ABERDEEN CITY COUNCIL

COMMITTEE	Pensions Committee
DATE	22 June 2018
REPORT TITLE	Internal Audit Report AC1827 – Pensions System
REPORT NUMBER	IA/AC1827
DIRECTOR	N/A
REPORT AUTHOR	David Hughes
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on the Pensions System.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of the Pensions System.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. OUTCOMES

7.1 There are no direct impacts, as a result of this report, in relation to the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place, or Enabling Technology, or on the Design Principles of the Target Operating Model.

7.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. APPENDICES

9.1 Internal Audit report AC1827 – Pensions System.

10. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

BON ACCORD

ABERDEEN

CITY COUNCIL

Internal Audit Report

Pensions System

Issued to:
Steven Whyte, Director of Resources
Fraser Bell, Head of Legal & Governance
Sandra Buthlay, Interim Head of Finance
Laura Collis, Pensions Manager
Gary Gray, Benefit Administration & Technical Manager
Mairi Suttie, Governance Manager
External Audit

Date of Issue: March 2018 **Report No. AC1827**

EXECUTIVE SUMMARY

The North East Scotland Pension Fund (NESPF) is administered by Aberdeen City Council within the Local Government Pension Scheme Regulations.

This fund is valued at over £3.8 billion and provides pension arrangements for 57 employers including Local Authorities, the Scottish Fire and Police Services, Further Education establishments and various charities and other bodies. It has 25,192 active members, 17,352 deferred members (who do not currently pay into the scheme) and pays benefits to 20,240 pensioners and dependents each month.

The objective of this audit was to consider whether appropriate control is being exercised over the system used to administer the Fund, including access, contingency planning and disaster recovery, data input, and that interfaces to and from other systems are accurate and properly controlled. In general there is adequate control over the system, and comprehensive written procedures.

Password protocols may need to be updated to reflect revised best practice, audit logs should be reviewed more regularly, manual secondary checks are in place but control could be enhanced through system development, and the data protection compliance of the test database needs to be reviewed. The Service has committed to reviewing these aspects and implementing relevant actions by September 2018

Whilst the Service considers the system to be reliable, and remote supplier hosting arrangements reduce the risk of local hardware issues compromising access, there remains a risk of incidents occurring which are beyond the supplier's ability to repair within targeted timescales. The Service will create a local contingency plan to address this.

The Service has recently entered into negotiations for a new 10 year contract with the software provider under a tendered framework agreement which will shortly expire. Alternative options including a new joint tender have been considered and not progressed as the Service considers these do not offer best value. The Pensions Committee approved the cost of the new system at £252,946 per annum, and following advice from Internal Audit and Commercial and Procurement Services the Service has sought further approval for additional costs which may be incurred due to contract price inflation.

1. INTRODUCTION

1.1 The North East Scotland Pension Fund (NESPF) is administered by Aberdeen City Council within the Local Government Pension Scheme Regulations.

1.2 This fund is valued at over £3.8 billion and provides pension arrangements for 57 employers including Local Authorities, the Scottish Fire and Police Services, Further Education establishments and various charities and other bodies. It has 25,192 active members, 17,352 deferred members (who do not currently pay into the scheme) and pays benefits to 20,240 pensioners and dependents each month.

1.3 The system which is used to administer the Fund is Altair and the objective of this audit was to consider whether appropriate control is being exercised over the system, including access, contingency planning and disaster recovery, data input, and that interfaces to and from other systems are accurate and properly controlled.

1.4 This involved an examination of current and potential future running costs of the Pensions system, written procedures for administration and management of the system including training, access to the system, users' data input, interfaces and reconciliations of data transfer, and contingency planning.

1.5 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Laura Collis, Pensions Manager, and Gary Gray, Benefit Administration & Technical Manager.

2. FINDINGS AND RECOMMENDATIONS

2.1 System Costs & Licences

2.1.1 The current pensions system Altair is provided by Heywood for which an annual fee is payable. The original cost of the contract, effective from April 2011, comprised an initial set up fee of £120,551 and ongoing annual costs of £167,784 for a period of 5 years, subsequently extended via Committee approval in 2016 for a further 2 years. The annual costs however were subject to an annual potential increase (at the Supplier's discretion) of the Retail Price Index (RPI) plus 5%. The RPI has averaged 3% during this time.

