The Highland Council

Audit and Scrutiny Committee – 20th June 2013

Agenda Item	7
Report No	AS/13/13

Action Tracking Report

Report by Head of Internal Audit & Risk Management

Summary
The Audit and Scrutiny Committee receives regular updates to provide assurance that the agreed actions arising from audit reports have been satisfactorily implemented. This report provides information regarding the most recent action tracking undertaken since the last update provided to Committee on 20/09/12. This update covers the period from 01/07/12 to 31/05/13.

1. Action Tracking Process

1.1 The action tracking process operates as follows:

(1) Audit reports contain an Action Plan which details the areas of concern; management agreed action; target date for implementation; and the title of the Officer responsible for implementation.
(2) Once all of the target dates in the audit report have passed, the audit recommendations are action tracked. This involves contacting the appropriate Manager(s) to confirm that the agreed actions have been implemented.
(3) Where the agreed management action has not been undertaken, an explanation is requested. However, if this response is considered to be unsatisfactory, it is subject to further audit enquiry and/ or investigation. A revised implementation date will be agreed and this is action tracked once this date has expired.
(4) Where the action is not implemented by the agreed date and a revised date is agreed, this is reported back to the Audit and Scrutiny (A&S) Committee. In addition, where target dates have been changed, this is also reported.

The monitoring of both internal and external actions are undertaken by Services through the Quarterly Performance Review (QPR) process and these should be recorded on the Performance and Risk Management system (PRMS). Where possible, the action tracking process utilises the information recorded in PRMS to monitor the progress in implementing the agreed actions.

1.2 Where an audit is undertaken on an annual basis, the management agreed actions are followed up as part of the following's year's audit work. Such audits include the Leader Programme, Verification of Statutory Performance Indicators, Housing and Council Tax Benefit payments and Corporate Governance. Any outstanding recommendations are carried forward into the following year's report.

1.3 In addition to the action tracking process, individual follow-up audits are undertaken where the previous audit report had a number of high priority findings and/ or the audit opinion consisted of "limited assurance". There are five such audits in the 2013/14 audit plan; Corporate Internet use, School

Meals Income Collection and Monitoring systems, Contractor's Framework Agreement for works up to £50,000, Payments to Nursery Providers and Business Continuity Planning arrangements.

1.4 Regardless of the method used as described in 1.1 – 1.3 above or section 2 below, the results are summarised in the table provided at Appendix 1.

1.5 The Internal Audit Reviews and Progress Report provided to the A&S Committee on 28/03/13 included 3 follow-up audit reports in respect of CareFirst, Administration of Fuel Cards and Car Park Income Collection. All of these reports identified that a number of the previous management agreed actions had not been implemented. As a result of the concerns raised by Members in response to this Report, the Chief Executive requested a report from the Head of Internal Audit & Risk Management for discussion at the Weekly Business Meeting of 15/04/13. This was undertaken and revised procedures have now been put in place to ensure that management agreed actions are implemented timeously, including where a revised date is required this is flagged as an issue and escalated, and requests for time extensions are approved by a senior manager/ Director.

2. Performance and Risk Management System (PRMS)

2.1 PRMS provides the report information for the Service QPRs and the standard template of information includes details of all internal audit actions, the responsible officer and the "RAG" (Red, Amber, Green) status. The system allows the responsible officers to update the audit actions and also provides a free text box for recording any additional information.

2.2 PRMS has been rolled out on a Service by Service basis and the final three Services (TEC Services, Planning and Development and the Finance Service) have recently implemented the system.

3. Action Tracking/ Follow-up Findings

3.1 The report attached as **Appendix 1** provides a summary of all audit reports issued which have been subject to action tracking/ follow up. This shows that a total of 127 audit recommendations were made and the current position is that:

- 110 actions have been satisfactorily implemented.
- 16 actions have not been implemented and have revised target dates, further details are provided in section 3.2 below.
- 1 previous agreed action was subsequently not undertaken as the role of Service Risk Facilitator was removed from the risk management process and therefore the agreed action became redundant.

Audits with revised target dates and actions carried forward into the following year's report are action tracked once the target dates have passed in order to ensure that the agreed actions have been satisfactorily implemented. The outcome of this will be included in the next annual action tracking report to Committee. Therefore, Committee can be assured that all agreed actions are subject to a robust action tracking process and are informed of the results on an annual basis.

3.2 There are 7 audits which have a total of 16 actions with revised target dates and these are summarised below. The original Action Plans are provided identifying which actions have been completed; where actions remain incomplete explanations are provided. These can be found at Appendices 2 –

8 of this report.

- Electronic Content and Document Management System (**Appendix 2**)
  There are still 2 actions which remain outstanding and are now due for completion by 31/12/13. There have been a number of changes to the target dates which were linked to the implementation of a software upgrade which had been delayed. The Service is now reviewing their ICT plan.

- Phoenix e1 System (**Appendix 3**)
  When previously reported there were 9 actions which had revised target dates from 31/03/12 to 31/08/12. 5 of these have since been addressed but 4 remain outstanding, mainly due to part actions still to be completed, 3 of which are due by 30/06/13. The remaining action is due for completion by 31/08/13.

