Pensions Audit Sub Committee

2.00pm, Monday, 11 December 2017

Lothian Pension Fund Internal Audit Update - 1st September 2016 to 31st October 2017

Item number	5.2
Report number	
Executive/routine	
Wards	All
Council Commitments	Delivering a Council that works for all

Executive Summary

The purpose of this report is to provide a summary of Internal Audit Activity for Lothian Pension Fund (LPF) during the period 1st September 2016 to 31st October 2017, and details of open and overdue Internal Audit recommendations as at 26th October 2017. Overdue recommendations are those that have not been closed by the agreed implementation date.

Of the three reviews included in the 2017/18 audit plan, one has been completed, with one at draft reporting stage and another in progress.

One further review was added to the 2017/18 Internal Audit plan (in September 2017) at the request of LPF management. This review assessed the design of the data security arrangements for a potential third party supplier who was being considered as an outsource provider for the LPF payroll. Given the commercially sensitive nature of this review, a progress update has been included in a separate B Agenda paper.

LPF had 3 open Internal Audit recommendations as at 26th October 2017. Of these, one had not been closed by the agreed implementation date and was reported as overdue to the City of Edinburgh Council's Corporate Leadership Team (CLT).

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Report

Lothian Pension Fund Internal Audit Update - 1st September 2016 to 31st October 2017

1. Recommendations

Committee is requested to:

1.1 Note Internal Audit activity and outcomes for period 1st April to 31st October 2017, and the status of LPF open and overdue Internal Audit recommendations as at 26th October 2017.

2. Background

2.1 The Internal Audit plan for the Lothian Pension Fund (LPF) was approved by the Pensions Committee on 20th March 2017 and includes the following three reviews.

- Business Continuity - Review of the Fund's Business Continuity Plan including IT disaster recovery for systems hosted by the Council and third party system providers.
- Information governance – Assessment of the processes and controls in place to ensure member data held by the Pension Fund is accurate, and is managed in compliance with Data Protection legislation.
- Pensions tax lifetime and annual allowances - Review of arrangements in place to ensure that pensions tax legislation is applied accurately, and that members are informed of its impact on their future pension provision.

2.2 One further review was added to the 2017/18 Internal Audit plan (in September 2017) at the request of LPF management. This review assessed the design controls operated by a potential third-party supplier who was being considered as an outsource provider for the LPFE payroll. Given the commercially sensitive nature of this review, a separate update has been provided and will be considered as B agenda item.

2.3 Internal Audit recommendations and agreed management actions are tracked monthly, with details of overdue recommendations (those that have not been closed by the agreed implementation date) reported monthly to the City of Edinburgh Council's Corporate Leadership Team and quarterly to the Council's Governance, Risk, and Best Value Committee. Evidence provided by management to support closure will be reviewed, validated, and tested (where appropriate) by Internal Audit to confirm that agreed management actions have been effectively implemented and the risks identified in the original audit report effectively managed

3. Main report

3.1 The current status of the audits included in the LPF Internal Audit plan is as follows:

- Information Governance – completed. The final report was issued in October 2017. Refer section 3.2 below for further detail.
- Payroll Outsourcing review - in progress. Further detail is included in a separate B agenda paper.
- Business Continuity – draft report has been shared with LPF for management responses. Final report is expected to be issued by end November.
- Pensions tax lifetime and annual allowances – in progress. Final report will be issued in December.

3.2 **Information Governance** - The scope of this review assessed the design and operating effectiveness of the controls in place to mitigate the risk that members' confidential data is lost or made public/breach of the Data Protection Act.

Our review confirmed that whilst no significant Data Protection Act breaches had been recorded by the Lothian Pension Fund (LPF) or were identified from our testing, some moderate weaknesses exist in the design and operating effectiveness of the key records management controls in place. These control weaknesses should be addressed to ensure full ongoing compliance with Data Protection requirements and ensure that the Fund is prepared for the new General Data Protection Legislation currently scheduled for implementation in May 2018.

