Pensions Audit Sub-Committee

3.00pm, Tuesday, 21 March 2023

Lothian Pension Fund - Internal Audit Update - February 2023

Item number 6.2

1.   Recommendations

The Pensions Audit Sub-Committee is requested to note:

1.1   Progress of delivery with the 2022/23 LPF annual internal audit plan, including the outcomes of the recent Third-Party Supplier Management Audit;

1.2   Note progress with delivery of the Information Governance audit currently underway;

1.3   Approve a request to defer the Information Security Arrangements audit to the 2023/24 Internal Audit Plan;

1.4   Note that the draft 2023/24 LPF annual internal audit plan is presented to the Committee for review and approval in a separate paper at this meeting; and

1.5   Progress with implementation of agreed management actions from previously completed internal audits.

Laura Calder

Head of Internal Audit, City of Edinburgh Council

Legal and Assurance, Corporate Services Directorate

E-mail: laura.calder@edinburgh.gov.uk | Tel: 0131 469 3077

Lothian Pension Fund - Internal Audit Update - February 2023

2. Executive Summary

2.1   This report provides details of the progress of Internal Audit's (IA) assurance activity on behalf of Lothian Pension Fund (LPF) overseen by the City of Edinburgh Council's (the Council) IA function.

2.2   Delivery of the four audits included in the 2022/23 IA annual plan agreed by Committee in September 2022 are underway, with two audits complete and a further audit currently in progress.

2.3   A report detailing the outcomes of the Third-Party Supplier Management is included for the Committee's review and scrutiny.

2.4   Due to unforeseen absence of key contacts, the Information Security Arrangements audit has been delayed. It is requested that this audit is deferred to quarter 1 of the 2023/24 IA plan.

2.5   It is IA's opinion that the three audits due for completion in the 2022/23 IA plan will be sufficient to provide an annual audit opinion for the year end 31 March 2023.

2.6   The draft 2023/24 LPF annual internal audit plan has been developed by the Council's IA function with support from PwC. The draft has been reviewed and discussed with management and is presented to the Committee for review and approval within a separate paper for this meeting.

2.7   As at 9 February 2023, LPF had 14 agreed management actions with one action passed the original implementation date.

3. Background

2022/23 Internal Audit Annual Plan

3.1   A revised 2022/23 LPF IA plan consisting of four audits was approved by the Committee in September 2022.

Internal Audit Follow-Up Process

3.2   IA follow up on progress with implementation of management actions arising from IA reports. A risk-based approach to follow-up is applied, with all high rated management actions validated by IA when presented for closure together with a sample of medium actions. The remaining medium actions and low actions are closed via a 'self-attestation' once confirmed as complete by management.

4. Main Report

Progress with delivery of the 2022/23 LPF IA annual plan

4.1 The 2022/23 IA annual plan includes the following reviews:

- Project Forth – Programme assurance
- Third-party supplier management
- Information governance
- Information Security Arrangements

4.2 The Project Forth - Programme assurance review is complete with outcomes reported to Committee in December 2022.

4.3 The Third-Party Supplier Management audit is complete with a report detailing outcomes included at Appendix 1.

4.4 The Information Governance audit is currently in fieldwork and is due to complete by end of March 2023 as agreed with management.

4.5 Planning is complete for the remaining audit of Information Security Arrangements with a Terms of Reference and programme of work agreed. Fieldwork has been delayed due to unforeseen absence of a key contact. In recognition that the key contact will require time to return to work following absence and to ensure sufficient time to complete this audit work thoroughly, it is proposed that that this audit is deferred to quarter 1 of the 2023/24 IA plan.

4.6 It is IA's opinion that the three audits due for completion in the 2022/23 IA plan will be sufficient to provide an annual audit opinion for the year ending 31 March 2023.

Status of Open IA management actions as at 9 February 2023

4.7 As at 9 February 2023, LPF had 14 agreed management actions (9 Medium and 5 Low) which were raised across the following audits:

- Project Forth - Programme Assurance (7)
- Bulk Transfers (4)
- Risk Management (2)
- Technology Model Development (1)

4.8 One management action has passed its original implementation date, details of which are set out below:

LOTHIAN
PENSION FUND

Audit	Action title / due date	Rating	Action and management update
LPF2003 Technology Model Development	3.1.2: Post-Implementation Activities 31/12/2022	Medium	LPF have produced user manuals and documentation for key/business critical systems and will review the requirements and suitability of the currently available generic documentation for the others during 2022. The action to address the issue is partially complete, however due to events out with LPF's control, unplanned leave by the issue owner and delegate, is delaying completion of this item. A revised date will be provided in due course.

4.9 The remaining 13 management actions are not yet due for completion and implementation is currently being progressed by LPF. Details of the management actions are provided at Appendix 2.

5. Financial impact

5.1 Failure to close management actions and address the associated risks in a timely manner may have financial impacts which are not yet measurable.

6. Stakeholder/Regulatory Impact

6.1 IA recommendations are raised as a result of control gaps or deficiencies identified during audits. If agreed management actions are not implemented, LPF will be exposed to the risks set out in the relevant IA reports, including the potential risk of non-compliance with applicable regulations.