- BACS Payments (**Appendix 4**)
  When previously reported 3 actions remained outstanding. 1 of these has been addressed and the remaining 2 actions have further revised target dates. In addition, 2 actions have been reopened as a result of changes to the process for the approval of BACS payments. All actions are now due for completion by 31/08/13.

- AXIS Counter Receipting and Income Management (**Appendix 5**)
  3 actions remain outstanding relating to the finalising of an Access Control Policy for the system; a review of AXIS sites to ensure that payment card data held on paper is retained in accordance with the relevant regulations and the finalisation of an Information Security Policy. All actions are due to be completed by 30/06/13.

- Corran Ferry Income Collection (**Appendix 6**)
  1 high priority action in respect of an appropriate solution to ensure password security in order to meet the Council's policy for the Acceptable use of ICT and PCI DSS requirements remains outstanding and has a revised date of 30/09/13.

- Matters arising from the Statement of Internal Control (**Appendix 7**)
  1 action has a revised date and this relates to the amendment of personnel policies to incorporate the requirements of the Bribery Act 2010 and this is scheduled to be completed by 30/06/13.

- Car Park Income Collection (**Appendix 8**)
  1 action has a revised date which relates to the requirement to correct the anomaly that paid fines were not being recorded, resulting in reminders being issued. This anomaly has been corrected but it was considered prudent to allow a period of time in order to check that no further problems were occurring before this action is recorded as completed. These checks are scheduled to be undertaken by 30/06/13.

4. Implications

4.1 There are no Resource, Legal, Equalities and Climate Change and arising from this report.

4.2 Risk: The implementation of the management agreed actions will reduce the risk exposure to the Council.

Recommendation
Members are asked to note the action tracking information provided including the revised target dates for the completion of outstanding actions and the assurance provided at section 3.1 of this report.

Designation:	Head of Internal Audit & Risk Management
Date:	11th June 2013
Author:	Donna Sutherland, Principal Auditor
Background Papers:	

Appendix 1

Action Tracking Report - Highland Council Completed Actions

Report Ref and Name	Final Issued	Number of Recommendations	Number				Comments
			Cleared	Date Revised	No Action	Outstanding	
HL24/002 – IT Communications and Operations Management	01/02/08	7	7	0	0	0	Final outstanding action now completed.
HL25/001.bf – Compliance with IT Policy and Legislation	06/02/09	7	7	0	0	0	Final outstanding action now completed.
HK20/002.bf.bf – Electronic Content and Document Management System (ECDM)	20/11/09	12	10	2	0	0	When last reported 3 actions were outstanding and the dates had been revised more than once. One of these actions has now been completed and 2 (5.2.3 and 5.3.3) have further revised dates and remain outstanding, see Appendix 2.
HA09/003 - Common Good Funds (Follow Up)	23/11/10	3	3	0	0	0	Final outstanding action now completed.
HK42/002 - Risk Management	08/11/10	13	12	0	1	0	When last reported 3 actions were outstanding and the dates had been revised more than once. All have now been completed.
HC13/009.bf - Phoenix e[1] System	09/09/11	9	5	4	0	0	When last reported there were 8 actions with revised dates. 4 of these have since been completed and 4 remain outstanding in parts (5.2 a & b, 5.4 b, 5.5 b, 5.10), see Appendix 3.

Report Ref and Name	Final Issued	Number of Recommendations	Number				Comments
			Cleared	Date Revised	No Action	Outstanding	
HK07/006.bf.b.f.bf - BACS Payments	23/11/11	12	8	4	0	0	When last reported there were 3 actions with revised target dates and 1 where no action was proposed. Since then 2 actions have been addressed but 2 still remains outstanding with further revised target dates. In addition, 2 actions which were previously recorded as complete (5.2 (iv) and 5.5 (ii)) have been reopened and have new target dates, see Appendix 4 for details.
HK19/001 - Insurance	15/12/11	11	11	0	0	0	The target date for 1 action in respect of the production of an Insurance Strategy was revised from 31/03/12 to 30/09/12 and was completed by this date.
HK21/003.bf - Non Domestic Rates - Billing and Collection	16/11/11	4	4	0	0	0	The target date for 1 action in respect of changes to the reconciliation process between NNDR and Assessor's records was amended from 31/07/12 to 14/09/12, and was completed by this date.
HK16/010.bf - AXIS Cash Receipting and Income Management	05/03/12	8	5	3	0	0	See Appendix 5, dates have been revised for 3 actions (5.2, 5.3, 5.6a).
HK25/008.bf - Payroll	10/07/12	8	8	0	0	0	
HG05/006.bf - Nursery Payments System Weaknesses	31/07/12	4	4	0	0	0	
HC39/007.bf.bf - Aquadome System Weaknesses	10/09/12	7	7	0	0	0	
HH14/005.bf - Corran Ferry Income Collection	10/09/12	3	2	1	0	0	The target date for 1 action in respect of password security has been revised from 31/12/12 to 30/09/13 and a suitable solution is being pursued, see Appendix 6.

