Pensions Audit Sub-Committee

2.00pm, Tuesday, 23 June 2020

Lothian Pension Fund - Internal Audit Opinion and Annual Report for the Year Ended 31 March 2020

Item number 5.3

1. Recommendations

The Pensions Audit Sub-Committee (Committee) is requested to:

1.1 note the Internal Audit opinion for Lothian Pension Fund (LPF) for the year ended 31 March 2020, and

1.2 refer the Internal Audit opinion to the Pensions Committee for noting.

Lesley Newdall

Chief Internal Auditor

Legal and Risk Division, Resources Directorate

E-mail: lesley.newdall@edinburgh.gov.uk | Tel: 0131 469 3216

Lothian Pension Fund - Internal Audit Opinion and Annual Report for the Year Ended 31 March 2020

2. Executive Summary

2.1 This report details Internal Audit's (IA) annual opinion for Lothian Pension Fund (LPF) for the year ended 31 March 2020. Our opinion is based on the outcomes of the three audits included in the LPF 2019/20 IA annual plan, and the status of open and overdue IA findings as at 31 March 2020.

2.2 IA considers that the LPF control environment and governance and risk management frameworks are generally adequate but with enhancements required and is therefore reporting an 'amber' rated opinion (see Appendix 1), with our assessment towards the middle of this category.

2.3 This assessment remains unchanged in comparison to the 2018/19 IA opinion.

2.4 The key themes emerging from the outcomes of the three completed 2019/20 audits highlight the need for LPF to ensure the continued effectiveness of their third party supplier relationship management framework, and focus on the adequacy of cloud based system controls for systems provided and maintained by external suppliers that are used by LPF to support their ongoing investment and fund administration activities.

2.5 This report is a component part of the overall annual assurance provided to LPF, as there are a number of additional assurance sources that the Committee should consider when forming their own view on the design and effectiveness of the control environment and governance and risk management frameworks within LPF.

3. Background

3.1 The Public Sector Internal Audit Standards (PSIAS) provide a coherent and consistent internal audit framework for public sector organisations. Adoption of the PSIAS is mandatory for IA teams within UK public sector organisations, and PSIAS require annual reporting on conformance.

3.2 It is the responsibility of the Council's Chief Internal Auditor to provide an independent and objective annual opinion on the adequacy and effectiveness of LPF's control environment and governance and risk management frameworks in line with PSIAS requirements. The opinion is provided to the Pensions Audit Sub-Committee, and should be used to inform the LPF Annual Governance Statement.

3.3 Our opinion is based on the outcome of LPF audits completed in the 2019/20 financial year, and the status of open internal audit findings as at 31 March 2020.

3.4 Given LPF's dependence on the City of Edinburgh Council for a number of support services (most notably Digital Services in partnership with CGI for provision network; security; and technology support services), we have also considered the outcomes of relevant work performed on the Council's control environment and governance and risk management frameworks. The Council's 2019/20 annual IA opinion is currently scheduled for presentation to the Governance, Risk, and Best Value Committee meeting in August 2020.

4. Main Report

4.1 2019/20 Internal Audit Opinion

4.1.1 IA considers that the LPF control environment and governance and risk management frameworks are generally adequate but with enhancements required and is therefore reporting an 'amber' rated opinion (see Appendix 1), with our assessment towards the middle of this category.

4.1.2 This opinion reflects some moderate areas of weakness in the LPF control environment and governance and risk management frameworks identified from the audits performed, and the risks associated with open IA findings that may put the achievement of organisational objectives at risk.

4.1.3 This opinion is subject to the inherent limitations of IA (covering both the control environment and the assurance provided over controls) as set out in Appendix 2.

4.1.4 IA is not the only source of assurance provided to LPF as there are a number of additional assurance sources (for example, external audit who provide assurance on the LPF financial statements and key financial controls) that the Committee should consider when forming their own view on the design and effectiveness of the LPF control environment and governance and risk management frameworks.

4.2 Audit outcomes

4.2.1 Three IA reviews were completed during the year, with one assessed as 'Effective' (green); one assessed as 'Some Improvement Required' (amber); and one assessed as 'Significant Improvement Required' (red).

Charles River Project – pre-implementation testing – Effective (green)

4.2.2 Implementation of the Charles River Investment Management Solution was a significant technology project for LPF, and our review confirmed that the control environment and governance and risk management frameworks established by LPF to support completion of system and user acceptance testing prior to system

implementation were adequately designed and operating effectively, enabling LPF to proceed with a 'soft launch' on 14 October 2019.

4.2.3 One medium (amber) rated IA finding was raised in relation to post implementation operational processes and controls that would normally be designed and implemented prior to live system implementation. The most significant of these reflected the need for LPF to review the service organisation control (SOC 2) assurance report provided by the supplier to confirm that it did not include any adverse system control gaps that could impact ongoing use of the system, and the need to confirm the appropriateness of both LPF and system supplier remote user access profiles.

Pension Entitlement Calculations – Some Improvement Required (amber)

4.2.4 Whilst minor control weaknesses were identified in the design and effectiveness of the control environment established to support the completeness and accuracy of pension entitlement calculations performed by LPF using the Aquila Heywood Altair system, the established controls provide reasonable assurance that risks are being managed, and that LPF's objective to accurately perform pension entitlement calculations in line with applicable legislative and regulatory requirements should be achieved.

4.2.5 Our review covered the period 1 April to 31 December 2019, and during this time, the high rated finding raised in the Pension Tax audit (completed in April 2018) that highlighted the need for LPF to obtain independent assurance from Aquila Heywood in relation to the ongoing accuracy of Altair system code supporting pension tax calculations remained open. As the risks associated with this finding were also relevant to the system code supporting pension entitlement calculations, these were considered in determining the overall 'some improvement required' report rating.

4.2.6 Two low rated findings were raised reflecting the need for LPF to perform ongoing holistic user profile reviews across the full population of Altair system modules to confirm that no toxic user profile combinations exist that could result in potential exposure to the risk of fraud; and the need to update procedure manuals to support consistent application of workarounds performed in response to legislative and regulatory changes that have not yet been incorporated in the Altair system.

Settlement and Custodian Services – Significant Improvement Required (red)

4.2.7 As some significant and moderate control weaknesses were identified in the design and effectiveness of Lothian Pension Fund's (LPF) supplier management controls supporting delivery of settlement and custodian services by Northern Trust (NT), only limited assurance can be provided that the risks associated with these outsourced services (including custodial credit risk) are being managed, and that Lothian Pension Fund's objectives in relation to compliant and effective settlement and custodian services supporting ongoing management of their funds should be achieved.

4.2.8 One high; two medium and one low rated findings were raised highlighting the need to ensure that

- the current custodian contract is refreshed or re-procured;
- relevant regulatory requirements and risks specifically associated with outsourced services are recorded and effectively managed through established supplier management arrangements;
- appropriate contractual agreements are established to support custodian remote accesses arrangements to systems owned and hosted by another LPF supplier;
- there is effective ongoing oversight of LPF's access to the custodian system; and
- custodian system security controls are aligned with the UK Government's National Cyber Security Centre cloud security principles.

