded and assessed - scoring will be reassessed after first review in Sep 2021.	**32 Unchanged**
21 - Information Rights in accordance with regulations	Definition of risk expanded from only Freedom of Information (FOI) to Information Rights, which is a broader area and includes FOI, leading to an increased score. IGU DPIA carried out as part of IT migration identified potential risks relating to data cleansing, assurance on information governance, and individual rights. A project will be run to assess and resolve these issues.	**30 Deteriorated**
12 - Members' confidential data is lost or made public. Breach of Data Protection Act	The IT migration was substantially completed in Aug 2021, delivering improvements in security via multi-factor authentication, web filtering controls, access permissions. DPIA performed as part of migration flagged previously unidentified risk of non-compliance with data protection regulations in existing framework. This was not a result of the IT migration. An information compliance project will be run to assess and resolve these risks.	**30 Improved**
7 - Failure of IT systems	Previously increased score included risk of disruption during migration. IT migration substantially completed in Aug 2021, and expected to delivery meaningful improvements in this area. Will remain elevated until new systems and processes bedded in and service is reviewed.	**30 Improved**
11 - Business continuity issues	Improved due to IT migration and office refit completion. Remains elevated due to prevailing COVID-19 situation - all staff continue to work remotely. Phased return to office / blended model to begin in Sep 2021.	**30 Improved**
4 - Recruitment & retention of staff	Action taken to resolve previous issues with flooded market. New risk arising from local recruitment of qualified administrators and potential impact on turnover and workforce capability.	**30 Unchanged**
8 - Staff culture & engagement issues	A refreshed annual performance process has been embedded, with 2021 plans and objectives for all colleagues in place. Half year reviews completed on time. A People & Communications review by an external consultant was carried out in Mar/Apr with no material adverse findings. Recommendations are being reviewed and implemented.	**30 Unchanged**
20 - Regulatory breach	LPFI compliance monitoring has been enhanced and is picking up minor findings and recommendations, which shows it is working effectively.	**30 Unchanged**

Risk & reference number	Update	Score & movement
23 - Acting beyond proper authority/delegations	Due to prevailing circumstances and outstanding actions the risk remains amber, although there has been no breach in existing delegations. 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 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. Nevertheless a review and refresh of the delegations is underway, to more broadly map them to the functions within the LPF group.	**30 Unchanged**
25 - Procurement/framework breach	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. 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 18 months.	**30 Unchanged**
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. Transitional arrangements expected to arise from the Governance Review.	**30 Unchanged**
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. However, the Organisational Development Review has been successfully implemented and LPF anticipates that the risk will reduce over the next few quarters.	**30 Unchanged**
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.	**28 Unchanged**
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.	**27 Unchanged**
1 - Investment Performance pressure on employer contributions	Investment strategy was recently reviewed by JISP, and a number of actions taken, including adjustments to allocations, and strategy/unitisation reporting to JISP.	**25 Unchanged**
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.	**25 Unchanged**
35 - Inadequate, or failure of, supplier and other third-party systems (including IT and data security).	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.	**25 Unchanged**

Appendix 1 – Risk Scoring & Distribution Chart

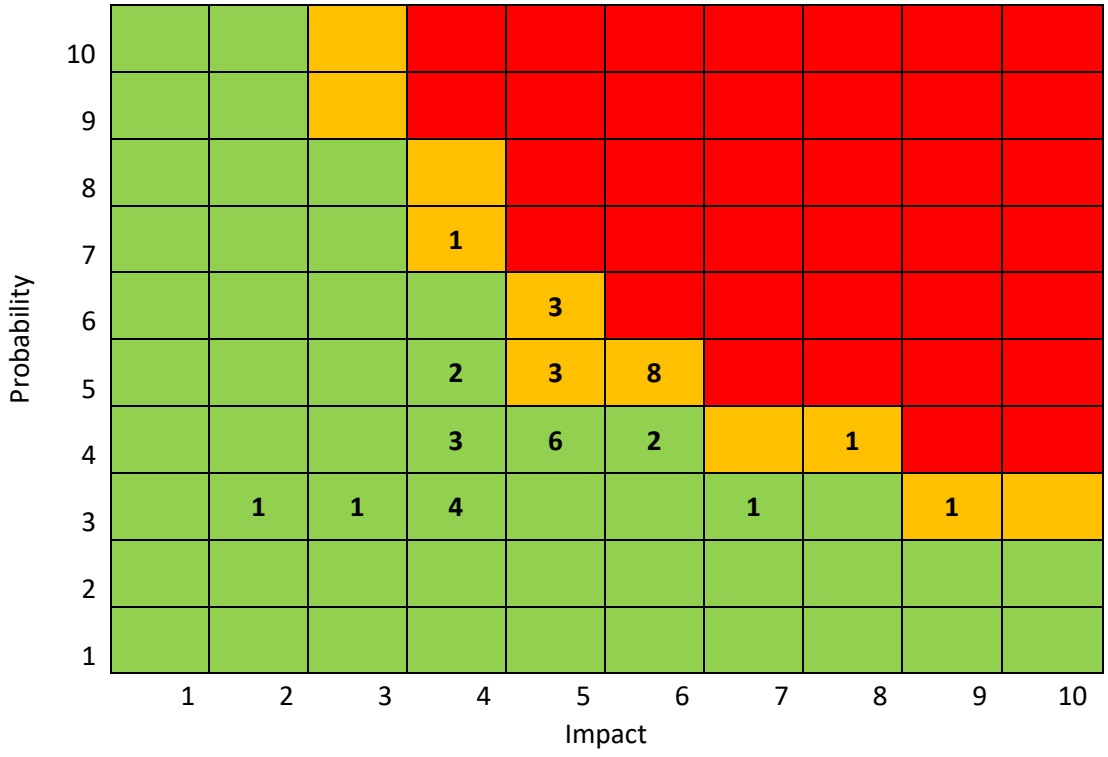
Risk scoring:

	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 18 Aug 2021:



Appendix 2 – Full Risk Key

Full risk register scores, including Red Amber Green (RAG) status at 18 Aug 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	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	

LOTHIAN PENSION FUND

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	Q2 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'**.*