Report Ref and Name	Final Issued	Number of Recommendations	Number				Comments
			Cleared	Date Revised	No Action	Outstanding	
HK47/001 - Matters arising from the Statement of Internal Control 2011/12	12/11/12	5	4	1	0	0	The target date for the amendment of the Council's personnel policies to reflect the requirements of the Bribery Act 2010 has been revised from 31/03/13 to 01/07/13. See Appendix 7 for details.
HA50/001 - Verification of Statutory Performance Indicators 2011-12	26/02/13	4	4	0	0	0	
HH02/003 - Investigation into missing public convenience income	07/03/13	2	2	0	0	0	
HH03/002 - Car Park Income Collection (Follow-up)	18/03/13	8	7	1	0	1	1 action in respect of correcting anomalies in the recording of paid fines is partially complete, see Appendix 8 for further details.
Totals		**127**	**110**	**16**	**1**	**0**	

Appendix 2

Electronic Content and Data Management System (HK20/002.bf.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2.1	The PC containing the ECDM Scheduler application was not located in an area with restricted physical access.	3	A request had previously been logged with Fujitsu Services to relocate the Scheduler to secure Fujitsu accommodation when ECDM is next upgraded. Relevant Finance staff would then be given remote access to it. In view of the fact that there are no scheduled plans at the moment to upgrade the ECDM system Fujitsu Services has now been asked (12 Nov 09) to investigate whether the Scheduler can be moved prior to an upgrade. The implementation target date is dependent upon response from Fujitsu Services. Fujitsu Services accommodation move in coming months could well affect implementation date.	Policy and Development Manager (Finance)	30/06/10 Revised to 31/05/11, 30/09/11, 30/06/12 then 31/03/13	Yes
5.2.2	The storage area for ECDM paper documents is shared with other Finance Service staff members.	3	There is a shortage of segregated space available to the Finance Service. We initially stored 6 months worth of scanned work which was later reduced to 2 months work. We will continue to attempt to source additional space so that our ECDM scanned documents and the Pensions documents can be stored separately. Overall, we don't consider this to be a material risk as access is limited to the Finance Service only. A formal review of secure storage space will take place by the target implementation date.	Operations Manager (Finance)	31/03/10	Yes

Appendix 2

Electronic Content and Data Management System (HK20/002.bf.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2.3	There are too many users with access to the ECDM System User Maintenance screen.	2	During implementation in 2007, the Policy and Development Team requested that administration and user functions be separated. At that time, the supplier could not provide such a separation. A further request has been made, via Fujitsu Services (12 Nov 09), seeking the supplier to separate administration and user functions. In addition, discussions will be held with members of the Policy and Development, Finance Systems Administration and Operations Teams to consider whether the current number of users can be reduced/whether profiles need amended. **Update** The Service has stated that they are going through the process of reviewing their overall ICT plan at the moment to achieve efficiencies through business transformation.	Policy and Development Manager	31/03/10 Revised to 31/05/11, 30/09/11, 30/06/12, 31/03/13 then 31/12/13	No
5.2.4	Whilst agreements are in place with all third parties who can access the ECDM system, these do not comply with ISO 27002 requirements.	3	Provide corporate guidance to system owners that addresses security with third parties e.g. access and change is auditable and authorised.	IS Client Manager (Chief Executive's Office)	31/05/10	Yes
5.2.5	Some password controls were in place, but these do not fully comply with the requirements of the Council's ISSF.	3	FSAT to investigate password configuration options and update as necessary after testing.	Finance Systems Officer	31/01/10	Yes
5.3.1	The standard interface programmes which reconcile the ECDM and the Revenues and Benefits systems data, provides limited control totals.	2	Call logged 16/4/2009 and work scheduled to commence after Fujitsu change freeze and Revs & Bens V6 project completed.	Finance Systems Officer	31/03/10	Yes

Appendix 2

Electronic Content and Data Management System (HK20/002.bf.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.3.2	An internet e-mail is published on the Council's website and may be used by members of the public and external bodies to provide information to Operations staff. There is no warning provide that internet e-mail is not regarded as a secure medium for transferring personal data.	2	Assure a consistent corporate approach to the use of internet e-mail addresses, i.e. always use standard form and have standard warnings on top of page. Produce corporate guidance for all ICT users that sending unencrypted internet e-mails containing personal, or sensitive personal, information to the public or staff in external organisations represents bad practice and is not in line with ICO recommendations. Initial guidance to be part of the 2nd ICT security newsletter and the revised Acceptable Usage Policy.	IS Client Manager (Chief Executive's Office)	31/05/10	Yes
5.3.3	There are no archiving or secure disposal procedures in place for electronic documents held within the ECDM System.	3	Procedures to be developed in accordance with corporate guidance. **Update** As per 5.2.3.	Policy and Development Manager	31/03/10 Revised to 31/05/11, 30/09/11, 30/06/12, 31/03/13 then 31/12/13	No
5.3.4	There is no report available which tracks changes to user access, such as the creation and deletion of users.	2	A report run through Crystal reports has been developed and does this. This has been sent to Audit for review.	Finance Systems Officer	01/06/10	Yes
5.3.5	There is no business continuity plan for the ECDM System.	2	Business Continuity Plan to be developed.	Policy and Development Manager	31/03/10	Yes