7. Background reading/external references

7.1 Public Sector Internal Audit Standards

7.2 Lothian Pension Fund – Internal Audit Update as at 31 August 2022 (item 6.4)

8. Appendices

Appendix 1   Third-Party Supplier Management Internal Audit Report

Appendix 2   All LPF outstanding audit actions as at 9 February 2023

Internal Audit Report

Lothian Pension Fund - Third Party Supplier Management

8 March 2023

LPF2203

Overall Assessment	Significant improvement required

Contents

This Internal Audit review is conducted by the City of Edinburgh Council for the Lothian Pension Fund under the auspices of the 2022/23 internal audit plan approved by the Pensions Audit Sub-Committee in September 2022. The review is designed to help the Lothian Pension Fund assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the Lothian Pension Fund. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and members as appropriate.

Executive Summary

Overall opinion and summary of findings

Our review of Lothian Pension Fund's (LPF) Third Party Supplier Management Framework recognises that it has recently been developed and implemented and that it takes time to embed such frameworks. The following findings have been identified which are designed to enhance and strengthen LPF's control environment:

- **Supplier management processes for Critical Suppliers** – the criteria used for identifying critical suppliers requires improvement to ensure they are specific and consistent with regulatory expectations. Tier 1 criteria is inadequate as it fails to consider a regulatory impact of engaging with a supplier, while the criteria for Tiers 2 and 3 are ambiguous and too subjective.

- **Contract exit planning** – a strategy for contract exit planning or business continuity for suppliers has not yet been documented or considered by LPF.

- **Design of the Supplier Management** – the framework document requires improvement to ensure it provides an adequate level of detail for Third Party Risk Management on key areas such as: governing body responsibility for oversight of outsourcing, intra-group outsourcing (LPFI and LPFE Limited), defined risk appetite, risk and issue identification and management, and exit planning.

- **Supplier onboarding processes** – supplier onboarding processes require improvement to ensure they effectively manage supplier risk. Issues noted include the lack of a Quality Assurance process following the materiality assessment, and gaps and inconsistencies in the Legal review process.

- **Training and awareness** – there is currently no supplier management risk training and awareness programme for relevant LPF employees.

- **Ongoing monitoring and oversight** – there is limited reference to City of Edinburgh Council's (the Council) role and responsibilities within the supplier management framework. There are also gaps in the processes in place for governance of the framework as well as in the management and oversight of the supplier database.

Areas of good practice

Our review identified the following areas of good practice:

- LPF's risk register includes supplier risks and consists of key metrics such as impact, probability, target risk level, and mitigation actions.

- The Data Privacy Impact Assessment (DPIA) process is clear and consistent with our discussions with LPF employees. The cooperative approach between LPF (data processor) and the Council (the data controller) in this process is adequate from a design perspective, and the Data Protection Assessment (DPA) approach is successful in assessing the applicability of a supplier DPIA.

Management response

The LPF Supplier Management Framework was developed during 2022 prior to which LPF managed suppliers through a contract database that mirrored and relied on CEC contract management processes. LPF had since acknowledged the need to operate an appropriate standalone framework to facilitate the management and oversight of LPF suppliers to mitigate risks in respect of supplier underperformance or failure. This framework was rolled out during Q2-Q3 2022, and during the period of the review, has only had a limited time to embed in the business. Notwithstanding, LPF management welcome design and operational observations at this early stage of the framework's maturity which provide an opportunity to reflect on areas which can be improved and make enhancements as appropriate.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
Strategy & oversight, risk appetite, and policy maintenance	🟠	🔴	Finding 1 – Supplier management processes for Critical Suppliers	High Priority
	🟠	N/A	Finding 3 – Design of the Supplier Management Framework	Medium Priority
Third-Party Supplier offboarding and exit plans	🔴	🔴	Finding 2 – Exit planning	High Priority
Third-Party Supplier onboarding	🟠	🟠	Finding 4 – Supplier onboarding processes	Medium Priority
Monitoring and oversight	🟠	🟠	Finding 5 – Ongoing monitoring and oversight	Medium Priority
Training and communication	🟠	🟠	Finding 6 – Supplier Management training and awareness	Low Priority

See Appendix 1 for Control Assessment and Assurance Definitions

Background and scope

Lothian Pension Fund (LPF) engages with a number of third-party suppliers to support its business functions. These range from ad-hoc arrangements to reliance on larger, more complex service providers. The effective management of all third-party suppliers is key to ensuring business objectives are met. It is therefore expected that Senior Management demonstrates adequate and appropriate oversight, and that monitoring controls are in place to enable a holistic and effective approach to third party supplier risk management.

Scope

The objective of this review was to assess the adequacy of design and current operating effectiveness against industry good practices, PwC's interactions in the market, and the key controls established (where appropriate) to ensure LPF has appropriate processes and procedures in place to manage its third-party suppliers.

Risks

The review also assessed the following LPF risks:

- **Supplier and third-party systems** - inadequate, or failure of, supplier and other third-party systems (including IT and Data security).

Our assessment included matters that we consider relevant based on our understanding of the key risks to the organisation.

