The Highland Council

Audit and Scrutiny Committee – 20th June 2013

Agenda Item	4
Report No	AS/10/13

Updates of Actions Arising from Internal Audits of Fuel Cards, CareFirst and Business Community Planning

Report by the Head of Internal Audit & Risk Management

Summary
This report provides Members with an update of the progress in implementing the actions arising from three reports which were presented at the last meeting on 28th March 2013.

1. Background

1.1 At the last Audit & Scrutiny Committee of 28th March 2013 Members were presented with eight final Internal Audit reports, of which three were follow up reports. In view of the limited assurance given to two of the follow up reports and the numbers of actions still to be completed, Members requested that a report should be submitted to the next meeting in order to confirm that the recommendations had been completed satisfactorily. The reports concerned are as follows:

- Administration of Fuel Cards (follow up)
- CareFirst (follow up).

In addition, Members also requested an update with regard to the following review in view of the limited assurance given together with the high number of actions to be completed:

- Business Continuity Planning.

2. Updates of Actions Arising

2.1 Administration of Fuel Cards (follow up)

The actions taken to date are provided at **appendix 1** which shows that all of these have been completed. In respect of the high priority action referred to at Section 3.3.2, this was to complete an options appraisal for a fuel monitoring system by the end of June 2013. Further comments on this are as follows:

(i) The options appraisal has now been completed and on 17th May 2013 a meeting took place between the Director of TEC Services, the Director of Finance, the Head of Internal Audit & Risk Management, the Head of Roads & Community Works, the Head of Procurement and the Fleet & Maintenance Manager. The appraisal noted that information on fuel drawings using the Council's Vectec system (relating to drawings from in-house fuel tanks) and using fuel cards (relating to external drawings at agency garages) is held in different systems, managed by different staff and that these need to be reconciled before fuel consumption can be managed effectively.

(ii) The above meeting concluded that monitoring by TEC Services Stores staff was the best immediate solution but the introduction of vehicle tracking would provide a better longer term solution. The following actions were therefore agreed:

- The Vectec system suppliers would be asked to provide a quote for the supply of software to merge the two sets of fuel data. This action has now been completed.
- The latest version of Vectec software will be introduced in order to facilitate Stores staff in implementing the change.
- A staff resource would be provided within the Stores Section to undertake monitoring.
- A business case for vehicle tracking would be developed with a view to undertaking a procurement exercise.

The above actions are due to be completed by 1st November 2013 or earlier.

(iii) It is important to emphasise that a number of additional measures have also been taken in the interim:

- The Director of TEC Services has instructed his management team to make supervisory staff aware of the potential for misuse of fuel cards, and for them to be vigilant.
- The audit report which was presented to the last meeting highlighted that the recording of mileages by drivers is currently poor. TECS Area Managers have now been instructed to monitor mileage recording more vigorously and use the disciplinary process if drivers persistently fail to record mileages.
- An exercise is under way to review in-house fuel storage with the objective of reducing it, except where needed as a strategic reserve in emergency situations.
- The use of fuel in cans (for small plant such as strimmers) is being reviewed as part of the overall fuel control exercise and numbered, colour coded and labelled cans are being issued to assist monitoring.

Members are asked that if they have any specific facts regarding fuel misuse to report these to the Head of Internal Audit & Risk Management for investigation.

2.2 <u>CareFirst (follow up)</u>

The actions taken to date are provided at **appendix 2** which shows that the high priority action has been addressed and that two medium priority actions now remain outstanding as follows:

(i) Section 3.1.3 refers to the production of corporate third party guidelines which have now been incorporated within the ICT User and Network Control Policy. However, to comply with ISO 27001, there needs to be a process to ensure that all third parties are made aware of the Council's information security policies. An Information Security Policy is due to be completed by the end of June 2013. It is necessary for ICT Services to review all ICT contracts, including those resulting from software procurements by other Services, e.g. Phoenix e1 system and Axise

Pensions system, to ensure non-disclosure agreements are included. This is now in progress and the ICT Delivery Manager has contacted the Procurement Section to ensure that it specifies, in their procedures, that ICT Services need to review any ICT related procurement contract.

(ii) The original audit report on CareFirst gave positive assurance that the majority of good practice password controls are in place within the system. However, it was highlighted that the system did not have the facility to force users not to re-use their existing password. Although this action has been progressed by the Health & Social Care Service Team Leader (Projects and Technology), it is dependent upon a new software release from the supplier which will be available by January 2014. In the meantime, passwords continue to be reset securely on a quarterly basis. Additional security is also provided through the need to access the Highland Council network before CareFirst can be accessed.