Consequently, two 'Medium' and three 'Low' rated Findings were raised. For further details of the Findings raised, please refer to the full report which is included at Appendix 1.

4. Open and Overdue Internal Audit Recommendations

4.1 LPF had 3 open Internal Audit recommendations as at 26th October 2017. Of these, one had not been closed by the agreed implementation date and was reported as overdue to the Corporate Leadership Team (CLT). Details of open and overdue recommendations are included in the table below:

Review and Recommendation	Rating	Status	Revised Date	Original Date
Disaster Recovery – CW1602	Medium	Open	-	30/11/17
Service Level Agreements with Outside Entities – RES1605	Low	Open	-	30/11/17
LPF Cyber Security – RES1614	Medium	Overdue	31/03/18	30/09/17

4.2 The Disaster Recovery and Service Level agreements recommendations were allocated across all Service Areas within the City of Edinburgh Council (following agreement by the CLT in September 2017) to enable identification of all shadow IT systems (systems, applications and websites historically procured and implemented by Services that are not managed corporately by the Council's ICT service) and

arm's length organisations that provide services to and receive services from the Council.

4.3 The LPF Chief Risk Officer has provided an update on the overdue LPF Cyber Security recommendation which confirms that progress is being made with development of an LPF supplier management framework to provide assurance over third party Cyber Security controls. This work is being combined with LPFs General Data Protection Requirements (GDPR) project and the Fund's existing risk and compliance controls framework, and LPF is now working to a revised date implementation date of 31st March 2018.

5. Measures of success

5.1 Provision of assurance over the key risks faced by the Fund and effective resolution of control weaknesses identified from audits.

6. Financial impact

6.1 There are no direct financial implications.

7. Risk, policy, compliance and governance impact

7.1 There are no adverse impacts arising from this report.

8. Equalities impact

8.1 There are no adverse equalities impacts arising from this report.

9. Sustainability impact

9.1 There are no adverse sustainability impacts arising from this report.

10. Consultation and engagement

10.1 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.

11. Background reading / external references

11.1 None

Lesley Newdall, Chief Internal Auditor

E-mail: Lesley.newdall@edinbrgh.gov.uk | Tel: 0131 469 3216

12. Appendices

12.1 Appendix 1 – Internal Audit report – Information Governance

Appendix 1

The City of Edinburgh Council

Internal Audit

Lothian Pension Fund - Information Governance

Final Report

13th October 2017

RES1705

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2017/18 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2017. The review is designed to help the City of Edinburgh Council 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 is a number of 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 City of Edinburgh Council. 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 elected members as appropriate.

1. Background and Scope

Background

Lothian Pension Fund ('the Fund') is the second largest local government pension fund in Scotland with over 70,000 members. The Fund holds both personal and sensitive personal data about its members and their next of kin which allows it to perform core functions such as collecting pension contributions and paying pension benefits. The Fund may share this data with employers and service providers for pensions administration and fraud prevention purposes.

This review was included in the 2017/18 Internal Audit Plan to assess the Fund's information governance maturity before the General Data Protection Regulations come into force in 2018, and in response to a number of minor data protection breaches in the past year.

Pensions records are maintained on the pensions administration system, Altair an employer data transfer portal; Pensions Web; the Fund's shared drive; and electronic mailboxes. Altair and Pensions Web are provided by third party suppliers Aquila Heywood and Civica respectively. A Lothian Pension Fund website links to My Pension Online, for members to administer their details and obtain information on the value of their fund.

Scope

The scope of this review assessed the design and operating effectiveness of the controls in place to mitigate the risk that members' confidential data is lost or made public/breach of the Data Protection Act.

Testing, where appropriate, was performed for the period 1 August 2016 to 31 July 2017. For the associated controls objectives and full terms of reference see appendix 2.

2. Executive summary

Total number of findings

Critical	0
High	0
Medium	2
Low	3
Advisory	1
Total	**6**

Summary of findings

Whilst no significant Data Protection Act breaches had been recorded by the Lothian Pension Fund (LPF) or were identified from our testing, our review noted some moderate weaknesses in the design and operating effectiveness of the key records management controls in place. These control weaknesses should be addressed to ensure full ongoing compliance with Data Protection requirements and ensure that the Fund is prepared for the new General Data Protection Legislation currently scheduled for implementation in May 2018.

