Pensions Audit Sub Committee

8.30am, Monday, 26 March 2018

Lothian Pension Fund Internal Audit Update – 1 November 2017 to 31 March 2018

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

Executive Summary

This report provides a summary of Internal Audit assurance activity for Lothian Pension Fund (LPF) for the period 1 November 2017 to 31 March 2018, and details of open and overdue LPF Internal Audit recommendations as at 31 January 2018.

Three reviews were included in the 2017/18 Internal Audit annual plan, and one further review was added to the plan in September 2017 at the request of LPF management.

Three reviews have now been completed, with a total of 10 Internal Audit findings (3 High; 2 Medium; 4 Low; and 1 Advisory) raised. The final review of Pensions Tax is at draft reporting stage, and the outcomes will be reported to the June Committee.

This paper includes a summary of the outcomes of the IT Business Resilience and Disaster Recovery review. The Information Governance review was completed in October 2017, with the outcomes reported to Committee in December 2017.

Given the commercially sensitive nature of the third-party Information Security Due Diligence review that was added to the plan, the final outcomes and Internal Audit report have been included in a separate B Agenda paper.

LPF had five open Internal Audit recommendations as at 31 January 2018. Of these, two had not been closed by the agreed implementation date (1 Medium and 1 Low) and were reported as overdue to the Council's Corporate Leadership Team (CLT) and Governance, Risk, and Best Value Committee (GRBV). One of the overdue recommendations was closed in February 2018.

Report

Lothian Pension Fund Internal Audit Update – 1 November 2017 to 31 March 2018

1. Recommendations

Committee is requested to:

1.1 note Internal Audit activity and outcomes for period 1 November 2017 to 31 March 2018, and the status of LPF open and overdue Internal Audit recommendations as at 31 January 2018, and

1.2 highlight any points that it would like raised at the Pensions Committee on 26 March 2018.

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.

2.1.1 **Review of IT Business Resilience and Disaster Recovery** - Review of the Fund's Business Continuity Plan including IT disaster recovery for systems hosted by the Council and third-party system providers.

2.1.2 **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.

2.1.3 **Pensions Tax** - **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.

2.1.4 **Information Security Due Diligence review for Payroll Outsourcing** – this review was added to the 2017/18 Internal Audit plan in September 2017 at the request of LPF management, and assessed the design of information security controls operated by a potential third-party supplier who was being considered as a payroll outsource provider for LPFs subsidiary companies. Given the commercially sensitive nature of this review, a separate update has been provided and will be considered as B agenda item.

Open and Overdue Internal Audit recommendations

2.2 Open and overdue 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 CLT and quarterly to the GRBV Committee.

2.3 Evidence provided by management to support closure is 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 mitigated.

3. Main report

3.1 Three of the four audits included in the LPF 2017/18 Internal Audit plan have been completed, with a total of 10 findings raised as detailed below:

	Findings			
Review	**High**	**Medium**	**Low**	**Advisory**
Information Governance	-	2	3	1
Review of IT Business Resilience and Disaster Recovery	2	-	-	-
Information Security Due Diligence for Payroll Outsourcing	1	-	1	-
Total Findings Raised	**3**	**2**	**4**	**1**

Review of IT Business Resilience and Disaster Recovery

3.2 The Scope of this review assessed the design adequacy and operating effectiveness of the controls established to mitigate the risk of failure to recover LPF business operations and key systems provided by third parties in the event of a disaster or business resilience incident.

3.3 Our review confirmed that significant improvements were required to ensure that existing LPF disaster recovery and business continuity arrangements provide assurance that critical systems and processes will be recovered in the event of a disaster.

3.4 Consequently, 2 ‘High’ rated findings were raised reflecting the need to improve existing LPF disaster recovery and business continuity arrangements; and that LPF Business Continuity and Disaster Recovery requirements should be specified in third party contracts.

3.5 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 As at 31 January 2018, LPF had 5 open Internal Audit recommendations. Of these, two had not been closed by the agreed implementation date and were reported as overdue to both the CLT and GRBV Committee.