2.3 Business Continuity Planning

The majority of actions are not due to be implemented until 31st July 2013 or thereafter. However, **appendix 3** shows that six individual actions have now been completed and that good progress is being made by both TEC Services and ICT Services who are responsible for completing these. With regard to the general Business Continuity Plan, this has been drafted and has been presented to the Weekly Business Meeting. This is now being presented and discussed at Service Management Teams.

2.4 Remaining Internal Audit reports presented at the previous meeting

In addition to the above three reports, the undernoted reports presented at the last meeting also provided a limited assurance opinion. Comment is therefore provided in respect of these:

(i) LEADER Programme 2011/12: The Scottish Government recently put a new process in place to review all live projects and this will therefore address most of the issues raised in the report. It should also be noted that the LEADER Programme is subject to an annual review and therefore all actions will be followed up as part of the 2012/13 audit report.

(ii) Car Park Income Collection (Follow Up): There were three outstanding medium/low priority actions identified in the report, Two have been completed and one remains partially outstanding. This refers to correcting anomalies where fines paid are not recorded. Although corrective action has now been taken it is prudent to ensure that this action is effective and, consequently, this will be reviewed at the end of June 2013.

(iii) Investigation into Missing Public Convenience Income: There was one outstanding action which has now been completed following the re-tendering of the contract.

3. Implications

3.1 **Legal & Risk:** The implementation of the agreed actions referred to within the audit reports will reduce the risk exposure to the Council.

3.2 **Resource:** The introduction of a fuel monitoring system will require to be resourced by the Director of TEC Services.

3.3 **Finance:** The introduction of a fuel monitoring system will require to be resourced by the Director of TEC Services.

3.4 **Equalities:** There are no implications

3.5 **Climate Change:** There are no implications

4. Conclusions

4.1 This report shows good progress with regard to implementing the agreed actions referred to in the three Internal Audit reports.

Recommendation
Members are asked to note the good progress in implementing the actions arising from three reports which were presented at the last meeting on 28th March 2013.

Designation: Head of Internal Audit & Risk Management

Date: 11th June 2013

Author: Nigel Rose, Head of Internal Audit & Risk Management

Background Papers:

Appendix 1

Follow up of management agreed action

Report Title:	Report Ref:	Final Issued:
Finance Service: Administration of Fuel Cards (Follow-up)	HK33/016	15/03/13

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.2.2	Medium	Although a standard process for requesting new fuel cards is in place, the procedure is not being fully adhered too.	Procurement staff will return all applications not made on the appropriate form. They are already held securely as per the retention schedule.	Principal eProcurement Officer	Immediate	Purchase Card Administrators do not accept applications without a completed application form.	Yes
3.3.1	Medium	4% of diesel purchases reviewed for a six month period, did not have the vehicle's mileage recorded. Whilst odometer reports are issued to budget holders, these are not followed-up to ensure that the appropriate corrective action has been taken.	A monthly report showing cards for fleet vehicles where there has been a nil odometer reading will be sent to the relevant Budget Holders. Cards that have recorded nil transactions for 3 consecutive months will be highlighted to the relevant Budget Holders for action. The Fuel Card guidance will be amended to reflect this change.	Principal eProcurement Officer	31/03/12	Monthly reports are produced and sent to Budget Holders. The process and user guide has been amended to reflect the escalation procedure. June 2013 will be the first point of escalation (3 months from commencement of revised process).	Yes
		Second cards have been issued to some card holders for the purchase of petrol only. However, this cannot be enforced and there is a risk that multiple cards could be mixed up and/ or misused.	Procurement can amend the record form to show which cards are for petrol, which for diesel and which for both.	Principal eProcurement Officer	31/03/12	The application for all new cards requires the fuel type to be provided. Fuel type for issued cards has been requested. Nil responses have been escalated to Service Directors	Yes