Consequently, two 'Medium' and three 'Low' Findings have been raised. One 'Advisory' Finding has also been raised reflecting best practice opportunities identified.

From the review the following areas of good practice were identified:

- The Lothian Pension Fund (LPF) website privacy & data protection policies outline the information that may be collected, how it will be used, and who it will be shared with;
- Information governance training has been undertaken by all staff;
- Regular compliance checklists are completed, linked to a breaches log and risk register, and supported by staff briefings, reminders and awareness communications;
- Data entry is automated via standard templates where possible, with manual data entry subject to peer reviews;
- Reconciliations of employers and retired members' data, and data matching for retired members are performed;
- Laptop security is enforced;
- Access to modules within the pensions administration system, Altair, are restricted by job role and connected people, with access change requests reviewed monthly by a Senior Manager;
- The shared drive is well structured and data is easily accessible;
- Contracts with third parties either reference data protection regulations or are supported by data sharing agreements; and
- Preparations for the 2018 General Data Protection Regulations (GDPR) are underway, and compliance with GDPR has been incorporated in the specification for the new pensions system.

Our detailed findings and recommendations are laid out within Section 3: Detailed Findings

3. Detailed findings

1. Records Retention and Disposal

Finding
The Fund's records management framework and supporting processes require improvement to ensure that Fund records are effectively managed in line with Data Protection Act requirements. Our review identified the following control weaknesses: • There is currently no formal records management plan and supporting processes; • Retention schedules and disposal logs are not used to record and action pre-determined disposal dates of Fund records; • Regular clear out days are not held to ensure that electronic and paper records are archived or scheduled for disposal; • Some records are duplicated between Pensions Web and the Fund's shared drive. • No documents have been archived in Pensions Web since its installation in 2013; and • The pensions mailbox is used to store correspondence that has not been attached to the Altair pensions administration system.

Business Implication	Finding Rating
Lack of formal governance supporting records management breaches the requirements of the Council's records management policy (sections 4.5 – 4.8) The lack of a records retention schedule, records management process and disposal log means that decisions are not being made regarding records, files and folders containing sensitive data that no longer requires to be held, or is being held in more than one location.	**Medium**

Action plans	
Recommendation	**Responsible Officer**
Retention and Disposal It is recommended that a records management plan is prepared that sets out the proper arrangements for the management of the Lothian Pension Funds records that include personal data. A model records management plan developed by National Records of Scotland includes 14 elements for effective records management. Whilst there is no statutory requirement for this plan to be applied, it would be good practice to incorporate as many of these elements as possible into existing records management processes where they are not already applied by LPF. The 14 elements of the plan are noted below and further information can be found at: https://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan 1. Senior management responsibility - *An individual at senior level who has overall strategic accountability for records management.*	Chief Risk Officer, Lothian Pension Fund

2. Records manager responsibility - *An individual within the Fund to have day-to-day operational responsibility for records management.* 3. Records management policy statement - *To underpin the effective management of the Fund's records and information.* 4. Business Classification Scheme to organise records - *A scheme describing what business activities the Fund undertakes.* 5. Retention schedules - *A list of pensions records for which pre-determined disposal dates have been established.* 6. Destruction arrangements - *Disposal arrangements must ensure that all copies of a record – wherever stored – are identified and destroyed.* 7. Archiving and transfer arrangements - *Mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions.* 8. Information Security - *Process by which records are protected and ensures they remain available.* 9. Data Protection - *High level statement of public responsibility and fair processing.* 10. Business continuity and vital records plans; - *A business continuity and vital records plan serves as the main resource for the preparation for, response to, and recovery from, an emergency that might affect any number of crucial functions in an authority.* 11. Audit trail - *Sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities.* 12. Competency framework for records management staff - *lists the core competencies and the key knowledge and skills required by a records manager.* 13. Assessment and review - *To ensure that records management practices conform to the Records Management Plan.* 14. Shared information - *Reference to information sharing protocols in place that govern how the Fund exchanges information with others.* When implementing these additional actions, reference should be made to governing legislation and advice available from the Council's Information Governance team. A review should also be performed of existing records held in Altair, Pensions Web, mail boxes and the shared drive to ensure that multiple copies of records are not held, records are held in the most appropriate place, and storage capacity is minimised where possible.	
Agreed Management Action	**Estimated Implementation Date**
Recommendations accepted – all actions recommended by Internal Audit will be fully implemented.	28/02/2018