Details of open and overdue recommendations are included in the table below:

Review and Recommendation	Rating	Status	Revised Date	Original Date
IT Business Resilience and Disaster Recovery - RES1706	High	Open	-	30/03/18
IT Business Resilience and Disaster Recovery - RES1706	High	Open	-	30/06/18
LPF Cyber Security – RES1614 (refer 4.2 below)	Medium	Overdue	31/03/18	30/09/17
LPF Information Governance - RES1705	Medium	Open	-	28/02/17
LPF Information Governance - RES1705 (refer 4.3 below)	Low	Overdue closed March 2018	-	31/12/17

4.2 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.

4.3 The Low rated overdue Information Governance recommendation reflected the need to clarify data controller responsibilities between LPF and the Council and update the LPF website to reflect the agreed position, and the need to update welcome letters to include a reference to the privacy policy and data protection content outlined in the website. This recommendation was closed in March 2018 following review of evidence provided by LPF.

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. Equality 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@edinburgh.gov.uk | Tel: 0131 469 3216

12. Appendices

Appendix 1 – Internal Audit report – Review of IT Business Resilience and Disaster Recovery

Appendix 1

Internal Audit

Lothian Pension Fund - Review of IT Business Resilience and Disaster Recovery

Final Report

22nd December 2017

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

Background

In May 2017, Lothian Pension Fund (LPF) recognised that existing Business Continuity ("BC") and IT Disaster Recovery ("DR") arrangements did not meet their current requirements, and were not aligned to increasing Financial Conduct Authority (FCA) expectations. As a result, they undertook improvement activity that included further development of their existing Business Continuity Plan.

LPF's major IT systems[1] are provided by either the City of Edinburgh Council (CEC) via an outsourced arrangement with CGI, or through direct outsourcing arrangements with external third-party providers. As a result, LPF is fully reliant on these suppliers to invoke effective DR procedures in the event of a major IT failure. Consequently, LPF does not maintain a separate Disaster Recovery plan, but considers both DR and BC within their BC plan. Within this report, we will refer to this combined BC and DR plan as "the Plan".

As LPF is dependent on third parties for DR arrangements, combining BC and DR processes in one document can be justified, providing that the following processes are documented and performed:

- A process for establishing and regularly re-assessing the criticality of LPF systems and determining recovery time (the target time for recovery of systems) and recovery point (the time period representing the maximum amount of data that can be lost) objectives.
- A process for maintaining oversight of supplier DR testing and BC arrangements relevant to the provision of LPF systems;
- A process to regularly assess the alignment of LPF's recovery objectives with the DR capabilities of suppliers; and
- Procedures for execution, testing and maintenance of BC activities that are within the control of LPF.

The importance of strong IT resilience for LPF was highlighted during the fibre optic cable failure in July 2016 which caused network connectivity failure. As a result, LPF relocated to the CEC building in Waverly Court to continue to perform their most important business operations, such as pension administration and customer services. The delays in restoration of connectivity prompted LPF management to reconsider the level of DR support for connectivity and to engage in talks with the CEC IT and CGI to enhance the criticality of this service.

The systems operated by LPF are used by its wholly owned subsidiary company LPFI, which is authorised and regulated by the Financial Conduct Authority (FCA). In July 2016, the FCA published *"Guidance for firms outsourcing to the 'cloud' and other third-party IT services".* LPF have highlighted an intent to align its resilience and recovery provisions with this guidance.

Scope

The scope of this review was to:

- Assess LPF's business continuity plans and confirm that these are consistent with business requirements and aligned to the disaster recovery capability;
- Assess the ability of the business to recover systems assessed as critical in the event of an incident;
- Assess the DR provisions reported by in-scope third parties used by LPF;
- Confirm that testing of disaster recovery plans and business continuity arrangements are performed on a regular basis; and

[1] CEC IT is outsourced to a third-party company (CGI) that provides LPF with network connectivity, telephone and data infrastructure and web interface hosting. Other major third-party system suppliers that support the LPF technology systems include Aquilla Heywood (pension administration system), Northern Trust (trading system) and Civica (employer communication and data transfer system).