Limitations of Scope

The following areas were excluded from scope:

- the Procurement function and its underlying processes were not within the scope of this review

- the review did not intend to be a complete traceability mapping exercise to regulatory/legislative requirements; hence we have not provided a view or opinion on whether LPF is compliant with the relevant regulatory requirements

- while this review considered due diligence and ongoing monitoring requirements, a detailed review of risk domains such as Information Security of third-party suppliers was not included in the scope of this review. This will be considered as part of the LPF Information Security Arrangements internal audit currently underway

- recognising that the framework has recently been implemented and therefore evidence of operational effectiveness may be limited, this review focused predominantly on the design of the framework.

Reporting Date

Testing was undertaken between 13 January 2023 and 10 February 2023.

Our audit work concluded on 10 February 2023, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Supplier management processes for Critical Suppliers

Finding Rating	High Priority

Critical supplier relationships should be managed in line with industry good practices to ensure LPF can exercise effective management, governance and oversight over critical outsourcing arrangements.

Our review noted the following issues with the design and operating effectiveness of LPF's supplier management processes for two critical suppliers, Charles River, and Northern Trust:

1. Business case documentation for Charles River and Northern Trust was not available therefore we were unable to assess whether onboarding processes for critical suppliers are fit for purpose.

2. Supplier monitoring of Charles River has not been carried out in line with the process detailed in the Supplier Management Framework, as detailed notes of key review meetings for Charles River have not been documented.

3. Due diligence has not been completed consistently, as documentation provided (such as additional external assurance documentation) for Northern Trust was not as comprehensive as that provided to us for Charles River.

4. The criteria used to categorise Tier 1 suppliers does not refer to suppliers which are 'critical to the LPF Group's compliance with law and/or regulation'.

5. Management advised that an incident involving Charles River which prevented LPF employees from carrying out their role occurred but was not formally reported internally to LPF Risk & Compliance until two weeks after identification, which indicates that internal compliance reporting processes are not operating effectively.

Risks

Supplier and third-party systems

- inadequate risk management processes for critical suppliers could result in regulatory censure as well as over reliance on dominant service provider(s) for core functions, potentially leading to loss of service on the collapse or withdrawal of that provider, and customer harm/loss. This risk is further elevated due to a limited understanding of the critical supplier risk profile.

- inadequate, or failure of, supplier and other third-party systems (including IT and Data security).

Recommendations and Management Action Plan: Supplier management processes for Critical Suppliers

Ref.	Recommendation	Agreed Management Action	Owner	Contributors	Timeframe
1.1	Business case documentation for all critical suppliers should be stored in line with LPF's record keeping policy.	LPF will review records for existing critical suppliers, and ensure that business case documentation is stored in correct supplier files. Supplier management policy will be	Chief Executive Officer (LPF)	Head of Legal (LPF)	30/09/2023

		updated to specify where supplier records, such as business case, should be stored.			
1.2	Tier 1 supplier monitoring should be carried out in line with LPF's documented supplier monitoring process. This includes the documentation and retention of detailed notes and individual meeting dates to ensure that meetings are taking place in line with agreed frequency.	LPF will carry out targeted training for Tier 1 supplier owners on monitoring, and consider appropriate oversight via RMG reporting.		Head of Legal (LPF)	30/09/2023
1.3	Due diligence should be consistent in terms of the level of scrutiny applied to critical suppliers. Management should ensure that annual due diligence for Northern Trust (and all Tier 1 suppliers) is aligned with Charles River in that recent vulnerability assessment results, penetration test reports and other external assurance reports are obtained and reviewed.	As part of action 1.2, targeted training will cover annual due diligence. Supplier framework document review will consider due diligence templates or checklists with set items, tailored to specific tiers.		Head of Legal (LPF)	30/09/2023
1.4	The tiering criteria used should be amended so that Tier 1 suppliers include those suppliers which are critical to the LPF Group's compliance with law or regulation. Cost of the supplier contract generally should not factor into the assessment of materiality (e.g., Tier 2 suppliers). To avoid subjectivity, the tiering criteria should include key areas highlighted by regulators including the potential impact of a disruption, failure, or inadequate performance of the firm's business continuity, operational resilience, and operational risk.	LPF will review and define the tiering criteria (part of action 3.1), then review tier classification of existing suppliers.		Head of Legal (LPF)	30/09/2023
1.5	Management should communicate the incident reporting policy to all LPF employees, to ensure that incidents are reported in line with documented incident reporting processes.	LPF will recommunicate existing incident reporting policies to all employees.		Chief Risk Officer (LPF)	30/06/2023

Finding 2 – Contract exit planning

Finding Rating	High Priority

Contract exit plans should provide for all scenarios and should be periodically tested and updated. Consideration should also be given to 'stressed' exits where withdrawal from a supplier relationship is sudden (such as liquidation or insolvency); and viable forms of exit from supplier relationships from such scenarios, with a focus on the ongoing provision of important business services following a stressed exit.

During the audit we noted the following gaps in relation to exit planning:

1. LPF does not have a defined exit planning process or strategy.
2. LPF does not have exit plan templates in place.

Risks

Supplier and third-party systems

- supplier Management Framework may not provide adequate guidance on roles and responsibilities for managing third party arrangements.
- exit plans are not fit for purpose, exceeding LPF's risk appetite and could expose LPF to business disruption.