4.3 Status of Internal Audit Findings as at 31 March 2020

4.3.1 LPF had a total of 2 overdue IA findings (1 high and 1 medium) as at 31 March 2020 that relate to reviews completed as part of the 2017/18 and 2019/20 annual plans.

4.3.2 LPF management has prioritised their focus on overdue findings with significant progress evident, as 5 of the 6 overdue findings as at 31 March 2019 were closed by 31 March 2020, with the remaining high rated finding closed in May 2020.

4.3.3 Evidence had been provided by LPF on 31 March 2020 to support closure of the 2017/18 high rated Pension Tax finding. The finding was then closed in May 2020 following management's acceptance of the residual risk associated with limited ongoing supplier assurance on the adequacy and effectiveness of key controls supporting the cloud based pensions administration system used by LPF. Further detail is included at Appendix 4.

4.4 Comparison to prior year

4.4.1 An amber rated opinion was reported in 2018/19 with IA's assessment towards the middle of this category, and this assessment remains unchanged for the 2019/20 financial year.

4.4.2 A direct comparison between annual Internal Audit opinions is not always possible as the scope of the audits included in the annual plans and the risks associated with open and overdue IA findings will vary in line with the changing LPF risk profile.

4.4.3 The 2018/19 IA amber rated opinion was directly attributable to the volume, significance, and age of open and overdue IA findings as at 31 March 2019, as the outcomes of the three audit reviews completed in the 2018/19 financial year were assessed as adequate with only 3 findings raised (1 medium; 1 low; and 1 advisory).

4.4.4 In contrast, whilst significant progress is evident with closure of overdue findings, the outcomes of the three LPF audits completed in the 2019/20 financial year were assessed as red (significant improvement required); amber (some improvement

required); and green (effective) with a total of 7 (1 high; 3 medium; and 3 low) IA findings raised. Consequently, the main driver of the 2019/20 amber rated opinion has been the outcomes of these reviews.

4.5 Internal Audit Independence and Conformance with Public Sector Internal Audit Standards

4.5.1 PSIAS require that IA must be independent and that internal auditors must be objective in performing their work. To ensure conformance with these requirements, IA has established processes to ensure that both team and personal independence is consistently maintained and that any potential conflicts of interest are effectively managed.

4.5.2 We do not consider that we have faced any significant threats to our independence during 2019/20, nor do we consider that we have faced any inappropriate scope or resource limitations when completing our work.

4.5.3 IA has fully conformed with PSIAS requirements during the period 1 April 2019 to 31 March 2020.

5. Financial impact

5.1 There are no direct financial impacts arising from this report, although failure to close IA findings raised and address the associated risks in a timely manner may have some inherent financial impact where associated financial risks have been identified.

6. Stakeholder/Regulatory Impact

6.1 IA findings are raised as a result of control gaps or deficiencies identified during audits. If agreed management actions are not implemented to support closure of Internal Audit findings, LPF will be exposed to the risks set out in the relevant IA reports.

7. Background reading/external references

7.1 Public Sector Internal Audit Standards

8. Appendices

Appendix 1	Internal Audit Annual Opinion Definitions
Appendix 2	Limitations and responsibilities of internal audit and management responsibilities
Appendix 3	LPF reviews completed between 1 April 2019 and 31 March 2020
Appendix 4	Status of LPF Internal Audit Findings as at 31 March 2020
Appendix 5	Final report – Pension Entitlement Calculations
Appendix 6	Final report – Settlement and Custodian Services

Appendix 1 – Internal Audit Annual Opinion Definitions

The PSIAS require the provision of an annual Internal Audit opinion, but do not provide any methodology or guidance detailing how the opinion should be defined. We have adopted the approach set out below to form an opinion for Lothian Pension Fund.

We consider that there are 4 possible opinion types that could apply to LPF. These are detailed below:

1 Adequate *An adequate and appropriate control environment and governance and risk management framework is in place enabling the risks to achieving organisation objectives to be managed*	**2 Generally adequate but with enhancements required** *Areas of weakness and non-compliance in the control environment and governance and risk management framework that that may put the achievement of organisational objectives at risk*
3 Significant enhancements required *Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk*	**4 Inadequate** *The framework of control and governance and risk management framework is inadequate with a substantial risk of system failure resulting in the likely failure to achieve organisational objectives.*

Professional judgement is exercised in determining the appropriate opinion, and it should be noted that in giving an opinion, assurance provided can never be absolute.

Appendix 2 - Limitations and responsibilities of internal audit and management responsibilities

Limitations and responsibilities of internal audit

The opinion is based solely on the internal audit work performed for the financial year 1 April 2019 to 31 March 2020. Work completed was based on the terms of reference agreed with management for each review. However, where other matters have come to our attention, that are considered relevant, they have been considered when finalising our reports and the annual opinion.

There may be additional weaknesses in the LPF control environment and governance and risk management frameworks that were not identified as they were not included in the 2019/20 LPF annual internal audit plan; were excluded from the scope of individual reviews; or were not brought to Internal Audit's attention. Consequently, management and the Committee should be aware that the opinion may have differed if these areas had been included, or brought to Internal Audit's attention.

Control environments, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the impact of unplanned events.

Future periods

The assessment of controls relating to LPF is for the year ended 31 March 2020. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other areas; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of Management and Internal Audit

It is Management's responsibility to develop; implement; and maintain effective control environments and governance and risk management frameworks that are designed to prevent and detect irregularities and fraud. Internal audit work should not be regarded as a substitute for Management's responsibilities for the design and operation of these controls.

Internal Audit endeavours to plan its work so that it has a reasonable expectation of detecting significant control weaknesses and, if detected, performs additional work directed towards identification of potential fraud or other irregularities. However, internal audit procedures alone, even when performed with due professional care, do not guarantee that fraud will be detected. Consequently, internal audit reviews should not be relied upon to detect and disclose all fraud, defalcations or other irregularities that may exist.

Appendix 3 - LPF reviews completed in 2019/20 and 2018/19

2019/20 Annual Plan	Findings				Report Rating
Review	**High**	**Medium**	**Low**	**Advisory**	
Charles River Project – pre-implementation system testing	-	1	-	-	**Effective**
Pension entitlement calculations	-	-	2	-	**Some Improvement Required**
Settlement and custodian services	1	2	1	-	**Significant Improvement Required**
Total Findings Raised	**1**	**3**	**3**	**-**	
Total 18/19 (3 reports)	-	*1*	*1*	*1*	

2018/19 Annual Plan	Findings				Report Rating
Review	**High**	**Medium**	**Low**	**Advisory**	
Unlisted investment valuations and application of fund administration fees and charges	No findings raised				**Adequate**
Stock Lending	No findings raised				**Adequate**
Unitisation	-	1	1	1	**Adequate**
Total Findings Raised	**-**	**1**	**1**	**1**	

Appendix 4 – LPF Overdue Internal Audit Findings as at 31 March 2020

Review	High	Medium	Low	Status - 31st March 2020	Days / Months Overdue at 31/03/20	Status – 15th May 2020
Pension Tax	1	-	-	Overdue - original due date was 23/04/18 Finding was proposed for closure by LPF on 31st March 2020, however the final outcomes did not fully address the risks raised in the original finding. A risk acceptance document was subsequently prepared and signed by the LPF CEO; Head of Finance and Executive Director of Resources. This was received by IA on 8 May 2020 and the finding was then closed.	18 months / 535 working days	Closed 08/05/20
Charles River Project	-	1	-	Overdue - original due date was 14/02/2020 Finding was proposed for closure on 6 March 2020, but was not closed by IA as not all agreed management actions had been completed.	1 month / 33 working days	Overdue
Total	**1**	**1**	**-**	**2 findings were overdue at 31 March 2020** **Evidence had been provided to IA for both findings, however further action was required to support closure.**		
Total 18/19	*3*	*1*	*2*	*All findings were overdue at 31 March 2019* *Evidence had been provided to IA for 2 High and 1 Low rated findings.*		

Appendix 5

The City of Edinburgh Council

Internal Audit

Lothian Pension Fund: Pension Entitlement Calculations

Final Report

6 March 2020

RES1912

Overall report rating:

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 that Lothian Pension Fund's objectives should be achieved.