2.1.2 Figures obtained from the Service show the annual cost of the system has increased to £252,946 per annum as of 2017/18, this increase consisting of membership banding increases and an increase in the hosting agreement to allow for 30 users, in addition to annual price increases of an average of 3%. Whilst the cost increase reflects agreed enhancements to the system during this time, including options for additional users and payees the annual increase has still been substantial.

2.1.3 A report to the Pensions Committee on 1 December 2017 recommended entering a new contract with the current supplier at an annual cost of £252,946 for a period of 10 years. These arrangements should be compliant with procurement regulations, having been tendered as a sole provider framework in 2014 for four years by Northumberland County Council.

2.1.4 Commercial and Procurement Services noted that the proposed contract length may be too long, given the framework from which it is to be called off from will expire shortly, and other Scottish LGPS Funds are in the process of completing a joint tender exercise for a software administration provider.

2.1.5 The Service has stated they remain happy with the proposal, for the reasons stated in the Committee report, which include limited alternatives, cost sharing for updates as part of a national group of administering authorities using the same system, and potential data migration costs of transferring to a new system. In addition, the supplier has stated that new and renewed contracts are normally subject to a £500,000 initial set up fee, which will be waived if the Service commits to a contract without further competitive tendering.

2.1.6 Review of the framework terms and conditions shows that although the initial fee (referred to as 'the price') is kept constant for the life of the contract (£0) there remains an option for the supplier to increase the support and maintenance fee by RPI plus 5% annually. Over the contract period this could result in the payment increasing to £505,000 per annum – double its current rate based on an 8% per annum increase. Whilst the Service considers this unlikely as historically only the Retail Price Index increase has been applied, the Contract does allow for these levels of increase. However, the Committee was not advised of this risk.

2.1.7 From 2011 to 2017, the average historic increase has been 3% per annum peaking at 5% in 2012/13 through to the lowest increase in 2016/17 of 1.5%. Yearly increases have mirrored Retail Price Index figures as of July the previous year. Applying the average 3% annual cost increases means an additional £370,282 will be paid to the supplier, resulting in a total spend of £2,899,742 compared to £2,529,460 which the Committee would have assumed on the basis of the December 2017 report – an additional 15%.

2.1.8 The Council's Procurement Regulations, used by the Service, set out that contract costs (which have to be calculated over the entire length of the contract) cannot vary beyond the lesser of 25% or £100,000 without further Committee approval. Such cost increases are therefore not within Officers' delegated powers to accept, and need to be transparent for the Committee to take a decision.

Recommendation
The Service should ensure the Pensions Committee is provided with the full estimated cost of the proposed contract and alternative options.

Service Response / Action
NESPF have provided evidence to demonstrate the substantial cost referred to in 2.1.2 was attributable to system enhancements and increased membership, not because of annual increases applied by the supplier. In the proposed contract duration there will be no requirement to change payroll system and there are currently no major scheme changes planned, however should that change it is likely that that they will not be as significant as moving from Final Salary to Career Average Revalued Earnings on 1 April 2015. The proposal has future proofed exceeding our membership banding by increasing our limit to 80,000, a figure which will not be exceeded during next 10 years.

The joint tender exercise referred to in 2.1.4 is led by Lothian Pension Fund (LPF) with 7 other Scottish funds named on the tender document albeit under no obligation to go with contract award, the duration of the contract is for 168 months (10+2+2 years). LPF requirements differ significantly from NESPF and that is one of the reasons why, following consultation with Commercial and Procurement Services, we decided to use the Northumberland Framework.

The option for the supplier to increase support and maintenance fee by RPI plus 5% referred to in 2.1.6 has never been used. This option exists in our current contract and was reviewed by Legal in March 2011. Evidence has been provided to show that the average annual increase applied by the supplier has been 3%, which was slightly below inflation. It is also worth noting that the annual increases published by the supplier apply to all authorities that participate in the CLASS Group which consists of all 11 Scottish Funds, Northern Ireland and majority in England and Wales.

There is no evidence to suggest anything like the potential cost increases referred to in 2.1.6.

Further approval will be sought from the Pensions Committee as appropriate. A report has been prepared for the meeting of 16 March 2018.