Recommendations and Management Action Plan: Exit planning

Ref.	Recommendation	Agreed Management Action	Owner	Contributors	Timeframe
2.1	Management should define an exit planning process or strategy for the exiting of a supplier relationship under 'stressed' and 'non-stressed' scenarios. This should also consider the materiality of a supplier e.g., exit plans for Tier 1 suppliers should be tested and signed off by an appropriate level of management.	LPF will define the supplier exit process, as part of supplier management process review and refresh. See action 3.1.	Chief Executive Officer (LPF)	Chief Risk Officer (LPF) Head of Legal (LPF)	30/06/2023
2.2	Management should create an exit plan template which can be used as part of the Supplier Management Framework.	LPF will create an exit plan template, as part of the exit plan process. See action 3.1.			30/06/2023

Finding 3 – Design of the Supplier Management Framework

Finding Rating	Medium Priority

LPF's Supplier Management Framework should provide end-to-end coverage of the Third Party Risk Management lifecycle.

Our review noted that the LPF Supplier Management Framework does not include a sufficient level of detail around the following key areas:

1. Material outsourcing (e.g., outsourcing of an Important Business Service including regulated activities) vs. non-material outsourcing
2. Supporting process documents
3. Approach to intra-group arrangements
4. Approach to contracting and written agreements
5. Roles and responsibilities (particularly with regards to the Council)
6. RACI matrix
7. Defined risk appetite
8. Risk and issue identification and management processes
9. Exit planning and business continuity plans and processes for suppliers
10. Procedures for the identification, assessment, management, and mitigation of potential conflicts of interest
11. Supplier incident reporting

Risks

Supplier and third-party systems

- insufficiently articulated framework or supporting procedures and guidance for the management of third-party supplier risk, resulting in a lack of clarity over roles and responsibilities, governance, and oversight.

- an inadequate governance framework and structure would fail to ensure effective management of third party arrangements by LPF, leading to potential undermining of LPF's ability to provide a continuous and satisfactory service to its policyholders.

- receiving services without adequate contractual protection which could result in LPF not being able to sufficiently control and monitor its relationships with third party suppliers.

Recommendations and Management Action Plan: Design of the Supplier Management Framework

Ref.	Recommendation	Agreed Management Action	Owner	Contributors	Timeframe
3.1	The Supplier Management Framework should be updated to include the following: 1. Clarification on LPF's approach to material outsourcing and if/how it differs to non-material outsourcing. 2. Links to supporting process documents such as ICT Security assessment and DPIA guidance.	LPF will review existing Supplier Management Framework document and all related supporting document (templates, checklists), and update. New supporting documents will be created where necessary.	Chief Executive Officer (LPF)	Chief Risk Officer (LPF) Head of Legal (LPF)	30/09/2023

9

3. Detailed approach to intra-group arrangements including LPFI and LPFE Limited.
4. A defined process for contracts and written agreements (e.g., at what point Legal function is engaged and relevant approval flow).
5. A RACI matrix which includes key business functions (e.g., Legal, ICT Security, DPO, Board) and the Council.
6. Amendment to Roles and Responsibilities section to include the Council.
7. Risk appetite should be developed to detail how Key Risk Indicators (KRIs) should be applied when managing supplier risk and linked to the LPF Group's overarching risk management framework and risk appetite.
8. Risk and issue identification and management process should be outlined or linked within the framework.
9. A business continuity process for suppliers
10. A process for identifying and managing potential conflicts of interest.
11. A process for supplier incident reporting.
	1) Existing Supplier Management Framework review will be updated to ensure it covers:
	  • Onboarding process, including approval flows and RACI matrix
	  • Tiering criteria, and tiering approval checks
	  • Exit processes
	  • Approach to outsourcing
	  • Approach to Intra-group arrangements
	  • CEC role and responsibilities
	  • Links or clarifications on application of existing processes to suppliers e.g. Contract review; DPIA, IT assessment, risk appetite, risk and issue reporting, incident reporting, conflicts, business continuity
	
	2) New supporting documents will be created to cover:
	  • Onboarding process / checklist
	  • Exit plan template / checklist
	  • Legal contract review process / checklist
	  • Legal standard contract template
	  • Critical supplier due diligence review templates (may replace existing monitoring template)
		Service Director, Finance and Procurement (CEC)
		
		Interim Head of Commercial and Procurement Services (CEC)

Finding 4 – Supplier onboarding processes

Finding Rating	Medium Priority

Robust onboarding processes help to support effective management and oversight of risks posed by new suppliers and the services provided by them.

Our review identified the following issues which indicate that LPF's onboarding processes require further development to ensure that they are adequately designed and operating effectively:

1. There is no internal secondary review of the tiering assessment, or its outcome carried out during the onboarding process. Therefore, there is limited assurance that the tier assigned to a given supplier is correct and proportionate to the risk posed by it.