Contents

This internal audit review is conducted for the Lothian Pension Fund under the auspices of the 2019/20 internal audit plan approved by the Pensions Audit Sub Committee in March 2019. The review is designed to help 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 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 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 Pensions Committee members as appropriate

1. Background and Scope

Background

This review was undertaken as part of the 2019/20 internal audit plan approved by the Lothian Pension Fund (LPF) Pensions Committee in March 2019.

Applicable legislation and regulations

The *Finance Act 2004* (part 4) requires pension schemes (including public service pension schemes) to appoint an administrator to administer ongoing pension scheme activities.

Pension scheme administrators have a number of responsibilities, including calculation of pension entitlements in accordance with current pension legislation, and providing details to scheme members.

Calculation of pension entitlements is covered by the following legislation and guidance:

- *The Local Government Pension Scheme (Scotland) Regulations 2018*
- *The Local Government Pension Scheme (Transitional Provision and Savings) (Scotland) Regulations 2014*

Lothian Pension Fund (LPF) Pension Administration Model

Pension schemes can either perform their own administration activities with established in house teams, or alternatively outsource these responsibilities to an external third-party administrator, whilst remaining accountable for the risks associated with ongoing administration activities. Where pension fund administration activities are outsourced, organisations must implement appropriate supplier performance oversight arrangements to provide assurance on the adequacy and effectiveness of the supplier's key pension fund administration controls.

LPF's administrative activities are performed by an established in house team (circa 18 employees), using the web based Altair pensions administration system provided by Aquila Heywood (AH) to support calculation of member pension entitlements. Consequently, it is important to ensure ongoing compliance with the Council's protocol for externally hosted "Cloud" ICT Services.

It is also important to note that the accuracy of pension entitlement calculations is dependent on member information, e.g. pensionable pay, provided to LPF by its employers.

Pension Entitlement Calculations

The main types of pension entitlement calculations performed by LPF are:

- **Retirals** – calculation of the pension benefit accrued by a member at their planned retirement date.
- **Deaths** – calculation of pension benefits at the time of a member's death including the value of ongoing pension payments to beneficiaries (where relevant).
- **Transfers (in and out)** – calculation of the value of funds at a point in time when a member requests the transfer of funds into or from another scheme.
- **Refunds** – calculation of the value of cash refunds for members with less than two years membership.
- **Aggregations** – calculation of a consolidated fund value where members are entitled to aggregate their funds where concurrent roles result in more than one pension scheme entitlement.

- **Miscellaneous -** a number of miscellaneous calculations are also performed to provide information to members on the impacts associated with additional pension contributions, and member option choices.

Manual Pension Entitlement Calculations

Whilst Aquila Heywood is contractually required to update system codes to reflect regulatory changes (for example, changes in applicable pension legislation or changes to tax rates), instances occur where this is not achieved in sufficient time and workarounds are required to support calculation of entitlement calculations in the Altair system.

Where system workarounds are implemented, it is essential that LPF procedure manuals and documents are updated to ensure that the total population of workarounds (detailed in a document referred to as the 'Known Error List' – KEL produced by Aquila Heywood) are consistently applied.

The known error list as at 25 February included a total of 97 non calculation errors relating to (for example) disclosures and statements included in member correspondence; and 411 known calculation errors where workarounds are currently required.

LPF management has advised that KELs that remain unresolved for a period by the supplier typically relate to calculations that are not performed frequently; apply to a restricted membership cohort; or have no material impact on the calculation, with significant KELS prioritised for rectification in the next software release.

Scope

The objective of this review was to assess the design adequacy and operating effectiveness of the key controls established to ensure the completeness and accuracy of both system and manual pension entitlement calculations performed by LPF.

The review will also provide assurance in relation to the following LPF risks:

- Risk of incorrect pension payments
- Regulatory breaches
- Incorrect communication with members
- Limited or incorrect data from employers leading to incorrect valuation of liabilities /benefit payments / fines from Pensions Regulator

Testing was performed across the period1 April to 31 December 2019.

Our areas of audit focus as detailed in our terms of reference are included at Appendix 2.

Limitations of Scope

The following areas were specifically excluded from the scope of this review at the request of LPF:

- Adequacy of AH key performance measures in relation to ongoing maintenance and accuracy of pensions entitlement calculations performed in the Altair system, and LPF performance monitoring.
- Timeliness of completion and provision of pension entitlement calculations in line with applicable regulatory requirements.

Reperformance testing to confirm the accuracy of pension entitlement calculations was limited to a sample of 105 calculations (45 retiral; 30 death; and 30 transfers) including 20 manual calculations performed by LPF as supplementary validation of the calculations.

It was not possible to validate a larger sample of calculations using data analytics as Aquila Heywood could not provide a system extract of the full population of pensions calculations for the period reviewed.

Reporting Date

Our audit work concluded on 25 February 2020, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 2

Summary of findings raised	
Low	1. Review of Altair system user access profiles
Low	2. Ongoing maintenance of procedure manuals

Opinion

Some Improvement Required

A high rated finding reflecting the need for LPF to obtain independent assurance from Aquila Heywood in relation to the ongoing accuracy of Altair system code supporting pensions tax calculations was raised in the Pensions Tax audit completed in April 2018. The risks associated with this finding are also relevant to the Altair system code supporting pensions entitlement calculations, and these current risks have been considered in determining the overall 'some improvement required' report rating.

Whilst some new minor control weaknesses were identified in the design and effectiveness of the control environment established to support the completeness and accuracy of pension entitlement calculations performed by Lothian Pension Fund (LPF), they provide reasonable assurance that risks are being managed, and that LPF's objective to accurately perform pension entitlement calculations in line with applicable legislative and regulatory requirements should be achieved.

Consequently, 2 low rated Internal Audit findings have been raised.

The first low rated finding highlights a minor control weakness in relation to Altair system user access profiles, as LPF does not currently perform ongoing holistic user profile reviews across the full population of Altair system modules and users to confirm that there are no inappropriate or 'toxic' user profile combinations that could result in exposure to the potential risk of fraud. Whilst some compensating controls have been established, these are not adequately designed to identify any potentially fraudulent transactions resulting from inappropriate access to the Altair system.