- In the event of a major outage, confirm that LPF have sufficient workplace recovery arrangements to allow the business to operate.

The third-party suppliers originally within the scope of this review were:

- Aquila Heywood (Pension Administration System);
- Civica (Employer Communication and Data Transfer System); and
- Northern Trust (Trading systems).

During our work, we noted that the failure of fibre optic cable in June 2016 exposed LPF to a number of operational and regulatory risks. According to the original Terms and Conditions of this engagement, the third-party supplier to which the provision of the fibre optic cable is outsourced – CGI - was not in scope for the detailed review. Once this event was brought to our attention by LPF management, we reviewed the provision of network connectivity provided by CGI. While this supplier provides LPF with a number of different IT services, network connectivity is the only service delivered by CGI which was considered in detail as part of this review.

For the full terms of reference see Appendix 2.

2. Executive summary

Total number of findings

Critical	0
High	2
Medium	0
Low	0
Advisory	0
Total	**2**

Summary of findings

Our review confirmed that significant improvements are required to ensure that the current LPF disaster recovery (DR) and business continuity arrangements provide assurance that critical systems and processes will be recovered in the event of a disaster. Consequently, 2 'High' rated Findings have been raised.

We established that LPF does not currently have a clear view of the criticality of their technology systems or internal recovery requirements. Additionally, there is no provision for LPF DR requirements in two out of three of third party system supplier contracts reviewed as part of this audit (please refer to the scope).

Where DR arrangements are included in contracts, we found that they are not consistently aligned with current industry good practice as there is no established process to monitor and regularly update DR arrangements with third parties or ensure visibility of underlying DR testing.

The fibre optic cable failure in July 2016 which resulted in lack of network connectivity for LPF highlighted the requirement to improve the DR service provided by the Council in partnership with CGI. This lack of network connectivity resulted in LPF staff relocating to the Council's building at Waverly Court to ensure ongoing delivery of business operations. Whilst there was no significantly adverse impact on LPF's ability to operate as a result of this incident, implementation of controls recommended in this report could help to mitigate the impact of future incidents caused by failure on the part of third party suppliers.

LPF has already taken some steps towards improving DR and BC processes, notably engaging system suppliers to investigate potential opportunities to improve systems recovery capability. This has included working with CGI to improve the level of network connectivity DR capability provided. LPF has also implemented a third-party supplier questionnaire, which includes an appropriate range of questions covering third party BC and DR arrangements. This questionnaire has been used in a recent tender process.

Whilst this review does not validate alignment of LPF's BC and DR plan with current FCA guidance, we have highlighted specific areas where further management action is required to improve effective alignment.

Our detailed findings and recommendations are laid out within Section 2: *Detailed Findings.*

3. Detailed findings

1. Adequacy of existing Disaster Recovery and Business Continuity arrangements – High.

Findings

Our review established that existing LPF Disaster Recovery (DR) and Business Continuity (BC) processes are not sufficiently robust to provide assurance that LPF systems and services can be recovered in a prioritised and timely manner. Specifically:

1. **System criticality and recovery objectives** - LPF has not specified their system criticality requirements or prioritised recovery time and point objectives for the systems used to support their operations. Instead, LPF adopts existing suppliers' recovery capability as de facto recovery objectives.

