The Highland Council

Pensions Committee – 14th August 2014

Agenda Item	**9**
Report No	**PC/09/14**

Internal Audit Report - Pensions System

Report by the Head of Internal Audit & Risk Management

Summary

This report refers to the audit work undertaken since the last report to the Pensions Committee on 14th November 2013. In addition, details are provided of the audits being undertaken as part of the 2014/15 plan of work.

1. Introduction

1.1 Whilst only the Report Summary and the Action Plan is attached for consideration by Members, it should be noted that full copies of reports are available if requested.

Each Internal Audit report contains an audit opinion based upon the work performed in respect of the subject under review. There are five audit opinions which can be provided:

(i) **Full Assurance**: There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.

(ii) **Substantial Assurance**: While there is a generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

(iii) **Reasonable Assurance:** Whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk**.**

(iv) **Limited Assurance**: Weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.

(v) **No Assurance:** Control is generally weak, leaving the system open to significant error or abuse, and/ or significant non-compliance with basic controls leaves the system open to error or abuse.

2. Final Report – Pensions System

2.1 This report has an audit opinion of Substantial Assurance as the three audit objectives were substantially achieved but a number of areas for improvement were identified. As a result there were seven recommendations made which were due to be implemented by 31/05/14. Six of these have since been actioned and the remaining high action (ref 3.2.1) has a revised target date of 30/09/14.

3. Audit Plan 2014/15

3.1 The following work is being undertaken as part of the 2014/15 the Pension Fund Audit Plan:

(i) Audit Review of Pension Fund Payments - this work is at the stage of the fieldwork being completed.

(ii) Work to support the Statement on Internal Control for 2013/14 – this audit has been completed and the draft report has been issued.

It is expected that both of these audit reports will be provided to the November Committee meeting.

4. Implications

4.1 There are no Resource; Legal; Equalities; Climate Change/Carbon Clever; Risk and Gaelic and Rural implications arising from this report.

Recommendation
Members are invited to consider the attached Final Report and note the status of this year's planned audits.

Designation:	Head of Internal Audit & Risk Management
Date:	1st August 2014
Author:	Donna Sutherland, Audit & Risk Manager

Background Papers

AUDIT REPORT SUMMARY

Report Title

Finance Service - Pensions System

Report No.	**Type of Audit**
HK28/004.bf	Computer

	Issue Date
Draft Report	25/10/13
Final Report	03/12/13

1. Introduction

1.1 This computer audit was undertaken as part of the annual plan for 2012/13. The findings from this audit were included within the annual Pension Fund Statement of Internal Control.

1.2 The Highland Council is the Administering Authority for operating the Local Government Pension Scheme Pension Fund. The Fund provides pensions for eligible employees of the Council, Comhairle Nan Eilean Siar, and other Scheduled and Admitted Bodies. As at 31/03/12, in addition to the Council and Comhairle Nan Eilean Siar, there were 14 Scheduled and 25 Admitted Bodies within the Fund.

1.3 Towards the end of the review a new release of the Pensions System software was installed. An examination of the new release was not included in this review except for a reference to new access control groups which have been introduced.

2. Review Objectives

The objectives of the review were to ensure that:

2.1 Physical and logical access controls comply with best practice.

2.2 Application controls in terms of input, processing, output, audit trail, backup, restore and business continuity are satisfactory.

2.3 Contractual license, security and support arrangements are in place.

3. Main Findings

The main findings of the review, referenced to the above review objectives, are as follows:

3.1 This objective was substantially achieved. The supplier has an ISO 27001 certificate which is valid until 19 December 2014. The certificate states that its Information Security Management System complies with the requirements of ISO 27001. Users connect to the supplier's website via a secure Citrix Xenapp link. In order to access the system users have to complete a user access form. It then has to be signed by a senior member of the Pensions Section. Hence a formal user registration system is in place. Access permissions to the system for users are set up by the Finance Systems Administration Team in accordance with their job roles. Password complexity is enforced by the system. Access to the Pensions Section shared network folder is only accessible by two Pensions Section windows security groups. Membership of these groups has been authorised by senior Pensions Section staff.

However three areas of improvement were identified:

- An Access Control Policy is required to document business and information security access requirements. Users who access the system should be set up in accordance with the Policy
- Pension users should be automatically disabled if they have not logged into the Pension System after a specified period of time in order to reduce the risk of unauthorised access
- Access to the Pensions Section Office should be physically restricted by numerical keypad lock as the office contains a lot of paper based confidential personal information. The office is also shared with the Payroll Section, two Revenues Sections

and two managers from Transport Environmental and Community Services.

3.2 This objective was substantially achieved. There are some documented procedures in place in relation to data input. A check of employee pension contributions which had been loaded to the Pensions System via the interface showed that all were correctly loaded. Output reports are checked to be correct. There is an audit trail of user actions on the system. The supplier contract identifies the backup and recovery arrangements in place and the business continuity plan.

The areas for improvement are as follows:

- Many employers currently email spreadsheets with details of pension contributions insecurely to the Pensions Section because they do not have access to the government's secure email system. Employee year end pension contribution totals should be transferred using the Council's secure extranet
- Employers should send in Compliance Certificates to verify that they complied with Highland Council Pension Fund and regulatory requirements
- The documentation relating to the load of employee year end pension contributions needs improvement. It needs to be more specific in relation to the actual tasks carried out and more up to date as, for example, it refers to files dating from 2002/2003. It also states that interface files should be stored on a c: drive which is not recommended as c: drives are not backed up.