Whilst appropriately designed processes have been established to ensure that procedure manuals are updated to demonstrate the workarounds to be performed where legislative and / or regulatory changes have not yet been incorporated into the Altair system code, these processes are not consistently applied and evidenced. Recalculation of a sample of 105 pension entitlement calculations (including some where system workarounds were required) did not identify any material errors, confirming that LPF team members are aware of the workarounds that should be applied to ensure that calculations remain aligned with currently applicable regulatory and / or legislative requirements. Consequently, a low rating has been applied to this finding.

Further information on the findings raised is included at Section 3.

Progress towards closure of the high rated finding on Altair code supporting system calculations

In response to the previously raised high rated finding highlighting the need for independent assurance from Aquila Heywood in relation to the ongoing accuracy of Altair system calculations, LPF management agreed that appropriate ongoing assurance would be requested from Aquila Heywood.

Whilst this high rated finding has not yet been closed, management has advised that progress is being made despite significant challenge from Aquila Heywood, and that the ongoing assurance requested from them will cover all calculations performed by the Altair system (including pension entitlement calculations). LPF management is currently towards a completion date of 13 March 2020 to either reach agreement on this matter with Aquila Heywood, or (alternatively) accept the risks associate with lack of provision of independent assurance on the ongoing accuracy of Altair system calculations.

3. Detailed findings

1. Review of Altair system user access profiles	Low

Whilst LPF reviews a monthly change log that highlights any changes to individual Altair user profiles, there is currently no evidence of a holistic review of user profiles across the full population of Altair system modules and users to confirm that no inappropriate or 'toxic' system user profile combinations exist.

Management has confirmed that existing Altair user access is assessed prior to authorising changes to user profiles to ensure that the change requested will not result in any potentially inappropriate access across Altair system modules, however this assessment is not documented.

It is acknowledged that LPF employees would not be able to create new member details on the system as this information is provided by employers, and management has advised that appropriate 'know your customer' validation checks are performed to confirm the identity of all new members.

Management has also advised that compensating controls operate that are designed to prevent LPF employees from making unauthorised adjustments (including calculating pensions entitlements) to connected member accounts, with the most relevant the requirement for all employees to provide details of any connected persons (for example, close relatives) who are also LPF scheme members.

Where connected persons exist, their member accounts are locked on the Altair system and cannot be accessed by the relevant connected LPF employee. It should be noted that the effectiveness of this control is limited as it is dependent on full disclosure by LPF employees, and that locked accounts were not tested during the audit as its existence was confirmed by management when finalising the draft report.

Whilst the connected persons control (if operating effectively) would prevent connected LPF employees from calculating pensions entitlements for connected members, there are currently no established controls to detect instances of inappropriate amendments to member records where these connections have not been disclosed, or where potentially toxic user profile across Altair system modules has not been identified.

Management has also confirmed that all payments are subject to independent review and validation prior to their release.

Risks

The potential risks associated with our findings are:

- Toxic user profile combinations across Altair system modules are not identified and resolved;
- The existing change log control would not identify toxic user profiles resulting from changes to user profiles made over a number of months; and
- LPF employees have access to connected LPF members.

1.1 Recommendation: Review of Altair system user access profiles

1. LPF management should assess and clearly define any potential toxicity scenarios in relation to Altair system access.
2. LPF management should also engage with Aquila Heywood (the Altair system provider) to ascertain whether a system report can be generated that includes details of the full population of user profiles across all Altair system modules.

If this report can be provided, then:

- ongoing reviews of holistic user profiles across Altair should be implemented (at least quarterly) to assess whether any potentially inappropriate or toxic user access profiles exist.
- where user profiles indicate inappropriate segregation of duties or toxic combinations, appropriate action should be taken to ensure that these are addressed.
- the outcomes of this review should be documented, including details of any changes made to user profiles.

If a system report cannot be generated, then:

- a manual check of a sample of individual users should be performed each month that reviews access to Altair modules for each individual user to confirm whether these appropriate.
- the monthly check should cover the full population of Altair users within one year.
- where user profiles indicate inappropriate segregation of duties or toxic combinations, appropriate action should be taken to ensure that these are addressed.
- the outcomes of these reviews should be documented, including details of any changes made to user profiles.

Agreed Management Action: Review of Altair system user access profiles

1. Altair role profiles will be reviewed and aligned as far as possible on to ensure standardisation on a 'least access' privilege basis;
2. Toxicity scenarios will be assessed and mitigating controls documented.
3. A risk based Altair entitlement review process will be implemented with all employees covered at least once per year.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Doug Heron, Chief Executive, Lothian Pension Fund (LPF); John Burns, Chief Finance Officer, LPF; Struan Fairbairn, Chief Risk Officer, LPF.	**Implementation Date:** 30 September 2020

1.2 Recommendation: Connected user access rights

1. A review should be performed to confirm that connected LPF employees cannot access connected member accounts included in the LPF connected persons log.
2. Where connected LPF employee user profiles have been subject to change, a check should be performed following implementation of the change to confirm that the employee cannot access connected member accounts.

Agreed Management Action: Connected user access rights	
The Internal Audit recommendation will be implemented as detailed above.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Doug Heron, Chief Executive, Lothian Pension Fund (LPF); John Burns, Chief Finance Officer, LPF; Struan Fairbairn, Chief Risk Officer, LPF.	**Implementation Date:** 30 September 2020

2. Ongoing maintenance of procedure manuals	Low

Whilst an appropriately designed process has been established to support ongoing maintenance of procedure manuals and inclusion of workarounds to be applied to address known system errors, it is not consistently applied. Specifically:

- there is no clearly documented list detailing ownership of individual procedure manuals and supporting documentation.
- version control logs for procedure manuals are not consistently updated to reflect changes made.
- evidence of independent review of changes to confirm their accuracy is not consistently recorded. We noted that evidence was available to support independent review of 8 changes completed across circa 122 procedure manuals and supporting documents.

This finding has been assessed as low reflecting that reperformance of a total of 45 retiral; 30 death; and 30 transfer pension entitlement calculations that included a sample of 20 manual calculations did not identify any material differences, providing assurance that workarounds applied as a result of known system errors were consistently and effectively applied across the limited sample tested.

Risk
The potential risks associated with our findings are that inaccurate pensions entitlement calculations could be performed if workarounds are not applied to address 'known errors' as procedure manuals and documentation have not been updated in alignment with the known errors list.
3.1 Recommendation: Ongoing maintenance of procedure manuals
Management should ensure that the requirement to follow the established process for ongoing maintenance of procedure manuals is reinforced across LPF teams involved in calculating pensions entitlements and should implement sample based spot checks to confirm that procedures detailed on the known errors log have been updated and reviewed and supporting version control documentation updated.
3.1 Agreed Management Action: Ongoing maintenance of procedure manuals
The Internal Audit recommendation will be implemented as detailed above.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Doug Heron, Chief Executive, Lothian Pension Fund (LPF); John Burns, Chief Finance Officer, LPF; Struan Fairbairn, Chief Risk Officer, LPF.	**Implementation Date:** 30 September 2020

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the 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 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 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 of the organisation.
Low	A finding that could have a: • ***Minor*** impact on 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.