2. Certain aspects of the Legal review process do not provide adequate contractual protection, including the following:

   a) LPF's standard Terms and Conditions do not contain the following key clauses:
   - Frequency of review of Key Performance Indicators (KPIs)
   - Business continuity clauses
   - Right to audit, incident handling and reporting
   - Exit planning and strategy

   b) LPF's contractual review checklist does not include the following expected checks:
   - Right to audit
   - Supplier incident handling and reporting
   - Business continuity clauses

   c) LPF's contractual review checklist lacks clarity with regards to which suppliers require a clearly defined set of KPIs.

3. In addition, there is no mechanism in place to alert the ICT Security team that a supplier ICT security assessment has not been carried out.

Risks

Supplier and third-party systems

- inadequate onboarding processes could result in LPF onboarding an inappropriate supplier that is not capable of providing the required services to the requisite level.
- inadequate, or failure of, supplier and other third-party systems (including IT and Data security).

Recommendations and Management Action Plan: Supplier onboarding processes

Ref.	Recommendation	Agreed Management Action	Owner	Contributors	Timeframe
4.1	Management should consider the inclusion of an internal secondary review of the tiering assessment and its outcome during in the onboarding process. This should be carried out by an appropriate level of management when a supplier's tier has been assigned.	LPF will implement a review of the tiering assessment during the onboarding process (action 3.1)	Chief Executive Officer (LPF)	Chief Risk Officer (LPF) Head of Legal (LPF)	30/09/2023

| 4.2 | LPF's Supplier Contract Legal review process should be amended to include the following:

1. Addition of the following clauses to LPF's standard Terms & Conditions:
  • Frequency of review of KPIs
  • Business continuity clauses
  • Right to audit
  • Incident handling and reporting including defined timelines
  • Exit planning and strategy
2. Addition of the following checks to LPF's contractual review checklist:
  • Right to audit
  • Supplier incident handling and reporting including defined timelines
  • Business continuity clauses
3. LPF's contractual review checklist should be amended to clarify criteria for which suppliers require a clearly defined set of KPIs. Generally, language like 'if appropriate' should be avoided. | LPF will review the existing contract review process, add suggested checks to the checklist. (overlap with action 3.1). | | Head of Legal (LPF) | 30/06/2023 |
| 4.3 | LPF's supplier onboarding process should include a clear mechanism which notifies the ICT Security team if an assessment is not carried out. This could include the inclusion of a requirement to notify ICT Security if a supplier service processes LPF data/confidential data. | LPF will review the supplier onboarding process as part of Supplier Management Framework document update (action 3.1), and introduce a clearer, centralised process with defined approvals to be followed for all new suppliers. | | Chief Risk Officer (LPF)

Head of Legal (LPF) | 30/09/2023 |

Finding 5 – Ongoing monitoring and oversight

Finding Rating	Medium Priority

Ongoing monitoring controls support LPF Senior Management and their ability to demonstrate adequate and appropriate oversight over supplier management activities.

During the audit, the following issues were noted with regards to ongoing monitoring and oversight:

1. LPF's supplier database and the data fields included are not in line with industry good practices.
2. The Council's roles and responsibilities in relation to overseeing and managing third party supplier relationships for LPF are not defined.
3. LPF's governance structure does not sufficiently cover supplier management.

Risks

Supplier and third-party systems

- management may not receive appropriate visibility of key risks, issues, escalations, incidents, and threats preventing effective decision making, remediation and management of third-party risks.

- the Supplier Management Framework may not provide adequate guidance on roles and responsibilities for managing supplier arrangements, which could result in ineffective supplier risk management.

Recommendations and Management Action Plan: Ongoing monitoring and oversight

Ref.	Recommendation	Agreed Management Action	Owner	Contributors	Timeframe
5.1	Management should consider the following actions: 1. Inclusion of data fields to record recent supplier assessments (e.g., ICT Security, The Data Privacy Impact Assessment (DPIA) carried out as well as their outcomes. 2. The supplier database should also be reviewed by an appropriate level of management and the results of this review should be stored somewhere easily accessible to enable LPF Senior Management to exercise effective oversight of suppliers.	LPF will enhance existing supplier database to include additional data fields, including dates of IT assessment and DPIA, and links to full records. A review of the database will be established, with results provided to senior management as part of RMG oversight.	Chief Executive Officer (LPF)	Chief Risk Officer (LPF) Head of Legal (LPF)	30/09/2023

5.2	The Council's role and responsibilities in relation to supplier management and oversight for LPF should be defined in the Supplier Management Framework document.	This will be documented as part of refresh of Supplier Management Framework document (3.1).			30/09/2023
5.3	Management should consider the following: 1. Inclusion of a supplier management section within the Risk Management Group (RMG) pack and Terms of Reference (ToR). 2. Addition of a version control and review history section to the Risk Management Group's Terms of Reference. In addition, the Terms of Reference should be reviewed annually to ensure they are relevant and up-to-date. 3. Supplier management should be included as a distinct agenda item at the RMG. The discussion could include issues identified relating to Tier 1 suppliers, recent Tier 1 suppliers onboarded, and consideration of exit strategies and plans.	LPF will update RMG responsibilities to include supplier management, and consider how best to incorporate into existing agenda and MI. LPF will add document control to RMG Terms of Ref, including version history and frequency of review.		Chief Risk Officer (LPF)	30/06/2023

Finding 6 – Supplier Management Training and awareness

Finding Rating	Low Priority

Training and awareness controls support core third party supplier management procedures and help to ensure LPF employees are aware of their roles and responsibilities in relation to supplier management.