2. Adequacy of BC Plan – Review of LPF's current plan confirmed that:

- **Supplier Recovery Objectives** – Third parties' recovery time and point objectives, currently offered by suppliers for recovery of critical processes, are not documented within the Plan.
- **Review of Third Party DR Tests -** The Plan does not include a process for oversight, monitoring and follow up of DR testing performed by suppliers to assess the potential impact of the outcomes on LPF. Currently, LPF is not engaged in third party DR testing arrangements (with the exception of pension administration system DR performed by Aquilla Heywood).
- **Workplace recovery requirements –** LPF has not formally established their workplace recovery requirements with CEC to ensure that operational processes can be relocated in the event of an incident.
- **Business Impact Assessments** - No process has been established to support completion of ongoing Business Impact Analysis (BIA) for inclusion in the plan.
- **Critical Processes –** Whilst process owners provided their input to the design of the Plan in relation to critical processes, there is no documented evidence confirming that this input has been obtained.
- **Responsibilities -** The Plan lists the names of individuals responsible for DR activity, however, it does not clearly specify their roles and responsibilities before, during and after any incident.
- **BC Training and Awareness -** The Plan does not include a section on provision and completion of BC awareness training for the key staff involved in DR and BC activities.
- **Business Continuity Rehearsal -** The Plan has been successfully invoked in the past during both planned and unexpected outages. However, LPF has not established an ongoing BC rehearsal programme and currently has no defined plan for future rehearsals under number of different scenarios. Additionally, the Plan does not clearly specify whether CEC workplace recovery provisions meet LPF's operational requirements, and that communication arrangements are effective.
- **Annual Review of Plan -** The Plan is scheduled to be reviewed annually, or in the event of a serious disruption to the business, organisational, or other change that could impact its effectiveness. We noted that LPF has no established process to review and update the Plan

The Findings detailed above relate to some sections of the FCA guidance. The guidance provides recommendations which include, but are not limited to, the following actions that the organisation should take:

- Document their strategy for maintaining continuity of its operations, including recovery from an event;
- Establish plans for communicating and regularly testing the adequacy and effectiveness of this strategy (testing has been covered below);
- Put in place arrangements to ensure that the regulator has access to data in the event of disruption;
- Regularly update business continuity and planning arrangements and test arrangements to ensure their effectiveness; and

- Consider the likelihood and impact of an unexpected disruption to the continuity of its operations.

Business Implication	Finding Rating
• LPF cannot assess whether current arrangements with third party suppliers (limited by suppliers' capacity and capability) adequately meet their requirements for recovery of critical systems, resulting in potential unacceptable service recovery delays. • LPF have not performed a business systems criticality assessment, which might lead to inappropriate prioritisation of recovery in the event of the incident. • Lack of regular business impact assessment exercise may adversely affect the process of updating the Plan. As a result, the Plan might be invalid and affect management's ability to restore services in line with current business requirements. • Team members may be unclear on their respective roles and responsibilities in the event of an incident resulting in failure to fully execute the plan. • Failure to implement effective testing and staff training may lead to a decreased quality of a response in the event of an incident • The content of the plan may not include all necessary critical operational processes. • LPF has no assurance that the plan will support effective restoration and relocation of services in the event of a disaster. • Not having controls aligned with good practice and the FCA guidance may expose LPFI to regulatory risk.	**High**

Action plans

Recommendation	Responsible Officer
1. LPF should identify and document the criticality of systems and processes they rely on to enable service provision in the event of an incident. 2. Criticality requirements, and the procedures that suppliers will apply in the event of an incident, including their recovery time and point objectives for LPF's web based systems should also be reflected in the Plan. 3. LPF should introduce a process for oversight, monitoring and follow-up of DR tests performed by third party suppliers, ensuring that any adverse outcomes that cannot be resolved are recorded in the risk register. 4. LPF should establish and formally communicate their workplace recovery requirements with CEC to ensure that critical operational processes can be relocated in the event of an incident. 5. An annual Business Impact Analysis (BIA) should be performed to establish whether recent internal and external changes affect current DR/BC arrangements. Where changes to the Plan are required, these should be implemented in conjunction with third party suppliers. 6. Involvement of process owners (and other stakeholders) in designing and updating the plan should be recorded to provide an effective audit trail and confirmation that all key processes have been included (where appropriate), 7. The Plan should be updated to include clear roles and responsibilities for all staff before, during and after any incident. This should include allocation of LPF owners for each critical system with specific responsibility for ensuring oversight of third party DR arrangements.	Chief Executive, Lothian Pension Fund