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives included in the review are:

Audit Area	Control Objectives
Supplier management	1. Roles and responsibilities for Aquila Heywood (AH) and LPF in relation to pension entitlement calculations and quality assurance are clearly specified in the AH contract. 2. LPF has appropriate ongoing assurance from AH to confirm that: • pension entitlement calculations included in Altair are aligned with applicable legislative and regulatory requirements; • controls applied to support calculation amendments are effective; • all calculation amendments are tested prior to release into the live environment; and • security controls (including user access) to the areas of the system that include pension entitlement calculations are effective. 3. Where assurance reports received highlight any issues or emerging risks, these are addressed with AH in a timely manner. 4. LPF receives advice from AH providing details of calculations that have not been updated in line with recent legislative or regulatory changes, including a "Known Errors List (KEL)".
Internal processing	1. LPF has established processes to identify any legislative or regulatory changes that impact pension entitlement calculations, and confirm with AH whether and when these changes will be updated in the Altair system. 2. Details of calculations that have not been updated in the Altair system and need to be performed manually are communicated to all relevant LPF employees. 3. The LPF pension administration team receives appropriate induction and ongoing training in relation to pension entitlement calculations. 4. The process for any manual calculation of pension entitlements that may be required is documented and updated in a timely manner to reflect any applicable regulatory or legislative changes. 5. Appropriate control procedures have been established to confirm the accuracy of data input to the Altair system for system-based entitlement calculations, and the accuracy of any manual entitlement calculations. 6. The risks associated with pension entitlement calculations have been identified, assessed, and recorded and appropriate controls established to ensure that they are effectively managed.

IT security	1. LPF Access rights to the Altair system are restricted to appropriate users based on their roles in relation to pension entitlement calculations. 2. Regular user access reviews are performed by LPF to confirm that segregation of duties remains appropriate and toxic user access combinations do not exist.
Validity of calculations	The sample of pension entitlement calculations selected for testing have been completed and accurately performed and communicated to members.

Appendix 6

The City of Edinburgh Council

Internal Audit

Lothian Pension Fund Settlement and Custodian services

Final Report

11th June 2020

RES1913

Overall report rating:

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 Lothian Pension Fund's objectives should be achieved.

Contents

This internal audit review is conducted for the Lothian Pension Fund under the auspices of the 2019/20 internal audit plan approved by the Pensions Audit Sub Committee in March 2019. The review is designed to help 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 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 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 Pensions Committee members as appropriate

1. Background and Scope

Background

A pension fund custodian is typically an approved bank; depositary; member of a recognised clearing exchange; a regulated clearing firm; or a firm whose permitted activities include safeguarding and administration of investment assets and client monies by pension funds on behalf of their members. The custodian maintains the investment assets (for example electronic share certificates) and client monies in named segregated client accounts with appropriate record keeping services to minimise the potential risk of loss, most notably in the event of the custodian's insolvency, or through fraud, poor administration, or negligence. Custodian record keeping responsibilities involve maintaining client accounts and recording subsequent asset purchases, sales and client money transfers. Custodian responsibilities can also include management of the collection of dividends, interest payments and foreign exchange transactions; corporate actions; proxy voting; and class actions associated with investment assets held on behalf of clients.

A number of custodian firms also offer investment transaction settlement services. All custodian arrangements should be supported by appropriate contractual arrangements that specify the roles and responsibilities (including ongoing regulatory compliance) of both the custodian and the client, with appropriate ongoing supplier management arrangements established to ensure that the custodian continues to meet its contractual and regulatory obligations.

Applicable regulations

Custodian firms are required to comply with the EU Markets in Financial Instruments Directive 2014 legislation that regulates firms who provide services to clients linked to 'financial instruments' (shares, bonds, units in collective investment schemes and derivatives), and the associated Capital Requirements Directive IV (CRD IV) EU legislation that specifies the prudential rules for banks, building societies and investment firms.

Lothian Pension Fund (LPF) custodian arrangements

LPF has appointed Northern Trust (NT) to act as its custodian and provide investment transaction settlement activities, and these arrangements are supported by a contract that was signed in 2011.

Supplier management arrangements have been established and management has advised that these include receipt of an annual Service Organisation Control report 1 (SOC 1) that provides assurance in relation to NT's financial controls, and that a SOC 2 assurance report on operational controls in relation to availability, security, processing integrity, confidentiality and privacy has been requested and received.

There are currently two types of SOC reports available in relation to both controls over financial reporting (SOC 1) and operational (SOC 2) controls. A type 1 report covers only the design of the controls at a specified point in time, whilst a type 2 report confirms whether the controls have operated effectively for a specified period of time.

The contract also provides for an annual oversight visit to NT by LPF. LPF visited NT in November 2019 and reviewed the NT processes for maintaining LPF assets; reconciliations; trade recording; receipts; and settlement.

All LPF investment transactions, with the exception of private markets, are advised to NT through the Charles River Investment Management Solution web based platform implemented in November 2019,

with settlement arrangements and NT custodian activities performed through the web based NT Passport system that can be accessed remotely by LPF.

As LPF uses two web based platforms to support the NT investment transaction settlement process and custodian activities, it is important to ensure ongoing compliance with the Council's protocol for externally hosted "Cloud" ICT Services.

LPF Management has also advised that

- Northern Trust is a US corporation which conducts its business through its US operations and its various US and non-US branches and subsidiaries. As at 31 December 2019, it had assets under custody of $8.50 trillion. It is subject to extensive regulation under state and federal laws in the US and in each of the jurisdictions in which it does business.
- the duration of LPF's contract with NT was extended by 2 years in light of the Scottish Ministers' structural review of the Local Government Pension Schemes in Scotland. NT granted enhanced commercial terms (namely a fee reduction) to LPF for s extension period.
- over the period between 2011 and present, LPF has engaged with NT on an ongoing basis, as part of its supplier management processes and otherwise, to update and refresh this arrangement where necessary and commercially pragmatic, and in some cases include additional services to the master custody agreement.
- key performance indicators have recently been established in relation to NT's management of corporate actions (for example voting at investment company AGMs) on their behalf.

Scope

The objective of this review was to assess the design adequacy and operating effectiveness of the key supplier management controls supporting delivery of settlement transaction and custodian services to LPF by NT during the period 1 April to 31 December 2019, and effective ongoing management of custodial credit risk (the risk of loss associated with any potential NT failure).

Limitations of Scope

The following areas were specifically excluded from the scope of this review:

- stock lending services provided by NT for LPF as these services were covered in the stock lending audit completed in May 2019;
- LPFI business activities;
- Managed broker services provided by NT.

Reporting Date

Our audit work concluded on 25th April 2020, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 4

Summary of findings raised	
High	**1.** Northern Trust Contract
Medium	**2.** Regulatory and Risk Management Oversight
Medium	**3.** System Access and Security
Low	**4.** Northern Trust Supplier Management

Opinion

As some significant and moderate control weaknesses were identified in the design and effectiveness of Lothian Pension Fund's (LPF) supplier management controls supporting delivery of settlement and custodian services by Northern Trust (NT), only limited assurance can be provided that the risks associated with these outsourced services (including custodial credit risk) are being managed, and that Lothian Pension Fund's objectives in relation to compliant and effective settlement and custodian services supporting ongoing management of their funds should be achieved.