2. System Access Controls

Finding
Altair Controls: • The current user list for the pensions administration system, Altair, was tested to confirm that access levels in place aligned to job roles. Whilst no inappropriate access rights were identified for LPF staff, a small number of historic users were listed from East, Mid and West Lothian Councils. These Councils previously used the Altair system to access their information, but now use Pensions Web, therefore the Altair user accounts are no longer required. • The Altair user access list was reviewed in July 2017 to identify leavers who should be removed. The outcomes of the review have been presented to management for approval. Shared Drive Access: • Some commercially sensitive records and LPF personnel folders within the LPF shared drive have access restricted to senior managers, however members' data held within the Pensions Admin folder can be viewed by all LPF staff, including those who do not require access to it. • A list of employees who currently have access to the Pensions Admin folder was obtained from CGI. Of 70 individuals with access permission, seven should not have access to this folder, including individuals who have never worked within LPF. A list of exceptions was passed to the Systems Manager for review and resolution. Pensions Web Access: • A Pensions Web LPF user list is not held locally, and is not regularly requested from the systems administrator, Civica, to enable completion of periodic user access checks. • Designated LPF officers are systems administrators for Pensions Web employer users. The full population of current users is reviewed throughout the year, however, the process supporting this quarterly review has not yet been fully embedded, and no evidence of previous checks retained.

Business Implication	Finding Rating
• Members personal data is available to all staff within the LPF which does not afford this data an appropriate degree of protection as required per Data Protection Act requirements. • Access rights to key systems that hold member data has been retained for LPF staff and employers who no longer require access to it.	**Medium**

Action plans	
Recommendation	**Responsible Officer**
System Access Controls Altair Controls • The current user list requires to be reviewed to ensure that all active accounts have a legitimate business purpose. • Any inactive accounts no longer required should be removed, • The system should be updated immediately to reflect any team changes. • An annual review of user Altair user access rights should be performed. Shared Drive Access • Access to shared drive folders containing members' data should be restricted to staff who require access to it. • Access to the shared drive should be updated immediately to reflect any team changes, and should be subject to an annual review. • Any inappropriate access rights identified should be raised with the Council ICT Security Manager as a security breach. Pensions Web Access • A revised list of current LPF users should be obtained from Civica to support each quarterly review performed throughout the year. • Evidence of quarterly reviews performed should be retained together with confirmation that the full population of users has been reviewed during the year.	Chief Finance Officer, Lothian Pension Fund
Agreed Management Action	**Estimated Implementation Date**
Altair Controls Although user accounts existed, these could not be utilised to access the Altair system as the essential first stage log-in through Citrix receiver had been removed for all such users. Following the notification by Internal Audit staff, the user access list was fully revised and deletions made for any users no longer required. Action on the recommendations is summarised as follows: • The current user list requires to be reviewed to ensure that all active accounts have a legitimate business purpose. • Any inactive accounts no longer required should be removed, • The system should be updated immediately to reflect any team changes An annual review of user Altair user access rights should be performed. Shared Drive Access • Access to the Pensions Administration sub-folder will be restricted to appropriate staff. Request will be submitted to the Council's ICT provider, CGI. In every instance, access requests for new starts and terminations for leavers will be submitted to CGI without delay, e.g. legal trainees on temporary placement with Lothian Pension Fund. • LPF will request CGI to provide shared drive user access details on an annual basis to enable them to perform a review and notify CGI of any inappropriate access rights as a security breach.	31/10/2017 31/10/2017 31/10/2017 31/12/2017 31/10/2017 31/10/2017