Implementation Date	**Responsible Officer**	**Grading**
Implemented	Mairi Suttie, Governance Manager	Significant within audited area

2.1.9 The number of named Employees who can access the system was increased in 2014/15 from 25 to 30. There are currently 29 named users of the system. Employer Service Users and Members can also log in and the system is configured to allow for a maximum of 50 concurrent users at any one time for both Employer Service Users and Members. The Service confirmed that the average number of logins per day was currently 30 meaning that the current allocation is sufficient. The system automatically prevents more than 50 members logging in at any one time meaning there is no risk of additional cost for 'overuse' of the system.

2.2 Written Procedures & Training

2.2.1 Comprehensive written procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance of correct and consistent practices being followed, especially in the event of an experienced employee being absent or leaving.

2.2.2 The Service has comprehensive written procedures covering the main areas of the service, which are available on the network to all users. These are updated on an ongoing basis. The Technical Manager participates in a national working group on Altair and is therefore in a position to be able to advise on changes and additional functionality which may become available.

2.2.3 Training is desk based with a member of the Technical Team training new employees in the basic functionality of the system and colleagues providing further support and explanations for specific role functions thereafter.

2.3 System Access & Passwords

2.3.1 In order to protect confidential information and prevent any fraudulent activity it is important that system access is suitably protected. Following a request from a Line Manager for access for an employee the Technical Team sends an email to the Supplier through their secure web portal to set up a new user on the system.

2.3.2 Where an employee no longer requires access to the system, the Technical Team remove the user's login access meaning they can no longer use the system. The user remains active on the system until such time as their work is reallocated.

2.3.3 In order to further increase security, all users are required to enter a 6 digit password of their choice which then requires to be changed every 3 months. Guidance from the National Cyber Security Centre suggests that enforcing regular password changes may be counterproductive and that passwords should only be changed where an attempt at fraudulent access is suspected.

Recommendation
The Service should ensure that password protocols reflect best practice.

Service Response / Action
Agreed. NESPF will review password protocols and adopt best practise.

Implementation Date	**Responsible Officer**	**Grading**
April 2018	Neil Middleton, Technical Manager	Important within audited area

2.3.4 It is important that attempts at password entry are limited to lessen the chances of attempted fraudulent access to the system. After 3 incorrect password entry attempts the system locks the user out of the system and passwords thereafter can only be reset by the Technical Team.

2.3.5 While it is recognised that there may be a need for a third party to access the system in order to carry out upgrades or resolve issues for instance, this should be limited and restricted. The Supplier is the only party that has access to the system and this must be requested by the Supplier and authorised by the Service, or the Service will contact the Supplier where an issue arises. When an issue has been resolved the Service is notified by the Supplier through a secure portal.

2.3.6 The Service maintains an audit log of third party access in which any activities carried out by the Supplier are recorded. The Service confirmed that this log is reviewed on an ad-hoc basis. It would provide greater assurance if third party activity were reviewed on a set basis, to identify any unrequested activity.

<u>Recommendation</u>
The Service should review the Audit Log of Third Party access at a set frequency.

<u>Service Response / Action</u>
Agreed. NESPF will review the audit log monthly to check for any unrequested activity and raise any instances identified with the supplier.

Implementation Date	Responsible Officer	Grading
April 2018	Neil Middleton, Technical Manager	Important within audited area

2.3.7 The Service confirmed that where an individual's details are to be viewed, in relation to a system issue, then their details are desensitised first which comprises of randomising key pieces of information such as National Insurance numbers, names and addresses meaning that an individual cannot be identified. By doing this there is assurance that an individual's details cannot be viewed by third parties where there is no business reason for them to have access to such details.

2.3.8 There is a test database in which the supplier and users can review and test processes following changes to the system, and test recoveries. This is updated periodically with 'live' data. Although use of and access to this data is controlled, there are risks to Data Protection compliance in using live data in test systems.

<u>Recommendation</u>
The Service should review the use of live data in its test database to ensure it is compliant with Data Protection requirements.

<u>Service Response / Action</u>
Agreed.

NESPF use live data in the test database to ensure the system delivers accurate benefit calculations in accordance with regulations. It is just not possible to create the volume or the many different membership types that have evolved on the system over many years in a test database. By using live data for testing purposes we significantly reduce the possibility of corrupting the live database which could result in a breach of Data Protection legislation.