During the audit, we noted that there is no risk training or awareness programme in place at LPF for supplier management.

Risks

Supplier and third-party systems

- training is insufficient, inadequate, or misaligned to recognised good practices which could result in LPF employees not carrying out their role as effectively as possible with regards to Third Party Supplier management.

Recommendations and Management Action Plan: Supplier Management Training and awareness

Ref.	Recommendation	Agreed Management Action	Owner	Contributors	Timeframe
6.1	Management should consider establishing a supplier management risk training and awareness programme, for all employees and new joiners with a role within supplier management. The training and awareness programme should be reviewed annually or in line with any material changes to ensure that it remains relevant and up-to-date, and employees should be required to complete regularly to ensure sufficient knowledge and awareness.	LPF will carry out training and awareness following update of all documents and processes referred to in other actions; and consider how to incorporate into existing annual training plan and onboarding.	Chief Executive Officer (LPF)	Chief Risk Officer (LPF) Head of Legal (LPF)	31/12/2023

Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed	🟢	Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory	🟢	Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity	🟠	Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity	🔴	Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	**N/A**	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and LPFs objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and LPF's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that LPF's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with several significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that LPF's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Appendix 2 - All LPF outstanding audit actions as at 9 February 2023

Audit	Date raised	Recommendation Title	Recommendation	Agreed Management Action	Priority Rating	Date Due
LPF – Bulk Transfers	13/08/2021	LPF2001 - Rec 1.1 Management oversight of external project management	LPF management should review and project plans; delivery progress; and the overall project RAG (red, amber, green) status to confirm their completeness and accuracy, and actively challenge external project managers to understand the reasons for any delivery delays, and their overall impact on the project. Details of this review and challenge should be recorded in project board / governance meeting minutes and logs, with appropriate action implemented by the external project manager to ensure that any concerns raised by the LPF management team are effectively addressed.	LPF commissioned specialist project management services from Hymans Robertson LLP in order to draw upon its expertise and experience in large scale LGPS bulk transfers. Accordingly, in light of the audit feedback, LPF sought and received comment from the company thereon. The key extract is: "Each Highlight report has the narrative to acknowledge that dates can and do move throughout the project – an example is noted as follows: Some milestone dates in the highlight report have altered since the last report, this is due to movement on some activities and refining of the plan. We would only expect to change any RAG status if there was a negative impact as a result of any delays. In a project like this, we know that there are a number of activities where issues can arise that are outside of our control, however we can we build in contingency to help manage them.