Appendix 2

Electronic Content and Data Management System (HK20/002.bf.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.4.1	There is no monitoring of the number of ECDM users against the number allowed by the User License agreement.	3	FSAT will monitor as part of the user control process of the Finance systems. In addition the purchase of a site license is being investigated which will remove the need to monitor the number of users.	Finance Systems Officer	01/12/09	Yes
	In addition the ECDM Service Description does not contain the number of users that the Council is licensed for.		The number of licenses will be included within the ECDM Service Description.	Finance Systems Officer	01/12/09	Yes
	There is a lack of monitoring of the number of users set up against all large computer applications.		The FSAT will monitor and the number of users set up against the other applications they manage. As part of the new Partnership Agreement ICT Services will work with Fujitsu Services to ensure all license arrangements are appropriately monitored and guidance will be provided to system administrators of large applications.	Finance Systems Officer & IS Client Manager (Chief Executive's Office)	31/05/10 Revised to 30/06/11	Yes
5.5.1	Staff members operating the ECDM System were unaware of the British Standard BSI 10008, the Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems.	3	Guidance to be provided to relevant users.	Policy and Development Manager	31/03/10	Yes
	The ECDM System supplier has not provided a statement of compliance with BSI 10008.		The ECDM System supplier will be asked to provide a statement of compliance with BSI 10008.	Policy and Development Manager	31/03/10	Yes

Appendix 3

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2	a) Although a draft Access Control Policy for Phoenix e¹ System exists, it has yet to be finalised. The lack of a finalised Access Control Policy which defines the standards of access to the system increases the risk of unauthorised access to the Phoenix e1 System.	2	The Access Control Policy will be finalised and sent to the Senior Information and Security Officer/ISMG for review and sign off. **Update** This has been drafted and will be completed and sent to the Senior Information and Security Officer by 14/06/13.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12, then 30/06/13	No
	b) Users were set up to access e¹ by the Project Team after being trained on e¹. A formal User Registration System which ensures that all changes to user access is properly authorised and evidenced is not yet in place. However steps are being taken to put one in place.		For secondary schools the Phoenix Manager has formally approved the access levels as at a given baseline date. Any changes after that date are recorded and formally approved by the Phoenix Manager for the school. For primary schools access for users is requested by the Head Teacher through the Fujitsu user management requests system and recorded by the Phoenix e¹ support team. The access of other corporate users is being recorded and has been formally approved as at a given date. Any future changes will be approved by the Phoenix e¹ Project Manager. A formal User Registration System will be established in order to comply with ISO27001. **Update** See a) above.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12, then 30/06/13	No

Appendix 3

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2 (cont'd)	c) As expected there are many different e¹ job roles set up to control user access. However it is not possible to obtain a report of user access rights or job role access rights. Therefore it is more time consuming and difficult to assess whether user job roles are appropriate for their posts.		Job Role Access Rights are known and available (via individual spreadsheet files). A request has been made for the supplier to supply a regular report on any enhancement or reductions made to a user's access rights (PPS6019).	Performance and Business Support Manager	31/03/12	Yes
	d) Some generic usernames exist within the Phoenix e¹ System. These have been picked up in the list of anonymous logins that was provided by the e¹ supplier to the Phoenix e¹ Project Manager.		This has been incorporated into the Service Description and will form part of the license agreement.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
	e) The system does not disable users who have not logged into e¹ for a considerable period of time, but an enhancement request (J2791) has been made by the e¹ team to automatically disable a user if the user has not used the system for 3 months.		The enhancement request to automatically disable users who have not used the system for a prolonged period has been made with the supplier. Timescales are awaited. If this enhancement is not forthcoming an alternative would be to ask the supplier to produce a report of user logins over 3 months and to disable staff who had not logged in during that period.	Performance and Business Support Manager	31/03/12	Yes
	f) The school staff questioned were not aware of the key points in the latest Council Information Security Newsletter.			Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes

Appendix 3

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.3	a) In one school visited paper documents containing personal pupil details are contained in a locked room where staff such as cleaners or the janitor could gain access to it.	2	A School Support Review is being carried out and consideration will be given as to how data protection responsibilities are incorporated within job roles in order to ensure that this control is delivered. The Review is due to report at the end of June 2011. These points were highlighted to schools in Admin Circular 4/10. The Service is also reviewing this guidance to schools in relation to information security and data protection and will highlight and strengthen this as required. Further monitoring arrangements will be established for school staff with regard to the security of paper based personal information. A School Support Review is being carried out and consideration will be given as to how data protection responsibilities are incorporated within job roles in order to ensure that this control is delivered.	Performance and Business Support Manager	31/03/12	Yes
	b) Primary 7 Pupil Profile Records (PPR) are transferred from the primary school to the secondary school by school staff using cars This is not the most secure method and the physical transportation is not carried out formally and securely, according to established and agreed protocols with sign-offs at each transfer stage.		The method of transfer of paper based PPRs will be reviewed with a view to making the transfer more secure. Recommendations will be incorporated into revised guidance issued.	Performance and Business Support Manager	31/03/12	Yes