We will review the use of live data in the test database and ensure we have appropriate procedures and security in place to comply with Data Protection requirements.

Implementation Date	Responsible Officer	Grading
September 2018	Neil Middleton, Technical Manager	Important within audited area

2.4 Data Input

2.4.1 Restrictions are automatically placed on a user's access rights upon setting them up on the system thereby restricting their access to information and functionality which would be inappropriate to their role. The Service confirmed that additional filters can be placed on any users restricting their access still further if this is deemed appropriate. Examples of these filters include preventing a user from performing calculations or preventing them from accessing individual records. However, this functionality is not regularly used. The Service does not routinely obtain declarations of interest from employees to provide assurance that they are not processing or viewing entries for e.g. relatives and close friends, therefore there is no way to determine which records an individual should or should not access.

2.4.2 It is important that all details which have been viewed, amendments and calculations performed and payment details input by all users are recorded to identify any erroneous entries and also for the purposes of fraud prevention. All inputs to the system and information viewed by users is recorded and these logs are retained by the Service. The Service confirmed that these logs are not routinely examined to identify any anomalies, rather reliance is placed on the fact that users have their access restricted at the point of access. Given the number of transactions which are processed every day, restrictions at the point of set up and the fact that all transactions are recorded and can be examined if inappropriate activity is suspected, this is a reasonable approach.

2.4.3 There are 3 'super users' within the system whose access exceeds that of 'normal users' in that they can amend and delete system data and also reports of their activity. Activity by super users is not routinely reviewed by another super user. However, everything they view and / or amend is recorded in the same way as normal users and although they can delete reports of their activity, these can be run again at any point.

2.4.4 It is important that fields cannot be bypassed, and that data cannot be input in an incorrect format, to avoid omissions or mis-matches of data. Data validation and input masks are included in data entry fields to ensure that data is valid. In addition, warning flags will be displayed on screen before a calculation is finalised where the system identifies potential errors, exceptions, or where additional data is required. This serves to remind the user to perform secondary checks on the information which they have input.

2.4.5 The system is not currently configured to require that calculations which have been performed require a secondary check by another user, although it is Service protocol for junior members of staff to have input and calculations checked by a Senior Officer prior to finalisation and for spot checks to be performed on all users of the system.

2.4.6 There therefore exists the possibility that a false calculation could be performed by an Officer to artificially enhance a person's pension. The Service confirmed that while this is possible, spot checks are performed on random records to ensure that the calculations are correct and monthly payroll totals are subject to checks which flag up errors if entries are outwith certain parameters.

2.4.7 In mitigation, payment details which are input into the system have to be authorised by a second person meaning that a user would not be able to input their own or false details without a second person being complicit in this. 'Super users' are subject to the same restrictions in this respect.

2.4.8 The Service also confirmed that it is considering a system upgrade which would require that a box has to be ticked online by a Senior Officer to indicate that they have checked each calculation before the calculated figures go on to the payroll system, thereby ensuring that all calculations have been secondary checked. This would provide greater assurance over the accuracy and validity of all calculations.

Recommendation
The Service should ensure that secondary calculation checks are a system requirement.

Service Response / Action
Agreed. The upgrade referred to in 2.4.8 is an enhanced administration to payroll interface that ensures adjustments can only be transferred into payroll by a Senior officer. NESPF welcome this recommendation and will contact our Supplier for more

details around implementation and cost before preparing a report for consideration by the Pensions Committee in June 2018.

Implementation Date	**Responsible Officer**	**Grading**
September 2018	Marie McLean, Benefit Administration Manager	Significant within audited area

2.5 Interfaces

2.5.1 Every month, payroll information is received from employers via the i-connect secure portal. This is then uploaded to Altair and reconciliations are performed between the information which has been sent and that which has uploaded to the system. At this point, any errors or information which has failed to upload is identified and investigated. Obvious errors, such as incorrect dates having been entered, are manually adjusted, and other errors are referred back to the Employer to obtain clarification prior to being manually adjusted.

2.5.2 A further reconciliation is then performed between the information received through i-connect and uploaded to the system to the payments which have been received to ensure that all match. The Service retains records of these reconciliations which are performed on a monthly basis.