In both scenarios, the signing of the Actuaries letters and the provision of DSAs, there was no negative impact on critical activities, therefore the RAG would remain Green and on track. Progress on each of these areas were discussed at the project meetings. As a result of the feedback, for future reports, the description of the RAG status at the foot of the highlight report will be updated to be more specific around the impact of any date changes to avoid any ambiguity." LPF echoes the sentiments expressed by Hymans Robertson LLP. Accordingly, with an expectation that a RAG status would only change if there was a negative impact as a result of any delays, LPF considers that the project management provided appropriate oversight and control. As stated, however, to avoid any potential ambiguity in future, suitable clarification will be embedded in procedures for any similar exercises. | Low Priority | 31/12/2024 |
| LPF – Bulk Transfers | 13/08/2021 | LPF2001 - Rec 2.1 Maintenance and oversight of a data transfer issues log | For any future data transfer exercises, LPF should maintain a data transfer issues log that should include but not be restricted to: A description of the errors identified; The date they were identified; The significance of the errors (for example, high, medium and low); What action is being / has been taken to correct the error;Who is addressing / has addressed the error; and Date of resolution.The issues log should be reviewed by an independent team member to: Confirm that all issues identified have a clear action, owner, and implementation date for resolution; Confirm that there is satisfactory progress with resolution of all significant issues prior to implementation date; andEnsure that any concerns in relation to lack of implementation progress is escalated to senior management.A sample review of actions completed to address data quality issues identified should be performed prior to live implementation to confirm that issues have been closed appropriately, and that evidence has been retained (where possible) to support their closure. Appropriate evidence of this review (including details of the sample testing methodology applied) should also be retained. | LPF accepts the recommendation.
As part of the process (outlined in the implementation study), the Fund's software supplier Aquila Heywood provided system generated reports reconciling the number of members transferred and several data items. This provided assurance that data taken from the ceding funds and loaded into LPF TEST service was identical. Any issues would have been flagged up at that time. Following receipt of these reports (which showed that the information between ceding fund and LPF tallied), LPF carried out a further data cleansing exercise using a portal created by the Actuary. This is an additional step in the process that LPF chose to do to ensure the quality of transferred data (please see Appendix B of the Fund's Funding Strategy Statement). The number of errors identified by this further cleanse was extremely small and covered only minor issues. An example was a postcode warning for an overseas pensioners – this is due to the difference in formats of UK and overseas postcodes. The small number of errors identified could be resolved very quickly and easily. Further data quality assurance was obtained in carrying out more than one parallel payroll run.LPF acknowledges that this transfer included a relatively small number of members and that data in this case was of a high standard, and that subsequent transfers may involve greater member numbers and poorer quality data. | Medium Priority | 31/12/2024 |
| LPF – Bulk Transfers | 13/08/2021 | LPF2001 - Rec 2.2 Completion of parallel payroll runs | When performing parallel payroll runs to confirm the accuracy of payroll data prior to live transfer, LPF should implement a formal process for confirming satisfactory completion of the payroll run and / or ensuring that all issues identified are recorded in the issues log (refer recommendation 1.1.). This could be confirmed via email to management confirming, as a minimum:The source of the data used;The month for the payroll run;The name of the team member who initiated and performed the payroll run;The name of the other team member who closed the payroll run;Confirmation that significant issues were / were not identified and will be addressed prior to live implementation; andConfirmation regarding whether the live implementation date can still be achieved. | LPF accepts the recommendation.
Parallel payroll runs were carried out using a process set out by the Fund's software supplier which has been developed and used successfully on many other occasions, together with documented processes for running payroll which are already fully documented and integrated within LPF. LPF's decision to carry out more than one parallel payroll run provided additional assurance that information supplied was correct. | Medium Priority | 31/12/2024 |
| LPF – Bulk Transfers | 13/08/2021 | LPF2001 - Rec 2.3 Review of membership communication listing | For future communications with members, LPF should ensure that:A reconciliation is performed between the total members on the communication list to the complete list of transferring members from the ceding funds;An independent review of is performed of the nature of communications (communication labels) to be provided to members to confirm their accuracy based on membership status and other relevant information;The listing contains details of the preparer and reviewer, and relevant dates; andThe reviewed listing is distributed by email communication to ensure a trail of accountability. | LPF accepts the recommendation.
Following the successful completion of the transfer, a system generated report listed all member data required for communications. This report was generated for members of each ceding fund and showed member status and member address. No differentiation in communication was required for active and deferred members (i.e. all active members received the same letter, and all deferred members received the same letter). As reports were produced by ceding fund and member status was included, the data was available in order to successfully identify which pensioner letter was to be used. Prior to sending letters, proofs were spot-checked against the initial report and LPF's Communications Partner reconciled the numbers back to the original report and confirmed with the Employer and Member Payroll Manager. | Medium Priority | 31/12/2024 |