8. The Plan should be updated to require completion of BC awareness training for key staff. 9. Business continuity rehearsals should be implemented on an ongoing basis at an appropriate frequency (at least annually). 10. The Plan should be assessed and updated on an annual basis to ensure that it is fit for purpose and aligned with LPF's structure and changing internal and external business environment. The process to assess the Plan should be carefully developed and formalised by LPF management, to ensure that approved and robust appraisal criteria are followed. 11. Third party contracts should be reviewed annually in conjunction with the LPF Plan, and processes should be implemented to review contractual arrangements in light of ad hoc changes (for example changes to regulatory requirements regarding IT resilience). 12. The Plan should be formally reviewed and signed-off by the process owner, Chief Executive Officer, and relevant governance forum / committee upon completion of each annual review.	
Agreed Management Action	**Estimated Implementation Date**
To address recommendations 1, 2, 3, 4, 6, 7 & 12: The Business Continuity plan will be updated to include: • LPF Business critical systems. • Procedures that will be applied by third parties in the event of an incident including supplier recovery time and point objectives for the web hosted systems used by LPF. • Oversight, monitoring and follow-up of supplier DR tests will be performed as part of the annual review of the LPF plan and any adverse outcomes that cannot be resolved will be included in the LPF risk register. • The LPF Management team will maintain oversight of the plan to ensure that key business processes and team roles and responsibilities in the event of a disaster accurately recorded. • The revised plan will be reviewed/approved by the LPF management team, the Head of Finance and the Executive Director of Resources and shared with the CEC Resilience Committee to ensure that CEC are fully aware of LPF requirements.	29th June 2018.
To address recommendation 5: Business Impact Analysis of LPF, including supplier recovery requirements, to be updated and communicated fed into CEC's Business Continuity arrangements, with subsequent updates provided annually.	28th February 2018 (for Q4 2017 sign-off)
To address recommendation 8, 10 and 11: Annual review of the Business Continuity plan, including Business Impact Analysis and awareness sessions/rehearsals, will be incorporated into the LPF compliance checklist to ensure they are undertaken regularly. Third party contracts will be reviewed annually in conjunction with the LPF Plan and any necessary contractual changes communicated and agreed.	30th March 2018
To address recommendation 9: LPF accepts the risk associated with lack of formal BC testing on the basis of ongoing cross working between the	N/A – risk accepted

current LPF location (Atria 1) and the CEC main building at Waverley Court and the City Chambers. Additionally, LPF team members regularly work at home, and the only critical requirement to support this is network connectivity.	

2. LPF Business Continuity and Disaster Recovery requirements are not specified in third party contracts - High

Findings

There is no established process within LPF to review alignment of third party disaster recovery (DR) contractual requirements and capability with LPF's requirements. Consequently, LPF is unable to identify systems where the DR provision falls short of LPF's requirements and where contracts may need to be revised.

A review of third party contracts supporting provision of LPF technology systems established that they do not consistently include DR provision clauses. Where DR provision is included, the requirements are based on supplier recovery capability which may not be aligned with LPF requirements. Our testing confirmed:

- **Lack of agreed DR provision between the Council (CGI) and LPF –** Provision of network connectivity by the Council via CGI is the most critical service provided to LPF, as connectivity failure significantly impacts LPFs ability to operate, exposing the fund to potential regulatory and reputational risks.

  Following an incident in 2016 where there was no connectivity for 2 days, LPF has commenced dialogue with the CGI via the Council's ICT team and has expressed an interest in increasing the DR criticality rating for the fibre optic cable that supports network connectivity. Whilst there is no evidence available to demonstrate that network connectivity has improved, LPF management has advised that CGI has improved the response time in the event of Atria connectivity failing
- **Lack of DR provision for the Trading Platform** - The DR clause within the current contract with Northern Trust does not include provision for recovery time objectives (RTO) or recovery point objectives (RPO) for the trading platform in the event of an incident where DR procedures are invoked.
- **Historic and inadequate DR arrangements for the Pension Administration System -** Contractual arrangements with Aquila Heywood have not been updated since 2009. The current recovery time objective specified in the contract (48 hours) for the pension administration system is not aligned with the Pensions Administration Standards Association guidance of a 24-hour RTO.
- **Lack of DR provision for communications platform** – The Civica contract, which covers provision of the communication platform between LPF and employers, does not include DR provision. In the event of a disaster, Civica would restore the platform, however this would only be on a "best endeavours" basis as no specific recovery time (RTO) or recovery point objectives (RPO) are guaranteed for LPF.
- **Ongoing communication with suppliers -** As noted in Finding 1, LPF has not articulated recovery objectives for systems that support their business processes. As a result, they are unable to fully articulate BC and DR requirements to CEC ICT or other suppliers. While inclusion of recovery objectives within contracts should be the key process for LPF, maintaining an active communication channel with the suppliers would be also beneficial for ensuring satisfactory DR arrangements. Without ongoing communication, prioritisation of LPF's critical services within suppliers' wider DR plans might not be aligned with LPF's needs.