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.3.2	High	Fuel consumption monitoring is not undertaken. In addition, there is no reference to fuel consumption monitoring in the Fuel Card User Reference Guide.	Options Appraisal to be produced.	Fleet & Maintenance Manager and Head of Procurement	30/06/13	Options appraisal produced and reviewed by Director of TEC Services and Director of Finance. Agreed to implement procedures to facilitate monitoring through TEC stores, which will reconcile information from the fuel card system with that from Vectec (Council system for in-house fuel bunkers).	Yes
3.3.3	Medium	Although a review of hire fuel cards has been undertaken, this was not documented. However, there has been a significant reduction in the number of such cards.	Further review to be undertaken and documented.	Business Support Operations Managers	31/05/13	Review completed.	Yes
		There is no guidance in place which sets out the necessary controls required for the use of unassigned fuel cards.	The Fuel Card User Reference Guide will be amended to more clearly reflect the requirement to maintain a log.	Principal eProcurement Officer	31/03/13	The Fuel Card User Reference Guide reflects the requirement to maintain a log.	Yes
		There are no checks undertaken to ensure that budget holders and card holders are complying with the requirements of the Fuel Card User Reference Guide.	Sample checks will be undertaken by Business Support on at least an annual basis.	Business Support Operations Managers	31/05/13	Sample checks completed and discussed with Internal Audit.	Yes
			The Fuel Card User Reference Guide will be amended to include the requirement by Business Support to undertake sample checks.	Principal eProcurement Officer	31/05/13	Fuel Card User Reference Guide has been amended.	Yes

Appendix 2

Report Title:	Report Ref:	Final Issued:
Health and Social Care Service / Chief Executive's: CareFirst (Follow Up)	**HG46/003.bf**	**18/03/13**

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.1.3	Medium	Carefirst information can potentially be accessed by third parties such as the Carefirst System supplier and the Council's ICT partner, but there is no clear corporate guidance on the monitoring and review of third party services.	Third Party Access Guidelines will be produced.	ICT Delivery Manager	30/06/13	The ICT User and Network Access Control Policy which covers Third Party Guidelines has been created and was approved on 16/05/13.	Part cleared
3.1.4	Medium	Although the majority of good practice password controls are in place, the Carefirst System does not have the facility to force users not to re-use their existing password	Release 6.11 is expected to be implemented before the end of April 2013.	H&SCS Team Leader (Projects and Technology)	30/04/13	Testing of release 6.11 has shown that the expected fix has not been included. This has been highlighted to the software supplier who has acknowledged the issue and committed to developing a solution by January 2014. This change is being implemented specifically at the request of THC and will be made available to all CareFirst customers in Scotland.	No

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.1.5	High	Although a variety of network access controls are in place, a corporate network access control policy does not exist to set the standard to control access to shared network folders that contain confidential CareFirst data.	A corporate access control policy on the use of network services has been drafted and will be finalised, approved and implemented.	ICT Delivery Manager	30/06/13	The ICT User and Network Access Control Policy which covers Third Party Guidelines has been created and was approved on 16 May 2013.	Yes
3.2.2	Medium	There is no corporate guidance for staff on sending emails with personal information to external recipients who are not on GSX email.	Advice has been sought from the Information Commissioner (ICO) which is awaited. Corporate guidance on sending emails containing personal information to external recipients who do not have access to GSX will be incorporated as part of the Information Security Management Framework.	ICT Delivery Manager	28/03/13	Guidance was obtained from the ICO in February 2013 Due to its importance a paragraph has been included in the revised Acceptable Use Policy which has been submitted for approval by the Finance, Housing and Resources Committee on 05/06/13.	Yes
3.2.3	Medium	It is not known whether a Database Administrator audit trail exists or is reviewed.	ICT Services will formally write to Fujitsu to obtain assurance on Database Administrator controls.	ICT Delivery Manager	28/02/13	ICT Services have received a positive response regarding the Database Administrator controls.	Yes

Appendix 3

Report Title:	**Report Ref:**	**Final Issued:**
TEC Services/ Chief Executive's: Business Continuity Planning Arrangements	**HH11/002**	**21/02/13**