LPF – Technology Model Development	03/03/2022	LPF2003 Recommendation 3.1.2: Post-Implementation Activities	1. A post-implementation review on the migration to the new externally hosted LPF technology network has not yet been performed or planned to identify improvements that could be applied to subsequent projects.LPF management has advised that a post implementation review will be completed by the end of December 2021. 2. Whilst user manuals are in place for some LPF third party hosted systems such as Charles River, Altair, and the Cased Dimensions technology, not all systems have manuals, such as Moorepay, Legal e-sign, and Bamboo.	LPF have produced user manuals and documentation for key/business critical systems and will review the requirements and suitability of the currently available generic documentation for the others during 2022.	Medium Priority	31/12/2022
LPF Risk Management	23/08/2022	LPF2103 2.1 Recommendation: Maintenance of risk registers	LPF management should: a) Review the risks included in the risk registers and ensure they are appropriately articulated. b) Agree definitions of Low/Medium/High impact and likelihood assessments and embed their application at risk subgroups.c) Review the controls listed in the corporate risk register to ensure that they are appropriately articulated in line with the who, what, why, and how control description principles included at Appendix 3 in this report. d) Ensure that all mitigating actions are specific, measurable, achievable, realistic and timely.	Likewise, we will look to re-review the sub-group registers (and tie-in with main group register) with these points in mind We will consider within Risk Management Group (RMG) and report back through the usual channels with any updates arising.	Low Priority	31/03/2023
LPF Risk Management	23/08/2022	LPF2103 1.1 Recommendation: Aligning corporate risks with strategic objectives and risk definitions	1. Management should review the current population of LPF corporate risks to confirm that they are complete and ensure that they align with the strategic objectives and goals set out in the LPF Strategy and Business Plan. 2. Risk definitions should be established for each risk category; agreed by management; and communicated across LPF for ongoing reference when identifying and assessing risks.	We will look to re-review our risks with this finding in mind and use it as an opportunity to step back and consider more holistically the risks we capture and how we can effectively manage and cascade granularity of definition with both ongoing operational risk management and reporting/governance in mind. The Risk Management Group (RMG) does seek to do this on an ongoing basis, and to strike the important balance between maintaining and reporting on the right number of risks (omitting gaps) and distracting the focus away from critical risks/strategic analysis with too much detail, but this is a helpful and timely point to review this. We will consider within RMG and report back through the usual channels with any updates arising.	Medium Priority	31/03/2023
LPF - Project Forth Programme Assurance	11/01/2023	LPF2201 2.1 Recommendation: Assurance plan	The Council and LPF should agree and plan internal audit, and any other programme assurance related activities such as those over data migration. These should be entered onto the plan to support key project milestone stage gates.The deviation from the planned assurance as per the PID should also be tabled at Steerco for visibility/transparency.	To ensure good project governance is maintained, LPF will propose a further review is included in CEC IA's 23/24 plan, to be scheduled after council approval. Meanwhile regular project updates will be shared with CEC IA as part of routine BAU meetings.In addition, place markers for audits are noted on the Plan on a Page ('POAP'). Once dates are provided the project plan and the POAP can be updated. An update on the PwC audit will be provided verbally to Steering Group in December 2022. The deviation will be raised at that time.	Medium Priority	31/03/2023
LPF - Project Forth Programme Assurance	11/01/2023	LPF2201 3.1 Recommendation: Benefits Management plan	A formal Benefits Management plan/approach should be documented, approved, and communicated to all appropriate stakeholders. Typically, this would include plans for at least: identification/ evaluation/ planning/realisation.review. The plan/approach should be referenced in the PID, and benefits should be mapped to specific tasks, risks, and deliverables.	A Benefits Management plan will be created post merger approval. Meanwhile a task to create the benefits management plan on the project plan will be referenced in the PID.	Medium Priority	30/06/2023
LPF - Project Forth Programme Assurance	11/01/2023	LPF2201 4.1 Recommendation: Formal Risk Management approach	A formal Risk Management plan/approach for identifying and capturing risks, assigning owners, and tracking and mitigating risks should be documented, approved, communicated to all appropriate stakeholders, and referenced to in the PID. The RAID log should be updated to include the milestones, dependencies, and benefits (see finding 5) that are impacted by each risk. The revised Business Case should be used as a source for this exercise; this will create clear linkage between, and visibility of, all key project documentation.	Project approach to risks will be added to the PID and shared at Steering Group and Working Group. The RAID log notes the deliverable the risk relates to. This will be enhanced to cover risks being raised against milestones and dependencies where appropriate	Medium Priority	31/03/2023
LPF - Project Forth Programme Assurance	11/01/2023	LPF2201 5.1: Recommendation: Quality Management plan	A formal, risk based, quality management plan should be documented, approved by all key stakeholders, and referenced to in the PID, RAID, and all other appropriate governance documentation.The plan should be robust and cover, at minimum, the following elements: quality planning,/ assurance (testing) /control /continuous improvement/ roles and responsibilitiesManagement should also ensure that staff used for assurance/testing are appropriately skilled i.e., have received appropriate training.	The WIDs highlight success criteria alongside deliverables for each workstream. The workstream lead is responsible for the quality of delivery of the workstream and each workstream has an executive (SLT) sponsor overseeing this. Additional scrutiny is provided by the steering group who have ultimate accountability. Specific and explicit quality assurance will be put in place for specific deliverables. We are particularly focussed on proportional quality management especially regarding the Heywood Migration Plan, employee consultation and TUPE, and the IT Data Transfer Plan, and will consider quality criteria, as appropriate.	Low Priority	30/06/2023
LPF - Project Forth Programme Assurance	11/01/2023	LPF2201 6.1 Recommendation: Absence of a Data Migration plan	As soon as is practicable after merger approval, a migration plan should be agreed with Heywoods; this should be included in all appropriate governance documentation. This should cover, at minimum:completeness, accuracy, and timeliness of data migration / definition of an agreed 'cut off' point for existing systems / roles & responsibilities i.e., Access, administration, change control etc.Any additional features / changes within the existing Heywoods application should also be documented as a user training manual post migration.	Placeholder exists in the project plan for the Heywood Data Transfer Plan, which will be the migration plan. This will be tailored to the project requirements as agreed by the Operations WSL. A mini data discovery session is planned between Heywood and LPF during Q1 to baseline some high-level expectations and enable costs to be proposed on a more informed basis.	Low Priority	30/06/2023
LPF - Project Forth Programme Assurance	11/01/2023	LPF2201 7.1 Recommendation: Critical path	Management should: define a 'critical path' and ensure that all workstream leaders understand it - particularly the key milestones, create an escalation process to address any threats to the critical path at the earliest opportunity - this could be done through the RAID log, document the impact of the critical path through all workstreams, considering findings 1 - 6.	The critical path cannot be properly defined until the legal structure has been agreed and consequent required actions and activities determined. In the meantime, PMO will create an event driven critical path. This will be shared at Steering Group and Working Group meetings. Threats to the critical plan will be reflected in the RAID where appropriate.	Low Priority	31/03/2023

| LPF - Project Forth Programme Assurance | 11/01/2023 | LPF2201 1.1 Recommendation: Change Management policy | Management should formally document, approve, and communicate the current informally applied change management policy to all appropriate stakeholders. This should reference all currently used documents and should cover: what constitutes a significant change, when/how to undertake change, the documentation levels required, potential Red, Amber, Green (RAG) ratings, resolution times for each priority level currently defined in the RAID log.Once complete, this policy should be referred to in the Governance policy document (V1.1), as well as the RAID log to link all existing project governance documentation. | Project approach to change will be added to the PID and shared at Steering Group and Working Group. The RAID log summarises the change request, which is held in the project documentation. | Medium Priority | 31/03/2023 |