Consequently, one High; two Medium; and one Low rated findings have been raised. These highlight the need to ensure:

- that appropriate contractual agreements are established to support current practice where NT remotely accesses systems owned and hosted by another LPF supplier to perform settlement and custodian activities (finding 1)
- that the current NT contract is refreshed or re-procured (finding 1)
- that relevant regulatory requirements and risks specifically associated with the outsourced services are recorded and effectively managed through established supplier management arrangements (finding 2)
- effective ongoing oversight of LPF user access to the NT system (finding 3)
- alignment of NT system security controls with the UK Government's National Cyber Security Centre cloud security principles (finding 3)
- that minor control weaknesses in existing NT supplier management arrangements are addressed (finding 4).

Lothian Pension Fund Management Response

We welcome the review from Internal Audit on our approach to oversight of custody arrangements and thank the team for their work. There are a number of clear and sensible findings in this review and we are committed to providing an appropriately urgent response to these. There are other points, including some aspects of the contract standards with NT, where we would ideally make changes but where market practice does not support such provisions, or the costs of achieving the changes in the relatively short remaining duration outweigh the benefits. We do not consider that these points represent material legal exposures for us and, subject to further analysis, we expect we will accept these points as ideas for us to include in our work with others in local government pensions schemes (LGPS) as we set the framework for a joint-procurement exercise to be known as the new Norfolk Framework for custody. Should the agreed

LGPS contract terms not include these then we will return to Internal Audit to provide notice of this when we enter into the new agreement. For clarity, we do not believe that these points individually or in aggregate represent a material risk to our assets being in safe custody.

However, the most significant finding in the report and the driver of it being returned as “red” relates to a potential contractual gap where NT are able to access the front office trading system, as they must do to provide the managed broker service, without evidence of there being a contractual protection in place for LPF such that in the event they proceeded to create their own instruction then we may rely on broad rather than specific contractual provisions for any claims that arose. This is now under investigation and we will compete this no later than 30 June and ordinarily would have done so before the reporting date but the timing of this falls against other significant and time-sensitive priorities for LPF and it will take time to investigate between LPF, Charles River and Northern Trust in order to determine the existence and extent of any gap. While we investigate we acknowledge the potential gap as highlighted by Internal Audit.

Notwithstanding the comments above, we will be further reflecting on the whole report from Internal Audit to develop our action plan and will ensure that Internal Audit and Audit Committee receive our plan as soon as we are able to produce it. The Fund is operating with substantial limitations to resource and the context of Covid-19 and the timing of this audit falling close to year-end has substantially impacted our ability to develop these plans any sooner. For avoidance of doubt, we will return to Committee in September with a fully developed plan and this will be structured to align to the convention of references in this report.

Areas of good practice

The following areas of good practice were also identified during our review:

- **supplier assurance reports** - a financial controls (Service Organisation Control report (SOC) 1) report dated September 2019 that covered both the design (type 1) and operating effectiveness (type 2) of key NT financial controls was received during the NT site visit in December 2019, and subsequently reviewed by LPF management to confirm that there were no significant control gaps.
- **annual site visit** – the annual NT site visit is comprehensive with extensive advance preparation evident by both LPF and NT. This involves completion of a pre visit questionnaire by NT and review of a custodian benchmarking report provided by NT that (together with the outcomes of weekly supplier management meetings) enables LPF to select relevant areas of focus for the site visit. Action plans are also prepared to address any areas of concern identified during the site visit with progress monitored at ongoing supplier management meetings.
- **settlement oversight –** LPF uses comprehensive checklists to support effective ongoing monitoring of trades settled by NT.

3. Detailed Findings

1. Northern Trust Contract	High

Our review of the current Northern Trust (NT) contract agreed in 2011 supporting settlement and custodian services delivered to Lothian Pension Fund (LPF) confirmed that:

1. **Relationships with other LPF suppliers –** LPF implemented a new cloud based trading system in October 2019 that is owned and hosted by Charles River. NT has direct access to this system to support completion of straight through settlement and custodian activities on behalf of LPF. This new arrangement does not appear to be covered by the existing NT contract, and LPF

management has not yet been able to confirm whether the security; data protection; and legal risks associated with this arrangement have been addressed.

2. **Regulatory requirements -** the contract refers to Financial Services Authority (now Financial Conduct Authority) regulations that do not apply to LPF and makes no reference to any other applicable requirements (for example Local Government Pension Scheme regulations 2018 and relevant European Union Directives). Additionally, the contract does not include any detailed clauses in relation to the requirement to ensure ongoing compliance with regulations, and does not detail the recourse available to LPF in the event of potential regulatory breaches. For example:
   - Section 19 of the contract (Page 14) includes a high level reference to the Financial Conduct Authority Client Asset Sourcebook (CASS) regulations, whilst section 19.2 includes a high level and brief reference to the Custodian having established procedures in accordance with Financial Services Authority (now the Financial Conduct Authority) requirements.
3. **Custodian obligations** - the contract is high level and does not clearly specify NTs specific custodian obligations, with NT's responsibilities implied and not detailed, for example
   - Section 6.2 specifies that the Custodian will process settlements in accordance with accepted industry practices, whilst section 6.3 gives the custodian the right to decline acceptance or custody of certain assets on behalf of LPF.
   - Section 7.1 specifies that the custodian will use all 'reasonable means' to advise on Corporate actions whilst sections 7.2 to 7.8 include limited detail on how corporate actions will be processed by NT.
   - Section 7.9 states that the custodian may provide information (MI) on performance targets and (7.10) that they shall agree to hold periodic performance reviews.
4. **Key performance measures –** New key performance indicators were agreed with Northern Trust in January 2020, however these were in place during the period of our review (1 April to 31 December 2019) and have not yet been incorporated into the NT contract. Management has advised that agreement on key performance indicators and supporting performance information was confirmed in meetings between LPF and NT that included the LPF Chief Executive Officer and the Senior Vice President of NT.
5. **Assurance reports** - system and organisation controls (SOC) annual assurance reports are provided by NT to LPF, however the requirement to provide these or other relevant assurance reports is not specified in the contract.
6. **Continuous improvement** – there is no contractual requirement for NT to support LPF with implementation of continuous improvement initiatives to improve the efficiency and effectiveness of custodian services. [

Risks

The potential risks associated with our findings are:

- LPF is exposed to legal risks in relation to Northern Trust (NT) access to the Charles River investment management system.
- the structure of the Northern Trust (NT) contract focuses on limiting potential NT liabilities and does not provide the same level of legal protection to Lothian Pension Fund (LPF).
- NT could stop providing ongoing performance and assurance information to LPF as these requirements have not yet been contractually agreed.

- penalties for poor performance and / or regulatory breaches cannot be applied. continuous improvement opportunities may not be implemented.

1.1 Recommendations: Northern Trust relationships with other LPF suppliers

1. LPF management should review existing contractual arrangements to confirm whether the technology security; data protection; and legal risks associated with Northern Trust's (NT) access to the Charles River investment management solution are appropriately covered.
2. Where existing contractual arrangement do not cover the risks associated with these system access arrangements, new contractual arrangement should be established and agreed between all relevant parties.