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.1.1	High	There is no BCP for the Council to be used in any situation. A BCP specifically for the previous Influenza Pandemic is in place but is no longer current.	Complete the general Business Continuity Plan (BCP).	Emergency Planning & Business Continuity Manager	31/07/13	The general BCP has been drafted and is on target to be signed off by the due date.	No
			Seek approval for the BCP from Senior Management Team.		31/08/13	General BCP to be approved by the Senior management Team.	No
			Undertake annual review of the general BCP.		31/07/14	Ongoing.	No
3.1.2	High	A number of areas of best practice have been identified which should be included in the Council's BCP such as work area recovery, transportation where necessary and salvage strategy.	Establish Service-specific BCP working groups to create service-level response plans. These will become an integral part of the BCP.	Emergency Planning & Business Continuity Manager	31/01/13	Service-specific BCP working groups have been established to develop Service-specific BCPs based on a model developed within TECS.	Yes
			Review the BCP.		31/07/14	Plan review of BCP	No
		In addition, there are some Service specific issues which remain outstanding or need to be addressed within the BCP.	Establish Service-specific BCP working groups to create service-level response plans. These will become an integral part of the BCP	Emergency Planning & Business Continuity Manager	31/01/13	As above	Yes
3.1.3	Medium	A sample of officers listed in the INBS Influenza Pandemic Area BCP were contacted and it was found that the majority were not aware of their roles and responsibilities, did not have a copy of the BCP and had not received any training.	Roles and responsibilities will be described in Service-specific BCPs. Training will follow on from there.	Emergency Planning & Business Continuity Manager	31/12/13	Roles and responsibilities will be defined within Service specific BCPs with training to follow.	No

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.1.4	Medium	A sample of responsible officers listed in the INBS Influenza Plan BCP was selected. A number of these officers no longer worked for the Council, and of those still working for the Council only half were accurately recorded.	The directory has been created and issued in its first format.	Emergency Planning & Business Continuity Manager	Complete		Yes
			Update the datasets on a 4 monthly cycle.	Emergency Planning & Business Continuity Manager	Ongoing	Latest update of the Council's Emergency Communications Directory (ECD) in preparation.	No
3.2.1	High	The recommendations from a report on the recent flooding at Inverness College, which resulted in a network outage, have not all been implemented.	The corrective actions will be completed through the improved networks resiliency plan which will address the single point of failure within HQ of the pathfinder network and the internet connection.	ICT Delivery Manager	31/07/13	Work to be carried out in two stages (11th June and later in June) to address the issues.	No
		The Council's Inverness HQ has been found to be a single point of weakness in the Council's network. Should the building be destroyed or suffer a power outage, the Council's network will not function.	The design review will be completed through a separate work stream will address the servers which were not migrated as part of the data centre migration. These servers are located within HQ and Drummond, previous Education ICT Unit.	ICT Strategy & Projects Manager	31/10/13	Progress is being made.	No
3.2.2	Medium	The Council's IT BCP documents are incomplete.	The appendix of Council Officers will be completed and will be reviewed on a yearly basis to assure details are up to date.	ICT Delivery Manager	31/07/13	A list of contacts has been created and has been validated by Services.	Yes

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.2.2 (cont)			The incomplete sections of the business continuity disaster recovery plan for the datacentres has been elaborated and will be reviewed when the DR/BC is invoked. Information will be completed and will be reviewed as part of the annual DR/BC exercise.	ICT Delivery Manager	31/01/14	Sections have been updated as part of the annual Disaster Recovery walkthrough.	No
3.2.3	High	The decision regarding which services are critical should the back-up data centre be used has not been agreed between ICT Service and the Council's Services.	The critical services will be reviewed on an annual basis as part of the DR/BC annual review. A DR/BC "invoke" operating procedure will be updated to reflect the prioritisation of systems by the responsible officer within ICT Services.	ICT Delivery Manager	31/10/13	Service-specific BCP working groups are identifying critical ICT services as part of the BCP model. Results will be passed to ICT Client services for their consideration.	No
			Identify the limited capacity of the back-up data centre and include in the corporate BCP.	Emergency Planning & Business Continuity Manager	31/10/13	The limited capacity has been identified and this is reflected in the BCP.	Yes
3.2.4	Medium	Arrangements with some third party IT suppliers exist without having a BCP in place.	For the ICT third party supplier contracts owned by the Council, as part of the supplier meetings BC services will be assessed. For the third party Contracts under the Fujitsu contract, together with Fujitsu in the review meetings the BC will be assessed.	ICT Delivery Manager	31/10/13	Actions in progress and on target	No

Report Ref.	Grade	Finding	Management Agreed Action	Responsible Officer	Action Due	Action Taken by Management	Cleared Yes/ No
3.2.5	High	No annual testing of the IT BCP and Disaster Recovery Plans has taken place.	An annual testing of the data centre will be completed March 2013 and will be undertaken on a yearly basis.	ICT Service Delivery Manager	31/07/13	A BCP and DR plan walkthrough took place on 18/04/13 demonstrating and providing re-assurance that all processes and procedures are in place.	Yes