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.3 (cont'd)	c) In one of the schools visited the school server was found in a locked storage room. However, it was located under a water pipe and was visible from the window. The server is left on overnight and there is no smoke alarm within the room. In another school that was visited the server was located in a classroom that was not always supervised.		This finding does not have specific bearing upon Phoenix e¹ but it is a risk that the Service needs to address. The Service will liaise with ICT Services and Fujitsu in relation to the risk assessment of the security of school servers. Guidance will also be incorporated into the review of information security guidance.	Performance and Business Support Manager	31/03/12	Yes
5.4	a) Supervisory sample checks are not carried out on the data entered into the system. The main check for pupils is the annual update of contact details whereby the school asks pupils to verify the contact details they have are correct and up to date. There is also an annual check carried out on staff details. However a brief review of one of the schools visited found that the personal details of staff who had not worked for the school for over ten years were still on the system. The area education guidance states that the records should be retained for six years after termination of employment. These examples may breach the Data Protection Act in that personal data is held for longer than is necessary.	3	A School Support Review is being carried out and consideration will be given as to how this control is delivered. The Review is due to report in November 2011. The Staffing Unit are now responsible for maintaining staffing records in e¹ and they will be given guidance in relation records retention for who have left the employment of the Highland Council. All secondary school information is being reviewed and updated currently by the Staffing Unit, and staff members who have left and whose personal details are no longer required will be removed from the system.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12, then 31/08/13	No
	b) Phoenix e¹ users were trained using supplier's training manuals. However they do not have documented in-house procedures for inputting data into the e¹ system.		In- house user procedures exist for specific aspects relating to e¹. Procedures will be produced, where required, which cover in-house specific procedures for areas not yet covered.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.4 (cont'd)	c) There is currently no timetable detailing the timing data input, data processing, and reporting activities. However, the Phoenix e[1] project manager said he would produce one.		A timetable covering all system activities including data input, the processing of interfaces and when output is required will be produced.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
5.5	a) The EMA interface does not have feedback to confirm the correct number of pupils will be paid to members of office staff in the schools who output the data from the Phoenix e[1] system.	3	The supplier and the EMA Unit will be asked if the interface procedures for Phoenix Central II can be changed to incorporate EMA control totals which will provide feedback to the schools on what exactly has been to be processed for payment.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
	b) A member of the office staff from one the schools visited said that all data processing procedures were not documented.		As with data input above all in house procedures relating to Phoenix e[1] will, where required, be properly documented. **<u>Update</u>** Assurance has been given that the interface procedures will be in place by 14/06/13.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12, then 14/06/13	No
5.6	Reports from e[1] can be downloaded onto the personal PCS/laptops of teaching staff. At this point the Council loses controls over equipment internet security, access, audit trail, secure disposal of the reports.	2	School staff members have been advised as follows "avoid saving personal data onto your laptop or home PC by copy and pasting or saving reports or documents onto the desktop or My Documents. Use an encrypted pen drive instead". This guidance will be reiterated and where necessary, strengthened with examples of work which contains personal information covered by the DPA, such as pupil report cards.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes

Appendix 3

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.7	a) The system has a form level audit trail, but this does not record all transactions, so it is incomplete and of limited value. In addition the Phoenix e¹ supplier can provide an audit trail of users who have logged in. However, the login audit trail is not monitored by HC staff on a regular basis.	3	The supplier has been asked to provide the sign on audit trail. It will be monitored on a regular basis for unusual activity. They will be asked whether or not Highland Council staff can have direct access to it as opposed to being sent reports.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
	b) The EMA audit trail does not pick up the authoriser from the username. Instead it has to be typed in. A change request ref J3387 has been logged with the supplier.		The change request ref J3387 to correct this has been logged and will be followed up	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
	c) It is not known how long the audit trails are retained for and there is no policy/procedure for archiving the e¹ audit trails.		The retention time for the audit trail will be identified and documented. A procedure for archiving Phoenix e¹ data, including the audit trails, will be produced.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
	d) The Phoenix e¹ supplier staff act as Database Administrators (DBA) for the e¹ system. As such they may have access to Highland Council staff and pupil personal information that is not recorded on e¹ access controls or audit trails, i.e. "access by the back door". Hence the controls over DBA activities are unknown		The supplier has confirmed that DBA activity is not logged in e¹, but administrator access is logged by the Windows o/s. The supplier will be asked to confirm, however, exactly how DBA activity is controlled and monitored e.g. via documented procedures	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
5.8	The length of time system back-ups are retained for is not detailed in the SLA, nor is the supplier's method of their method of secure disposal.	3	The supplier has confirmed that backups are managed by another company on their behalf. The supplier will be asked to clarify the length of time that system back-ups are retained and to identify the method of secure disposal.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes

Appendix 3

Phoenix e1 System (HC13/009.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.9	A requirement for a business continuity plan has been inserted into the License Agreement by the Highland Council. It is not known whether it has been accepted by the e¹ supplier.	3	The supplier has confirmed that they do have a Business Continuity Plan and full BS25999 documentation and they are tested regularly. They are not circulated, however. The business continuity plan will be agreed within the License Agreement and the supplier will be asked to provide it to the Council on a regular basis.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12	Yes
5.10	An unsigned copy of the license agreement was provided for review. Escrow is not included within the agreement.	3	The license agreement will be agreed and signed off. The inclusion of escrow will be re-considered. If it is not included then the Phoenix e¹ Project Board will be made aware of the risks of not doing so. **Update** Escrow has now been included in the Phoenix e1 Contract, but the Contract has not yet been agreed and it looks as if a re-procurement exercise will have to take place.	Performance and Business Support Manager	31/03/12 Revised to 31/08/12, then 01/04/14	No

Appendix 4

BACS Payments (HK07/006.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2 (i)	Staff involved in BACS processes do not all have direct access to BACS Rules and guidance documentation on the BACS website. BACS Service User's Guide and Rules to the Direct debit Scheme are updated on a regular basis.	2	Public Folders to be set up for relevant staff, and updated twice per year	Business Support Officer and Assistant Manager Income & Recovery, Finance	29/02/12	Yes
5.2 (ii)	There is no Access Control Policy with advice on logical and physical access requirements for BACS, access to the BACS Payments website, access to BACS software, access to BACS hardware and smartcards.	3	Access Control Policy to be drafted.	Business Support Officer & Systems Administration Manager, Finance	31/01/12 Revised to 30/09/12, then 31/08/13	No
5.2 (iii)	Council staff are not identified as Primary Security Contacts (PSC) for Highland Service Accounts. There is no nominated person or Section within the Council with overall responsibilities for BACS submissions as advised in the BACS Approved Bureau Scheme Support Guidelines. Instead, this is the responsibility of Fujitsu Services.	2	(Non submitter) Bank privileges for direct monitoring by PSC and Assistant to be set up. PSC to monitor daily, viewing reports of pending transactions, downloading and confirming that all batches are processed once correctly by Fujitsu.	Head of Exchequer & Revenues and Business Support Officer, Finance	31/12/11	Yes

Appendix 4

BACS Payments (HK07/006.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2 (iv)	Access levels in BACS software have not been set up in line with BACS Guidance and Rules, the ISO27002 Standard guidance on best practice and the Council's Financial Regulations. Operators all had high level Administrator access settings.	3	Access levels in BACS software to be reviewed in line with BACS Guidance and Rules, the ISO27002 Standard guidance on best practice and the Council's Financial Regulations. **Update** Fujitsu's staff duties were not separated but Finance staff were carrying out checks and so this action was recorded as complete. However, this Finance check stopped when the Fujitsu staff and BACS processing moved to Beechwood. A new BACS Service Description has been drafted which includes the appropriate segregation of duties. This has to be signed off by both parties.	ICT Service Delivery Manager	31/03/12, Revised to 31/07/13	No
5.2 (v)	PCs used for BACS processing also had non- BACS data (ODEX) stored on them. This does not follow BACS baseline physical security control guidance	3	The PCs used for BACS processing should not have any non BACS data stored. Both PCs should have the same build and provide resiliency for the BACS Service.	ICT Service Delivery Manager	29/02/12 Revised to 30/11/12	Yes
5.3 (i)	There is evidence of BACS being provided as a supported interface in the ICT contract agreed with Fujitsu Services. There is detail in some systems Service Descriptions, but there is no specific Service Description for BACS. The Council is registered as a direct submitter for BACS and Fujitsu officers complete BACS processing.	2	The issue will be addressed as part of contract management arrangements. **Update** Will be addressed by the new Service Description referred to at 5.2 (iv) above.	ICT Service Delivery Manager	30/04/12, Revised to 31/12/12, then 31/07/13	No

Appendix 4

BACS Payments (HK07/006.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.5 (i)	BACS operators have no warning in advance of transmissions required for each day so it is not possible for operators to plan for BACS workloads in advance.	3	A schedule will be set up between Fujitsu and Highland Council and logs will be kept of all BACS processing including the exceptional ones which are beyond the acceptable cut off time of 4 pm. Schedule to be populated with assistance from BACS Submitters contact list.	ICT Service Delivery Manager and Business Support Officer, Finance	31/03/12	Yes
5.5 (ii)	Input of submissions was completed by one single operator logging into BACS from start to finish. The BACS file was signed and submitted to BACS by the same operator. This does not utilise the option to separate these duties which BACS can provide and does not follow guidance in Financial Regulations – Internal Control.	2	Access control to be set whereby one processor creates the file and another processor logs in to check and submits. This would show as two separate ID's logged in the system and confirm a check is carried out for separation of duties. **Update** See 5.2 (iv).	ICT Service Delivery Manager	31/03/12 Revised to 31/07/13	No
5.5 (iii)	Guidance on addressing BACS file processing errors exists in the Fujitsu procedure notes for Council BACS Transactions. Error reports require timeous correction as reported in BACS guidance. However, Fujitsu reported that when these reports were forwarded to relevant Council contacts, they were not always acted on promptly.	2	The BACS guidance regarding the addressing of errors will be updated to include communication and escalation processes which will encompass the reporting on process errors. The Service User guide will be reviewed on a quarterly basis. Primary Security Contact to take pre-emptive action to ensure error reports are acted upon daily by BACs submitters.	Business Support Officer, Finance and ICT Service Delivery Manager	31/03/12	Yes
5.6 (i)	Audit trail detail of BACS processes is available to view by different means: Audit detail in the BACS software is not available to Council staff to view.	2	As necessary, designated council staff will be set with access to view the audit detail.	ICT Service Delivery Manager	Completed	Yes