• Access to Altair and the shared drive will be incorporated into the LPF leavers process to ensure access is removed in a timely manner. <u>Pensions Web Access</u> LPF recognises that, whilst control checks have been performed, processes and outcome reviews have not been formally documented. Accordingly, both recommendations are accepted and will be implemented. • A revised list of current LPF users should be obtained from Civica to support each quarterly review performed throughout the year. • Evidence of quarterly reviews performed should be retained together with confirmation that the full population of users has been reviewed during the year.	31/10/2017 01/11/2017 01/11/2017

3. Fair Processing

Finding
The Pensions website privacy policy & data protection section states that the City of Edinburgh Council is the data controller in terms of the Data Protection Act 1998. This is contrary to the Information Commissioners Office Data Protection Register entry which notes that the data controller is the Lothian Pension Fund. The welcome letter to new scheme members references the website, however it does not specifically draw attention to the privacy policy and data protection content outlined in the website. The Pensions website privacy policy & data protection pages will require revision to comply with GDPR by May 2018, for example, opt outs should be opt ins.

Business Implication	Finding Rating
• There is a lack of clarity as to who the Data Controller is; LPF or CEC • There is a lack of transparency at the point of entry to the scheme as to how new members' data may be used.	**Low**

Action plans	
Recommendation	**Responsible Officer**
Fair Processing • Agreement regarding data controller responsibilities between LPF and CEC should be clarified and the ICO registration and Pensions website updated accordingly. • The welcome letter should be updated to include a reference to the privacy policy and data protection content outlined in the website. • Website privacy policy & data protection pages should be reviewed to ensure compliance with GDPR requirements by May 2018.	Chief Risk Officer, Lothian Pension Fund
Agreed Management Action	**Estimated Implementation Date**
Recommendations accepted – all actions recommended by Internal Audit will be fully implemented.	31/12/2017

4. Monthly Reconciliations

Finding
Automated monthly reconciliations are performed using pension reference numbers to ensure that employers contribution data uploaded by scheme members to Pensions Web is completely and accurately transferred across to the Altair pensions administration system. Exception reports are generated and reviewed to confirm that the full population of records and contribution data submitted has been accurately transferred to Altair. City of Edinburgh Council (CEC) pension reference numbers are regularly changed in the Council payroll system and LPF is not notified. There was a batch change in November 2016 and old and new pension references were not provided, so completeness reconciliations could not be performed for City of Edinburgh Council employees. It was noted that CEC are to provide a report of monthly changes, however the effectiveness of this automated reconciliation control will be reduced as manual intervention will be required.

Business Implication	Finding Rating
Risk that CEC employee contribution data in the Altair system is incomplete and inaccurate with effect from November 2016.	Low

Action plans	
Recommendation	**Responsible Officer**
Monthly Reconciliations • LPF should liaise with CEC to ensure that reports of monthly changes are produced and provided. • Once reports are received from CEC, LPF should design and implement a revised contributions reconciliation process for CEC employees.	Chief Finance Officer, Lothian Pension Fund
Agreed Management Action	**Estimated Implementation Date**
At its meeting on 20 March 2017, Pensions Committee was advised of the following: "City of Edinburgh Council – Pension Record Identifier - The Fund is also addressing data issues caused by the inherent but undesired variability in the City of Edinburgh Council's payroll "position identifier" also being the identifier for pension records. This has caused significant issues as the Council is currently undergoing a review of their services and staff are being given a new identifier as part of this process." The Fund continues to liaise with the Council's payroll staff, both to ensure monthly reports are received and reconciliation to member records is effective timeously.	31/10/2017

5. Clear Desk Policy Compliance Breach

Finding
An after-hours walkabout to test compliance with the clear desk policy confirmed compliance in respect of individual workstations, however, sensitive data had been left in an in-tray in the business centre; payroll data and members statements marked 'returned to sender'. Additionally, LPF management have confirmed that office cupboards are not locked. Whilst there is controlled access to the LPF offices, these documents could potentially be viewed by (for example) by cleaning and maintenance staff with access to the building.