1.1 Agreed Management Actions: Northern Trust relationships with other LPF suppliers

This is now under investigation but the timing of this falls against other priorities for LPF and it will take time to investigate between LPF, Charles River and Northern Trust in order to determine the existence and extent of any gap. We are investigating this as a priority and, for now, acknowledge the potential gap as highlighted by Internal Audit.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Doug Heron, Chief Executive, Lothian Pension Fund (LPF); John Burns, Chief Finance Officer, LPF; Struan Fairbairn, Chief Risk Officer, LPF.	**Implementation Date:** Investigation to be completed by 30 June 2020 **Date for implementation of contractual arrangements (action 2) to be agreed (if required) following completion of investigation.**

1.2 Recommendations: Northern Trust Contract

Management has confirmed that a potential re-procurement / refresh of the Northern Trust (NT) contract is being considered. As part of the contract refresh process, management should ensure that the contract includes:

1. the requirement to ensure ongoing compliance with all relevant regulations that apply to delivery of custodian services, including any future regulatory changes.
2. details of NT's specific custodian obligations.
3. the process and penalties to be applied in the event of any regulatory breaches or failure to achieve agreed performance measures.
4. agreed key performance indicators and details of the management information required to support ongoing assessment of NT performance against these.
5. the requirement to provide LPF with annual assurance reports, and details of their specification.
6. the requirement to support LPF with any continuous improvement activities in relation to ongoing provision of custodian services.

1.2 Agreed Management Actions: Northern Trust Contract

We consider that the contract includes appropriate detail in line with standard industry practice and as would have been market norms in 2011. We will seek updates and enhancements where the benefit of doing so in the residual contract term outweighs the costs involved, and otherwise we will seek to

achieve additional protections and clarifications during the re-tender, as you would expect for any periodic re-tendering of a long-term critical service arrangement	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Doug Heron, Chief Executive, Lothian Pension Fund (LPF); John Burns, Chief Finance Officer, LPF; Struan Fairbairn, Chief Risk Officer, LPF	**Implementation Date:** 30 June 2022

2. Regulatory and risk management oversight — Medium

Review of the established Lothian Pension Fund (LPF) regulatory and risk management oversight processes confirmed that:

1. LPF does not currently maintain a schedule of all relevant regulatory requirements applicable to settlement and custodian activities performed by both LPF and Northern Trust (NT), for example, as detailed in Local Government Scheme (LGPS) regulations and other applicable European Union Directives. Additionally (as noted in finding 1 above) NT regulatory obligations are not clearly specified in the current contract or supporting contract addendums and documentation, and the contract is aligned with Financial Conduct Authority regulations that do not apply to LPF.
2. whilst the LPF risk register includes a generic supplier management risk, specific risks relevant to outsourced custodian services and supporting action plans identified from the annual NT site visit have not been recorded in departmental risk registers.

Risks

The potential risks associated with our findings are:

- Lothian Pension Fund (LPF) is unable to confirm that custodian services are delivered and performed in line with applicable regulatory requirements (for example, Local Government Pension Scheme requirements).
- LPF is unable to confirm that all relevant custodian services risks (including those identified from NT support management meetings and site visits) are recorded in departmental risk registers that then flow through to the LPF organisational risk register.

2.1 Recommendations: Regulatory and risk management oversight

1. Lothian Pension Fund (LPF) should maintain details of all relevant regulatory requirements that are applicable to custodian activities and confirm (via the established supplier management process and review of agreed regulatory key performance measures) that these continue to be applied by Northern Trust (NT).
2. LPF should record the specific risks associated with delivery of custodian services by NT. Any new and emerging risks and actions to address them identified at regular supplier management meetings and site visits should also be recorded, with resolution progress monitored at ongoing supplier management meetings. Any significant custodian risks should also be escalated for inclusion in the LPF risk register.

2.1 Agreed Management Actions: Regulatory and risk management oversight

Management consider that our risk management process adequately takes into account and considers custodian risk within LPF when that is appropriate. It does this through monitoring key suppliers, regulatory breaches and other associated risks which are purposefully focused on LPF's own business.

We can evidence appropriate risks having been identified, actioned and monitored over time, however, LPF does not seek to include all granular operational risks identified by sub-groups or specific supplier management processes but does have sufficient governance in place to ensure that where those risks are sufficiently material, they are escalated through the risk group for consideration and potential inclusion in the register. LPF's LR&C team are also involved in NT supplier management at appropriate junctures.

A further response to this finding will be provided as part of the fully developed plan in response to the audit that will be prepared by 30 September 2020

Owner: N/A – further action to be agreed (where appropriate) following completion of the plan in response to the audit to be prepared by 30 September 2020. **Contributors:** N/A	**Implementation Date:** **N/A**

3. System Access and Security	**Medium**

Review of Lothian Pension Fund's (LPF) user access management controls in relation to 26 users (20 of these are LPF employees) with access to the Northern Trust (NT) Passport system confirmed that:

- user access reports detailing LPF employee user profiles and system access rights for LPF employees are currently provided annually by NT for review by LPF.
- no evidence is retained to confirm that LPF employee user profiles and system access rights are reviewed by an appropriate LPF senior manager, with details of actions taken to address any potential concerns.
- One unnamed user (access profile LHPPFXX) had not logged on to the system since 20 December 2012, whilst user profile LHPPFZ8 has no recorded last log on date.
- User profile LHPPFNT is described as 'Northern' and has not accessed the system since 13 January 2019. Additionally, the e mail address associated with this account is that of an LPF employee.
- Two user profiles were noted that did not relate to named LPF employees (LHPPFZ8 and LHPPFXX).

Alignment with National Cyber Security cloud security principles

The UK Government's National Cyber Security Centre (NCSC) website requires all public sector organisations review their service provider compliance with their 14 cloud security principles (published in November 2018) and perform a gap analysis to determine the extent and potential impact of any residual risks and actions required to address them. This gap analysis has yet been performed by Lothian Pension Fund (LPF) in relation to Northern Trust (NT).

Whilst the service organisation control (SOC) reports currently provided to LPF by NT are not specifically aligned with the NCSC principles, much of the content included in SOC 2 type 1 and 2 reports would provide assurance on the NCSC requirements.

Risks

The potential risks associated with our findings are:

- Lothian Pension Fund (LPF) employees may have potentially inappropriate access to the Northern Trust (NT) passport system, with an associated risk of fraud.
- Inappropriate Passport system access rights are not identified and addressed in a timely manner.
- LPF is unable to demonstrate that NT (and potentially other system suppliers not included within the scope of this review) has appropriate security controls that are aligned with National Cyber Security Centre (NCSC) cloud security principles

3.1 Recommendations: System access controls

1. Northern Trust (NT) should be requested to provide Lothian Pension Fund (LPF) with system access reports at least quarterly, with this requirement specified in the refreshed contract (refer recommendation 1.1).
2. Review of appropriateness of user profiles and system access rights should be performed and recorded by an appropriately independent LPF senior manager.
3. LPF employees with edit and authorise access rights should be reviewed, and appropriate action taken to change access rights where these are not considered appropriate. Where review outcomes confirm that both edit and authorise access rights are required, the rationale supporting this requirement should be recorded and retained.
4. Users who have not accessed the system in the last financial year should be removed.
5. Management should investigate user profiles that do not relate to named LPF employees to understand who can use these profiles and the levels of access they provide to the system. Where these user profiles are not required, they should be removed, or the rationale supporting their ongoing use recorded and retained.