Appendix 4

BACS Payments (HK07/006.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.6 (ii)	Audit trail detail in BACS Input Reports has not been set up for Council accounts. In addition, Item Limits which provide exception reporting of data are in place for only 5 of the 9 Council's User Accounts for monitoring transaction values and not for the accounts that have high value batch totals. Therefore, Item Limits on BACS payments are not all matched to the Council's insurance cover (Council's fidelity guarantee covers for losses of up to £0.5m) or the Council's risk appetite for potential losses.	3	The usefulness of setting up audit trail facility and Item Limits for all accounts to be investigated with Clydesdale Bank.	Business Support Officer and Systems Administration Manager, Finance	29/02/12	Yes
5.6 (iii)	No detail on time periods for monitoring and following up BACS reports is available in a schedule or timetable for BACS processing for the Council, as in 5.5. The sponsor prompts the Council when reports are not acted on in good time.	3	See 5.5 (iii).	ICT Service Delivery Manager	31/03/12	Yes

Appendix 5

AXIS Counter Receipting and Income Management System (HK16/010.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.2	The Council's Information Security Policy, called the Information Security Framework (ISF) includes third parties in its scope section 1.2, but this document is still not finalised. The link to the Council's ICT Third Party Policy is not available to view.	2	The Information Security Framework is being revised and part of the work is to include a Third Party Management Policy. **Update** Third Party access control has been included in the draft Information Security Policy which is due to be completed by 30/06/13.	ICT Delivery Manager	30/09/12 Revised to 30/06/13	No
5.3	Access Control Policies for AXIS Counter Receipting (ACR) and AXIS Income Management (AIM) modules defining security controls in place are still in draft format, dated 2007.	3	Policies to be updated to Council preferred standard for AIM, ACR, PAYE.Net and AXIS Admin.	Income and Recovery (I&R) Manager	30/09/12 Revised to 31/12/12, then 30/06/13	No
5.4	A sample of Axis users tested found that not all users have a documented and signed authorisation access request form on file. Some of these users have higher access settings and also transferred over from the old CR2000 Income System.	3	FSAT to be asked to provide a list of users with Authorisation and a list with Administrator access level. Income and Recovery (I&R) will then seek relevant Authority from Senior Manager (Customer Services Manager/ Head of Exchequer & Revenues for example).	I & R Manager	30/04/12	Yes
5.5	Separation of duties was unclear in Axis Counter Receipting (ACR) live system for the higher access settings Supervisors and Administrators. Compensatory controls are applied to monitor and record transaction reversals in Axis.	3	FSAT to be asked to provide a list of all users with access to this role. Access will then be reviewed.	I & R Manager	30/04/12	Yes

Appendix 5

AXIS Counter Receipting and Income Management System (HK16/010.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.6	a)Data stored on paper: An officer at one Axis site visited reported taking payment details by phone if a customer phoned the site and wanted to make a payment. The old Customer Card Information Document (CCID) was still available to write down payment card details on site. The Council's Service Centre is the designated site to take payments by phone using the new Secure Bureau Service, to reduce payment card details being stored on paper. Old payments made by payment card were validated by signature and paper copies require to be retained for 18 months as evidence. These merchant copies of APACS receipts are stored on site. The Income and Recovery Officer maintains a log to confirm when sites are notified of dates of old receipts that can be securely destroyed.	3	An on-going audit of AXIS sites is to be undertaken by I&R. This will incorporate the following: o Storage of data and its disposal o User list o Access Levels o ICT software and Hardware including Chip and Pin locations. A full site profile to be developed and site inspections to take place if necessary.	I & R Manager	30/09/12 Revised to 31/12/12, then 30/06/13	No
	b)Data stored electronically: Payment data was moved off old APACS servers by Fujitsu during the review onto servers at a more secure storage site. Requirements for secure disposal of old APACS data were provided by ICT Services Security Officer to Fujitsu who completed the task during this review. As this was on-going during the audit review, final assurance on secure disposal is not available. However, it is recommended this is obtained when completed.		The payment data on the APACS servers to be removed and disposed of securely.	ICT Delivery Manager	30/04/12	Yes