Business Implication	Finding Rating
• Inappropriate access to sensitive personal data and potential Data Protection Act breach. • Non-compliance with LPF clear desk policy.	Low

Action plans	
Recommendation	**Responsible Officer**
After hours clear desk policy checks should be performed across all areas within LPF (including the business centre) to ensure that documents have been secured and cupboards lock with appropriate action taken where any exceptions have been identified.	Chief Executive Officer, Lothian Pension Fund
Agreed Management Action	**Estimated Implementation Date**
Recommendations accepted – all actions recommended by Internal Audit will be fully implemented.	31/10/2017

6. Best Practice Improvement Opportunities

Finding
Two best practice improvement opportunities were noted during the audit: 1. There is no specific procedure or script for requests from Independent Financial Advisors (IFAs) to prompt the requirement for a signed and dated mandate from the member to be provided with any IFA requests. It was noted that most IFAs automatically provide this mandate. 2. The action taken for a data protection breach identified and recorded in the breaches log in relation to members' self-service on 07/12/16 was considered to be inappropriate: *'We have changed the process, and if the member has issues registering we send the activation code by post rather than by e-mail'*. The decision to send activation codes by post appears to be excessive and would mean slower customer service. A more appropriate action would be to remind staff to take care when sending emails, and include a step in the process to delete links after posting / expiry of link after use.

Business Implication	Finding Rating
Business processes not operating as efficiently as possible.	**Advisory**

Action plans	
Recommendation	**Responsible Officer**
Best Practice Improvement Opportunities 1. Process documentation should be updated to ensure that a signed and dated client mandate is requested and received before client information is provided to IFAs. 2. Employees will be permitted to send activation codes via e mail, and a reminder will be issued to ensure employees are aware of the requirement to delete links after posting / expiry of link after use. 3. Review of a sample of activation emails will be performed on an ongoing basis to ensure that activation links have been removed.	Chief Finance Officer, Lothian Pension Fund
Agreed Management Action	**Estimated Implementation Date**
1. Where a request from an IFA is received on behalf of a member, if a signed mandate from the member is not provided with the request, the IFA is asked to provide one. A member's information would not be sent to an IFA without a current mandate.	In place
Our transfer out procedure is in the process of being reviewed and will incorporate IFA requests. The procedure will specify that a member's mandate is required where we get a request for information from an IFA, and that the mandate should be current (i.e. dated no older than a year from the request). If no mandate is provided, or it is out of date, then the IFA will be asked to provide a current one.	31/10/2017
2. This issue was caused by members not being able to locate the system generated email as it was being treated as spam by some email provides such as Hotmail and AOL. We have introduced a paragraph that is included in our email responses that are sent to members on	31/10/2017

how to trace the email and this has resulted in a resolution of most of the issues.	

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation or brand of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***;*** *or* • ***Significant*** impact on the reputation or brand of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's operational performance ; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Appendix 2 – Terms of Reference

Resources – Lothian Pension Fund

Terms of Reference – Information Governance

To: Clare Scott, Chief Executive Officer, LPF

From: Gemma Dalton, Principal Audit Manager Date: 20 July 2017

Cc: Stephen Moir, Executive Director of Resources
John Burns, Chief Finance Officer, LPF
Struan Fairbairn, Chief Risk Officer, LPF
Diane Sinclair, Deputy Pensions Operations & Development Manager, LPF

This review is being undertaken as part of the 2017/18 internal audit plan approved by the Pensions Committee in March 2017.

Background

Lothian Pension Fund ('the Fund') is the second largest local government pension fund in Scotland with over 70,000 members. The Fund holds personal data about its members and their next of kin which allows it to perform core functions such as collecting pension contributions and paying pension benefits. The Fund may share this data with employers and service providers for pensions administration and fraud prevention purposes.

This review was included in the 2017/18 Internal Audit Plan to assess the Fund's information governance maturity before the General Data Protection Regulations come into force in 2018, and in response to a number of minor data protection breaches in the past year.