The Findings detailed above relate to some sections of the FCA guidance in relation to oversight of service providers; risk management and relationships between service providers. The guidance provides recommendations which include, but are not limited to, the following actions that the organisation should take:

Oversight of service provider

- be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends;
- allocate responsibility for the day-to-day and strategic management of the service provider;
- verify that suitable arrangements for dispute resolution exist.

Risk management

- ensure the contract(s) provide for the remediation of breaches and other adverse events;
- monitor concentration risk and consider what action it would take if the outsource provider failed;
- should carry out a risk assessment to identify relevant risks and identify steps to mitigate them; and
- document this assessment.

Business Implication	Finding Rating
• Third party suppliers of LPF systems may not have sufficient capability to ensure recovery of critical systems within acceptable timeframes. • Failure to address LPF's DR requirements in the contract may leave crucial issues unspecified and open to implicit agreement. This lack of clarity over the DR responsibilities might lead to unexpected delays restoring critical processes in the event of an incident • Potential regulatory fines and reputational damage if critical systems and operations cannot be restored.	High

Action plans

Recommendation	Responsible Officer
1. LPF system criticality requirements and prioritised recovery objectives (recovery time and point objectives) should be communicated to third party system providers. 2. Contracts should be reviewed and where necessary renegotiated and updated to include DR provision where this is currently missing, or to ensure that DR clauses are updated to reflect LPF requirements. Contract revisions should include: • Agreed testing arrangements and frequencies; • RTOs and RPOs and penalties for failing to meet these; • Back up arrangements, including frequency, data security solutions applied by the supplier (e.g. type of encryption) and security measures in the location where the data will be stored. • Where contracts cannot be updated to reflect LPF requirements, the risk should be recorded in the LPF risk register. 3. LPF should request that the Council ICT Service establishes a dedicated LPF relationship manager to support them in defining and agreeing their BC/DR requirements with the Council and CGI. 4. LPF should also request representation at CEC Resilience Committee meetings to ensure that all relevant LPF recovery and resilience issues are discussed and addressed.	Chief Executive, Lothian Pension Fund
Agreed Management Action	**Estimated Implementation Date**

To address recommendations 1 and 2: The points noted by Internal Audit (including system criticality and recovery objectives) will be discussed with third party providers for services not provided via CGI (pensions administration systems and custodian) and renegotiated/added to contracts where possible and practical. (DR provision is included in the specification of pensions administration system in the tender which is currently underway. However, in other cases LPF's ability to vary established contractual provisions is expected to be limited). Where this cannot be achieved, the risk will be recorded in the LPF risk register.	30th March 2018
To address recommendation 3: Disaster Recovery requirements will be added to the list of ongoing ICT issues currently being discussed with ICT. LPF's full list of requirements will then be shared with the Resources ICT representative (to be established with ICT) to ensure that these are communicated to ICT.	28th February 2018
To address recommendation 4: LPF recovery and resilience requirements will be communicated to the Resources Resilience Business Partner for inclusion on the agenda at the next Resources Resilience Meeting.	28th February 2018

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

Terms of Reference – Lothian Pension Fund – IT Business Resilience and Disaster Recovery

To: John Burns

From: Lesley Newdall
Chief Internal Auditor Date: July 2017

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

Background

The availability and resilience of systems used by the Lothian Pension Fund are important to deliver and maintain service and protect the reputation of the Fund.