3.3 This objective was substantially achieved. An Application Services Provider Agreement is in place which ensures the Pensions System is properly licensed and supported. The Finance Systems Administration Team has set users up in accordance with the Agreement. Section 10 of the Agreement details how changes to the Pensions System are controlled.

The only area that could be improved is to ask the supplier whether the Application Services Provider Agreement could be in accordance with Scottish Law as opposed to English Law.

4. Conclusion

4.1 The objectives of the audit have been mostly achieved. The access controls and the contractual license and support that were checked were almost all in place. In addition the sample of employee year end pension contribution totals reviewed were all loaded correctly into the Pensions System. In terms of improvement, the Pensions Section should make use of the Council's extranet for the secure transfer of personal pension data.

4.2 There are seven recommendations in this report. One is classified as high priority and six are classified as medium priority. All the recommendations will be implemented by the end of May 2014.

5. Audit Opinion

5.1 The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Substantial Assurance** can be given in that while there is a generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

AUDIT REPORT ACTION PLAN

Report Title	**Report No.**
Finance Service - Pensions System	**HK28/004.bf**

The Action Plan contains **7** recommendations as follows:

Description	**Priority**	**Number**
Major issues that managers need to address as a matter of urgency.	High	1
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	6
Minor issues that are not critical but managers should address.	Low	0
Total recommendations		**7**

REPORT REF.	**GRADE**	**FINDING**	**RECOMMENDATION**	**MANAGEMENT AGREED ACTION**	**IMPLEMENTATION**	
					RESPONSIBLE OFFICER	**TARGET DATE**
3.1.1	Medium	**Access Control Policy Required** Although access permissions are set up by FSAT in accordance with their job roles, an Access Control Policy does not exist for the Pensions System.	An Access Control Policy should be produced by senior staff in the Pensions Section for the Pensions System.	An Access Control document based on standard template will be produced	Technical and Communication Officer	31/01/14
3.1.2	Medium	**Facility to Automatically Disable Users Required** The system does not have a facility to automatically disable users who have not logged into it for a prolonged period, e.g. 3 months	The member of staff from the Pension Section who attends the supplier's user group meetings should raise the need for this facility with the supplier.	The requirement will be raised with the supplier account manager	Payroll and Pension Manager	31/12/13

AUDIT REPORT ACTION PLAN

Report Title	**Report No.**
Finance Service - Pensions System	**HK28/004.bf**

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.1.3	Medium	**Restricted Access to the Pensions Office** The Pensions Section and the Payroll Section share the same open plan office with two managers from TECS and two teams from the Revenues Section. This office contains a lot of paper based personal information. There is no restricted access, such as a numerical keypad lock which requires an access code, on the two doors which are used to access the office. The effect of this is to make the office is to increase the risk that pensions and payroll information may be accessed by unauthorised staff.	Numerical locks should be put on the two access doors to the pensions and payroll office to help prevent unauthorised access.	This recommendation will be raised with all parties who use the office.	Head of Exchequer	31/05/14
3.2.1	High	**Insecure Delivery of Pension Contribution Data** At financial year end employers email spreadsheets to the Pensions Section which contain each employee's National Insurance Number and a total of their pension contributions for the year. Many of the employers do not have access to the government's secure email system which means that their employee personal information is being transferred to the Pensions Section via an insecure method.	Pension Section staff should contact the Senior Information and Security Officer in ICT Services to learn how to use the Council's secure extranet. They should then advise employers on how to use it to transfer spreadsheets containing employee year end contribution totals. The secure extranet should also be used for any other transfers of personal information from employers to the Council.	The Senior Information and Security Officer will be contacted in order to establish how Pensions staff can use the secure extranet. Once this is known, employers will be instructed on how to use it to transfer files securely.	Payroll and Pension Manager	31/05/14

AUDIT REPORT ACTION PLAN

Report Title	**Report No.**
Finance Service - Pensions System	**HK28/004.bf**

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.2.2	Medium	**Compliance Certificates** Employers who currently send in employee year end pension contribution totals to the Pensions Section do not send also send in Compliance Certificate. A Compliance Certificate is a statement by the employer verifying that it has complied with a range of Highland Council Pension Fund and regulatory requirements in relation to pension's administration. This method is used by the Strathclyde Pension Fund to ensure employer compliance.	The Pension Section should consider introducing a Compliance Certificate for employers to sign to verify that they have complied with a range of Highland Council Pension Fund and regulatory requirements in relation to pension's administration.	A certificate will be issued going forward.	Technical and Communication Officer	30/04/14
3.2.3	Medium	**Employee Contribution Load Documentation Needs Improvement** The documentation relating to the load of year end pension contributions needs to be completed and updated, so that it can be easily used by less experienced Pension Section staff if required. Reports which detail when text files containing employee year end contributions are not retained for a specified period.	The guidance relating to the load of employee year end pension contributions should be updated and improved to show clearly how to load pension data into the system is not up to date. Reports which document the results of text file load of employee year end pension contributions should be retained for a clearly defined period of time.	Year-end procedure documentation will be completed	Technical and Communication Officer	31/12/13

AUDIT REPORT ACTION PLAN

Report Title	**Report No.**
Finance Service - Pensions System	**HK28/004.bf**

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.3.1	Medium	**License Agreement not in Accordance with Scottish Law** The Application Services Provider Agreement was not checked by a member of Legal and the agreement is covered by English Law.	ICT Services governance arrangements should ensure that all IT license agreements are checked by a member of Legal and the agreement is covered by Scots Law is possible. The supplier should be asked whether the Application Services Provider Agreement could be in accordance with Scottish Law as opposed to English Law.	The requirement will be raised with the supplier account manager	Payroll and Pension Manager	31/12/13