Scope

The scope of this review will be to assess the design and operating effectiveness of the controls in place to mitigate the following risk:

- Members' confidential data is lost or made public/breach of the Data Protection Act.

Our audit approach is as follows:

- Obtain an understanding of the Fund's information governance processes through discussions with key personnel, review of systems documentation and walkthrough tests;
- Identify the key risks around information governance;
- Evaluate the design of the controls in place to address the key risks; and
- Test the operating effectiveness of the key controls.

Testing, where appropriate, will be undertaken for the period 1 April 2017 to date.

The sub-processes and related control objectives included in the review are:

Sub-process	Control Objectives
Responsibilities & Compliance	• Staff are aware of their information governance responsibilities and what support there is for them. • Staff know how to report an information security or data protection breach. • Information risks and incidents are identified, recorded and managed through the Fund's Risk Management Framework.
Data Quality	• Member data held by the Fund is accurate and reliable.
Protection	• Staff have appropriate access permissions to personal data. • Data is stored, organised, and clearly identified according to the sensitivity of its content. • Data is appropriately protected if it is taken offsite. • Data is secured against theft, loss, and damage. • Any removable media and hosted services (e.g. Apps and websites) are authorised, managed, and reviewed. • Staff use secure Council devices for all tasks where personal data is used or accessed. • Privacy is actively considered and assessed when designing or changing processes.
Data Sharing	• There are data sharing agreements and protocols in place for any routine data sharing undertaken. • Appropriate authorisations are sought from members/powers of attorney in relation to using or sharing their personal data. • Staff know how and when to share information with third parties. • Ad hoc requests for personal data from other organisations are dealt with according to Council policy.
Availability	• Data is available to the right staff in the timeframe needed to meet business need and statutory obligations.
Retention & Disposal	• Records containing personal data are closed and retained or disposed of against the relevant Council retention rule. • Records are disposed of according to the sensitivity of their content. • Redundant, obsolete, and trivial information is routinely identified and cleared out.
General Data Protection Regulations	• Changes required to the Fund's records management processes in order to comply with the General Data Protection Regulations have been identified. • Any such changes identified will be implemented by 25 May 2018, when the General Data Protection Regulations come into effect.

Limitations of Scope

The scope of our review is outlined above and is limited to members' personal data controlled and/or processed by Lothian Pension Fund.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	0131 469 3216
Gemma Dalton	Principal Audit Manager	0131 469 3077
Christine Shaw	Internal Auditor	0131 469 3075

Key Contacts

Name	Title	Role	Contact Details
Clare Scott	Chief Executive Officer, LPF	Review Sponsor	0131 469 3865
John Burns	Chief Finance Officer, LPF	Key Contact	0131 469 3711
Struan Fairbairn	Chief Risk Officer, LPF	Key Contact	0131 529 4689
Diane Sinclair	Deputy Pensions Operations & Development Manager	Key Contact	0131 529 4336

Timetable

Fieldwork Start	19th July 2017
Fieldwork Completed	4th August 2017
Draft report to Auditee	11th August 2017
Response from Auditee	18th August 2017
Final Report to Auditee	25th August 2017

Follow Up Process

Where reportable audit findings are identified, the extent to which each recommendation has been implemented will be reviewed in accordance with estimated implementation dates outlined in the final report.

Evidence should be prepared and submitted to Audit in support of action taken to implement recommendations. Actions remain outstanding until suitable evidence is provided to close them down.

Monitoring of outstanding management actions is undertaken via monthly updates to the Chief Finance Officer. The Chief Finance Officer liaises with LPF officers to ensure that updates and appropriate evidence are provided when required.

Details of outstanding actions are reported to the Pensions Committee on a quarterly basis.

Appendix 1: Information Request

It would be helpful to have the following available prior to our audit or at the latest our first day of field work:

- Records Management Manual, and/or other guidance on data handling issued to the Pensions Administration team

This list is not intended to be exhaustive; we will require additional information during the audit which we will bring to your attention at the earliest opportunity.