2.5.3 Reconciliations for 5 Employers were examined over a 2 month period. Records showed that in 3 of 5 instances all reconciliations had been performed and all figures matched. In one instance adjustments had been made following queries to the Employer over anomalies in the upload. In the other case there had been no reconciliations since the start of the financial year due to monthly files being received late from an employer and due to additional complexity in reviewing multiple periods' data there being insufficient time to review this data once it had been received. The Service confirmed that at financial year end reconciliations are performed for all Employers to ensure files received match funds received, however in not performing monthly reconciliations errors may not be identified in a timely fashion and it may become more difficult to determine appropriate measures to correct them.

Recommendation
The Service should reinforce to employers the necessity of prompt submission of monthly files, and ensure all reconciliations are performed timeously.

Service Response / Action
It has taken NESPF more than 5 years to get monthly data in our preferred format and this has been achieved by working together with employers who are well aware of the requirement.

We were one of the first authorities in Britain to achieve this and we must remember that there is no legal requirement for employers to provide monthly data. Experience shared by other Funds is that without monthly data it is likely that statutory requirements will not be met which results in having to report a breach of law to The Pensions Regulator.

Our Pension Administration Strategy was revised and approved by the Pensions Committee in March 2017 following a consultation with all employers. The main amendment was the requirement for all employers to provide monthly data using the I-Connect portal which now provided an alternative way for small employers to do so rather than providing an extract file. As part of the strategy the quantity and quality of monthly data received from employers is published quarterly and has been provided to Committee since June 2014.

Issues around receiving monthly files referred to in 2.5.3 has happened to 2 of our largest employers as a result of procuring the same payroll system that promised a working file extract but failed to deliver. This has been a major frustration for both and caused them additional work however they have overcome this by developing their own file extracts. Both maintained close contact with our Employer Relationship Team who provided assistance whenever possible and accepted temporary solutions to continue to deliver our requirements in the short term.

Implementation Date	Responsible Officer	Grading
Ongoing	Claire Mullen, Employer Relationship Manager	Important within audited area

2.6 System Backups & Contingency Planning

2.6.1 The system is backed up in line with the contract: an incremental backup is performed each day and retained for 4 weeks, full backups are performed weekly and retained for 12 weeks, and full monthly backups are retained for 12 months. In addition the Supplier confirmed that backups are held offsite.

2.6.2 It is important that in the event of the system 'crashing' or suffering catastrophic failure that the system and associated records can be restored from backups. This process is termed 'Disaster Recovery' and an exercise is undertaken annually by the Supplier to test this, with the Service invited to review the functionality of the system within a disaster recovery environment. A full recovery had taken place, and was reviewed by the Service, within the last year, with no issues identified.

2.6.3 In the event of the system being unavailable for any length of time it is important that a local contingency plan is in place. The Service confirmed that no such plan was in place as they are using a hosted Service and the current contract stipulates that in the event of access rights affecting all users the target for resolving this is 24 hours, for a few users the target time is 48 hours and for all other issues there is a target time of 14 days. The Service further confirmed that they had no records of any instance where system access had been restricted for more than 1 hour.

2.6.4 However, should an incident occur which is beyond the Supplier's ability to repair within the target timescales, or if the Supplier should cease trading, continuity of service might be affected, and it may be difficult to respond appropriately without a contingency / business continuity plan.

Recommendation
The Service should ensure that a Local Contingency Plan is established to give guidance in the event of prolonged system downtime.

Service Response / Action
Agreed.

In 2011 NESPF chose to go with our Suppliers hosted service to negate risks involved with hosting locally. Currently more than 40 local authority pension funds data is managed in the centre and this is why we believe it is the best option to safeguard delivery of pension administration.

We will create a Local Contingency Plan that will provide guidance and focus on communicating with members should an incident occur which is beyond the Suppliers ability to repair within targeted timescales.

Should our Supplier, the largest administration software provider in the UK and Ireland, cease trading this would impact not just the LGPS but majority of Public Sector pensions nationally.

Implementation Date	**Responsible Officer**	**Grading**
September 2018	Neil Middleton, Technical Manager	Significant within audited area

AUDITORS: D Hughes
C Harvey
D Henderson

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.