Appendix 5

AXIS Counter Receipting and Income Management System (HK16/010.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
5.7	a) Changes to Axis service provision have not been incorporated into a revised Service Description for Income System agreed with Fujitsu Services. b) Full terms and conditions of the licence agreement for Axis provision are not available.	3	As part of the Project going live an assessment is made internally by Fujitsu to evaluate impact of Service. Unfortunately the assessment was incorrect as it identified that there was no change to the Service Description. A new Service Description needs to be agreed which is the responsibility of Fujitsu. Fujitsu to be asked for an updated Service Description. The elaboration of this Service Description has been prioritised as part of the Correction Plan activities. The Terms and Conditions will be pursued and will be recorded in the ICT Services Contracts Register.	I & R Manager/ ICT Delivery Manager	30/09/12 Revised to 31/12/12	Yes

Appendix 6

Corran Ferry Income Collection (HK14/005.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
3.1.1	Explanations are not always provided for surpluses and deficits, and over the 6 month period to 30 September 2011, a net deficit exceeding £700 was recorded.	Medium	The ferry foremen already monitor and record surpluses and deficits and ask the pursers for explanation. They have been instructed to record action taken from now on. The Community Works Manager will monitor the actions taken by the foremen	Ferry Foremen	30/09/12	Yes
	For the same period, a total of 5 individual surpluses and 7 deficits were found to exceed the current £20 threshold but had not been reported to the Head of Internal Audit and Risk Management as is required by Financial Regulations Guidance Note "Receipt of Income".		The foremen have been instructed to inform the community works manager of individual surpluses or deficits over £20 and he will forward the information to the Head of Internal Audit and Risk Management.	Community Works Manager/Ferry Foremen	31/10/12	Yes
3.1.2	There are no formally documented procedures for the process of collecting and recording income. However, the ferry clerical assistants have started to document these in the form of a booklet.	Low	The procedures have been completed and put into use. With several months experience in use, these procedures are now being updated.	Business Support Officer, RSL Lochaber	Initial action complete; update by 31/10/12	Yes

Appendix 6

Corran Ferry Income Collection (HK14/005.bf)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
3.2	With regard to the acceptance of EFT card payments, not all requirements of the PCI DSS were being fully complied with. In addition, staff were unaware of the Council's IT policy on the Acceptable use of Information Systems, Communication and Technology.	High	The advice on individual passwords has not been possible to implement because of compatibility problems with the software for credit card payments, however the generic password is now restricted to the two ferry foremen and not the clerical assistants. This will need to be explored further with Fujitsu. The advice on protecting cardholder data, restricting physical access to cardholder data and destroying data which is no longer needed has been discussed with the ferry foremen, for immediate implementation. **Update** A call has been logged with Fujitsu in order to establish if a suitable solution can be identified.	Community Works Manager	31/12/12	No Revised to 30/09/13
			The policy on Acceptable use of Information Systems, communication and technology has been emailed to all staff and they have been informed verbally of the need to adhere to it.	Community Works Manager	Complete	Yes

Appendix 7

Matters arising from the Statement of Internal Control 2011/12 (HK47/001)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
3.1.1	A report to Audit & Scrutiny Committee on 22/09/11 outlined a number of Council policies which would be revised in light of the requirements of the Bribery Act 2010, however the Council's Whistleblowing Policy, Recruitment & Selection Policy and Code of Conduct for Employees have not yet been updated.	Medium	Update policies to reflect the requirements of the Bribery Act 2010.	Head of Legal & Democratic Services and Head of Human Resources, CEX's Service	31/03/13 Revised to 30/06/13	No
3.2.2	From a sample of 24 debtor invoices 8 invoices had not being processed within the required timescale set by Financial Regulations. 2 other invoices did not contain enough detail to determine when the service was provided. Also 4 invoices did not contain the correct level of detail required by Financial Regulations.	Medium	(1) Recent email issued to all AR users by Director of Finance confirmed need to adhere to Financial Regulations. (2) Instruction to be issued to ensure adequate information is included on future invoices.	Director of Finance Stores & Purchasing Manager, TEC Services	Complete 31/12/12	Yes Yes

Appendix 8

Car Park Income Collection (HH03/002)

Report Ref.	Area of Concern	Grade	Management Agreed Action	Responsible Officer	Target Date	Complete Yes/ No
3.1.2	Bank pay-ins in Lochaber are still based upon the audit ticket values rather than the actual income counted. In addition, it could not be verified whether there was any reconciliation undertaken between the cash counted by the bank to the values recorded by the audit tickets.	Medium	Input information into Oracle, undertake reconciliations and identify any anomalies.	Business Support Operations Managers	28/02/13	Yes
			Investigate anomalies and take corrective action if required.	TECS operational staff	28/02/13	Yes
3.2.1	There is no check undertaken within INBS Area to ensure that all fines issued can be accounted for. Audit checks identified 7 out of 535 issued fines which could not be accounted for.	Medium	Undertake reconciliations of fine notices on a regular basis.	Business Support Operations Manager (HQ)	28/02/13	Yes
			Correct anomaly in finance system where fines paid are not recorded in the council's finance system and examine opportunities for improving the service with the DVLA to access driver address. **<u>Update</u>** This anomaly has been corrected but time has been allowed to check that no further problems are occurring before this action is recorded as complete.	Income Recovery Manager and Business Support Operations Manager (HQ)	01/04/13 Revised to 30/06/13	No