Several systems (including the 'Pension Administration System', 'Employer Data Transfer Portal' and 'Global Custody Services') relied on by the Lothian Pension Fund are hosted by third party suppliers. The Fund places reliance on the controls operated by these third parties. For non-third party hosted systems, reliance is placed on the DR and Workplace Recovery arrangements provided by CGI and the City of Edinburgh Council.

This review will consider:

- How LPF'S Business Continuity requirements are captured, maintained, and tested;
- The approach to articulating and maintaining oversight of DR provisions provided by third party suppliers; and
- The scope of controls reported as in place by key third party suppliers identified by Lothian Pension Fund Management.

Scope

The scope of this review will be to:

- Assess LPF's business continuity plans and confirm that these are consistent with business requirements and aligned to the disaster recovery capability;
- Assess the ability for the business to recover identified critical systems in the event of an incident;
- Assess the DR provisions reported by agreed third parties used by the Lothian Pension Fund.
- Confirm that testing of disaster recovery plans and business continuity arrangements are performed on a regular basis; and
- In the event of a major council outage that LPF have sufficient workplace recovery arrangement to allow the business to operate.

The suppliers currently in scope of this review are:

- Aquila Heywood;
- Civica; and
- Northern Trust.

Approach

Our audit approach is as follow:

- Obtain an understanding of the Lothian Pension Funds processes through discussions with key personnel, review of documentation and transaction walkthroughs;
- Identify the key risks in relation to the processes;
- Evaluate the design of the key controls in place to address the key risks considered by assessing adequacy of assertions made by third party Management in response to questionnaires issued as part of this review; and
- Test the effectiveness of the key controls operated by LPF.

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

Sub-process	Control Objectives
Disaster Recovery Plans	• Plans are documented, signed off and reviewed regularly. • Plans are updated after major changes to the organisations systems and personnel. • Recovery Time Objectives and Recovery Point Objectives are agreed and documented between CEC IT and LPF. • Plans include latest system configurations and steps to be followed in the event of an incident (including communication with LPF).
Business continuity	• Critical systems have been agreed between CEC IT and the LPF. • System criticality is reviewed on a regular basis. • LPF Business Continuity requirements have been articulated to CEC.
Third Party Management	• Third Parties Disaster Recovery plans are linked with Lothian Pension Funds Business Continuity Plans. • Contractual provision for DR is included in third party contracts in scope. • Plans are agreed and understood by all parties.
Testing	• Regular testing of the ability to recover systems is performed. • Backups are completed on a regular basis and stored securely. • Workplace recovery provision is in place in the event of a major outage.

Limitations of Scope

The scope of our review is outlined above. The review is limited to the processes in place and to the third-party suppliers that provide critical infrastructure to LPF. The review will not cover services provided to Lothian Pension Fund by the City of Edinburgh Council Group IT function. The review will not undertake site visits to third party suppliers.

Our testing of documentation will be performed on sample basis, using PwC's methodology, agreed with Management at the start of the audit. It is Management's responsibility to develop and maintain sound systems of risk management, internal control, and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for Management's responsibilities for the design and operation of these systems.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	0131 469 3216
John Hinchcliffe	Senior Auditor	07702 699 175
Thomas Bruch	Auditor	07907 644 113

Key Contacts

Name	Role	Contact Details
John Burns	Chief Finance Officer	0131 469 3711
Struan Fairbairn	Chief Risk Officer	0131 529 4689

Timetable

Fieldwork Start	17 July 2017
Fieldwork Completed*	28 July 2017
Draft report to Auditee	04 August 2017
Response from Auditee	11 August 2017
Final Report to Auditee	18 August 2017
Final report available for presentation to the Pensions Audit Sub-Committee	TBC

* The date of completion of fieldwork will depend on the ability of third parties to respond to the DR Provision Questionnaire. In the event of delays we will update target dates in agreement with Management.