3.1 Agreed Management Actions: System access controls

1. Agree with recommendation, access reports will be requested and reviewed quarterly. Whilst this review has been undertaken annually, it is accepted that formal evidence should be retained.
2. Agreed – this action will be implemented as recommended.
3. Agreed – this action will be implemented as recommended.
4. Agreed – all non LPF user profiles will be reviewed and removed.

Owner: N/A – implementation date to be agreed (where appropriate) following completion of the plan in response to the audit to be prepared by 30 September 2020. **Contributors:** N/A	**Implementation Date:** **N/A**

3.2 Recommendations: National Cyber Security cloud security principles mapping

1. A mapping exercise should be performed by Lothian Pension Fund (LPF) to determine whether Norther Trust (NT) Passport system controls are aligned with the National Cyber Security cloud security principles; identify any potential gaps; and advise NT of any remedial action required to ensure alignment.
2. LPF management should consider whether a similar mapping is required for other cloud based systems provided by third party suppliers to support ongoing delivery of LPF services. Where this is required, the mapping should be performed; gaps identified; and suppliers advised of any remedial action required to ensure alignment.

3.2 Agreed Management Actions: National Cyber Security cloud security principles mapping	
Proceed as recommended with caveat that equivalent international or other jurisdiction standards will be deemed acceptable.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Doug Heron, Chief Executive, Lothian Pension Fund (LPF); John Burns, Chief Finance Officer, LPF; Struan Fairbairn, Chief Risk Officer, LPF	**Implementation Date:** 30 June 2021

4. Northern Trust Supplier Management	Low

Review of Lothian Pension Funds (LPF's) established Northern Trust (NT) supplier management arrangements confirmed that:

1. **Timing and adequacy of NT assurance reports –** during their site visit to LPF in December 2019, LPF received and reviewed:
   - a financial reporting controls (Service Organisation Control report (SOC 1)) report that covered both the design and operating effectiveness of key NT financial controls dated September 2019.
   - an operational controls (SOC 2) assurance report dated November 2018 that provided assurance on only the design of NT operational (non-financial) controls, and not their effectiveness. This report was used to provide assurance to pensions committee in March 2020.
   - whilst no significant findings were identified in the NT SOC reports, there was no evidence of LPF review of these reports other than the reference provided in the March 2020 update to Pensions Committee.
2. **Key performance measures (KPIs) –** quarterly key performance indicator (KPI) reports are provided by NT to LPF, however, there is currently no evidence of review by LPF to confirm the accuracy of the reports.
3. **Weekly supplier meetings -** an action log is produced detailing agreed actions from weekly LPF and NT meetings, however no record of decisions taken at the meetings in relation to performance; service improvements; accuracy of KPI reports; and other relevant service matters is maintained.

Risks

The actual / potential risks associated with our findings are:

- Pensions Committee did not receive assurance on the effectiveness of Northern Trust (NT) non-financial operating controls.
- LPF is unable to provide evidence of their management review of Northern Trust (NT) service organisation control (SOC) reports in the event of subsequent NT regulatory breaches or reviews.
- there is no record of decisions taken at ongoing supplier management meetings.
- retrospective legal advice is required in relation to decisions taken at supplier management meetings.

4.1 Recommendations: Supplier Management

1. requirements in relation to the nature and timeframes for provision of service organisation control (SOC) reports (for example SOC 1 and 2 type 1 and type 2 reports to be provided by a specified

date) should be agreed with Northern Trust (NT) and reflected in the NT contract (as per recommendation 1.1 above).

2. management review of SOC reports and details of any follow-up action taken with NT should be recorded and retained, even when the reports do not include any significant findings.
3. a process should be established to review the accuracy of key performance indicators provided by NT to confirm that they continue to be accurately calculated.
4. details of decisions taken at NT supplier management meetings should be logged.

4.1 Agreed Management Actions: Supplier Management

We consider that the approach taken to our oversight of NT is more robust than is indicated here. Beyond this point, we will conduct an internal review on the effectiveness of the arrangements for documenting service review meetings and due diligence reviews, but we believe substantial and effective reviews have been undertaken and appropriate action points raised.

Owner: N/A – further action to be agreed (where appropriate) following completion of the plan in response to the audit to be prepared by 30 September 2020. **Contributors:** N/A	**Implementation Date:** **N/A**

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the 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 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 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 of the organisation.
Low	A finding that could have a: • ***Minor*** impact on 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.

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

Appendix 2: Areas of audit focus

The areas of audit focus and related control objectives that were included in the review are:

Audit Area	Control Objectives
Northern Trust contractual arrangements	1. Roles and responsibilities for Northern Trust (NT) and LPF in relation to transaction settlements and custodian services are clearly specified in the NT contract. These should include but not be limited to the requirements for NT to: □ settle all completed trades in a timely manner with notification of settlement provided to LPF; □ record all completed trades on the NT system and record details of investment assets and client monies in appropriately named and segregated LPF client accounts; □ provide periodic statements (at a frequency agreed with LPF) detailing the value of all safe custody assets and client monies held by NT on behalf of LPF; □ reconcile client investment assets held in custody with LPF records at a frequency agreed with LPF; □ perform asset reconciliations in comparison to NT safe custody records to confirm the physical existence and completeness of all assets held on behalf of LPF; □ provide appropriate compensation (as agreed with LPF) for any losses associated with any shortfalls in client assets identified from the ongoing assets reconciliation process; □ accurately allocate all investment income and charges (dividend and interest income and tax charges) against the designated LPF client accounts; □ effectively manage all corporate actions associated with LPF investments based on an agreed approach with LPF; and □ accurate calculation and application of NT service fees in line with agreed contractual rates. 2. The contract includes appropriate clauses in relation to ongoing compliance with applicable regulatory requirements and the recourse available to LPF in the event of a NT regulatory breach
Ongoing supplier management	1. A framework of key performance measures (KPIs) has been established that is aligned with contractual roles and responsibilities in relation to NT investment transaction settlements and custodian services. 2. NT KPI performance is regularly monitored by LPF with any instances of underperformance addressed in a timely manner 3. LPF receives SOC 1 assurance reports from NT at least annually which confirm that key financial controls supporting the investment transaction settlement and custodian processes are adequately designed and operating effectively. 4. Where assurance reports received highlight any issues or emerging risks, these are addressed with NT in a timely manner. 5. the scope of the annual LPF NT site visit is determined by LPF and communicated to NT in advance of the visit. This includes appropriate evidence based review and oversight to confirm that the key controls associated with transaction settlement and

	custodian services are appropriately designed and operating effectively, and that concerns identified from previous visits have been addressed. 6. Any concerns identified from the site visit are discussed with NT and appropriate action taken to ensure that these are addressed, with LPF advised when these are completed.
Internal processing	1. LPF maintains appropriate trade settlement and investment assets records that are regularly updated to reflect all transactions and regularly reconciled with NT records. 2. All team members involved in maintaining LPF trade settlement and investment asset records have been appropriately trained in the process and also in use of the NT system. 3. The risks associated with transaction settlement for fixed interest securities and custodian processes have been identified, assessed, and recorded and appropriate controls established to ensure that they are effectively managed.
IT security	1. LPF Access rights to the NT Passport system are restricted to appropriate users based on their roles in relation to the settlement and custody processes. 2. Cloud protocols are in accordance with best practice and Council policy.