Causeway Coast and Glens Borough Council

Internal Audit Report Review of Prior Year Recommendations – ICT Environment

February 2018

Final

MOORE STEPHENS

Table of Contents

1 Introduction

This internal audit was completed in accordance with the approved annual Internal Audit Plan for 2017/18.

This report summarises the findings arising from a review of the progress made by CCAG BC in implementing the prior year internal audit recommendations in the area of ICT Environment; this was allocated 5 days.

1.1 Objectives and Scope

The scope of this audit was to review the progress made by Council in implementing prior year internal audit recommendations in the area of ICT Environment.

The agreed audit objective was therefore to confirm that the internal audit recommendations have been or are being implemented.

1.2 Background

Council is committed to ensuring that key risks are identified and addressed as far as possible, the system of internal control is adequate and operating effectively and the policies and procedures in place are up to date and being followed.

As Internal Audit reports and findings identify possible risk areas, an important part of the internal audit service is to review the progress made in addressing prior year recommendations.

In 2016/17, the following recommendations were made following a scheduled internal audit of the ICT Environment process:

Risk	Number of recommendations			Total
	Priority 1	Priority 2	Priority 3	
There may be an inadequate (or no) formal governance structure in place for managing ICT leading to an uncoordinated approach to the development and management of the ICT systems	-	1	4	5
Access to the ICT systems and networks may not be controlled, leading to potential unauthorised access to sensitive information	-	4	3	7
There may be inadequate back-up arrangements in place to protect systems and data, resulting in a potential loss of information and data in the event of a system failure	-	-	-	-
There may be inadequate contingency and recovery plans in place to enable the system to recover in a timely manner in the event of a failure or disruption to the system	1	-	-	1
Total	**1**	**5**	**7**	**13**

The above recommendations have been revisited as part of this year's internal audit work programme. For each recommendation, we have discussed progress with the relevant officer and reviewed evidence of progress.

2 Results of Review

We reviewed the progress made in implementing the recommendations. The table below notes overall progress against recommendations at the time of our review (January 2018).

Status	Number of Recommendations			Total
	Priority 1	Priority 2	Priority 3	
Issue addressed	**-**	2	1	**3**
Issue being addressed	1	2	4	**7**
Issue not yet addressed	-	1	2	**3**
No longer a priority issue	-	-	-	**-**
Total	**1**	**5**	**7**	**13**

Priority 1 Recommendations
There was a single Priority 1 recommendation made and this is currently being addressed.

Priority 2 Recommendations
The table above shows that 2 of Priority 2 recommendations have been addressed, 2 are in the process of being addressed, and 1 is yet to be addressed.

Priority 3 Recommendations
In relation to Priority 3 recommendations, the table above shows that 1 recommendation has been addressed, 4 recommendations are being addressed and 2 have yet to be addressed.

It is acknowledged that much progress has been made since the original internal audit took place and that with the recent appointment of an ICT Security Officer, implementation of audit recommendations can be prioritised. We recommend that management continue their efforts to address internal audit recommendations and ensure that progress is regularly monitored and reviewed.

3 Update on Prior Year Recommendations

3.1 ICT Environment

Recommendation	Priority Rating	Management response & deadline	Position at January 2018
ICT should progress the implementation of its plans set out in the report to the Corporate Policy & Resources Committee in June 2016 so that an integrated approach to ICT across all Council sites and legacy systems is put in place. Consideration should also be given to developing a more detailed ICT Strategy (including a roadmap or action plan) which supports the Council's Estates Strategy and demonstrates how ICT will support delivery of the Council's corporate objectives	3	Agreed. The 3 ICT Management posts of Infrastructure, Operations and Digital Services are expected to be appointed in November 2016. (Patrick McColgan 1st April 2017)	All 3 management posts have now been filled. The structure of the ICT team is largely now in place. We reviewed the organisational chart and met with the Infrastructure Manager, and the acting Operations Manager (covering maternity leave). An ICT Strategy (and action plan) is under development; however, it is not progressed enough to allow review. It is hoped to have a first draft by end June 2018. **Issue being addressed**
ICT should review the requirement for external ICT contract support in Ballycastle to determine if it is required under the proposed structures. If the arrangement is to continue, a formal contractual arrangement should be put in place to cover the services of the ICT contractor and the responsibilities regarding safeguarding and maintaining confidentiality of Council information	3	Agreed. Issue is currently being addressed, as part of ICT Structure. (Patrick McColgan 1st April 2017)	We were advised that the arrangement with the ICT support in Ballycastle has not caused any issues for Council to date, and is therefore not a priority to be reviewed. However, this will be considered when developing the ICT Strategy (and action plan) **Issue not addressed**
The ICT policies and procedures should be finalised and implemented as soon as possible and ultimately staff should sign the policy acceptance sheet as evidence that they have read and accept these.	2	Agreed. Union representatives and other interested parties will be consulted to ensure that we move, in a sensitive manner, from the different legacy policies and procedures to an agreed CGBC	A list of all policies and procedures required has been created and many have been drafted but not yet formally finalised. Audit was provided with all draft policies (25) and procedures (24) which have already been drafted and also a list of policies and procedures which need to be reviewed in light of GDPR. Policies

Recommendation	Priority Rating	Management response & deadline	Position at January 2018
Training should also be provided for staff on key points within the policies and procedures, particularly where these may be different from legacy practices (eg prohibition of use of personal pen drives and risks of using same, procedures if need a third party to log-on)		configuration. The new policies and procedures must balance the needs of the organisation with the customs and practise of the legacy organisations. (Patrick McColgan 1st February 2017)	and procedures will be updated to ensure GDPR has been considered, discussed with union representatives and finalised in the coming months. **Issue being addressed**
ICT should continue to progress the configuration of the Microsoft System Centre so that a helpdesk system can be implemented as soon as possible to ensure that there is an adequate process for logging and tracking all incidents and identifying similar types of incidents that could indicate other issues	3	Agreed. A more informal approach was prevalent in the smaller organisations. The formalised helpdesk is currently being piloted in a controlled manner. (Patrick McColgan 1st April 2017)	We were advised that an ICT support e-mail address has been put in place. It is currently used to prioritize and respond to requests for assistance and the majority of staff use it when seeking IT help. There are plans to use the data collected from the ICT Support e-mail to identify recurring issues. Audit was advised that the majority of staff use the ICT support e-mail when they require ICT services. **Issue being addressed**
Managers should be reminded to ensure that mobile phone request forms are adequately completed and appropriately authorised. ICT should ensure that all forms are centrally stored as part of records management procedures. ICT should also request that all individuals issued with a mobile phone sign the Mobile Phone Policy Declaration as acceptance of the conditions of use. Further, consideration should be given to introducing a similar acceptance sheet for mobile devices such as iPads.	3	Agreed. ICT must take a more robust approach both with colleagues to ensure that the relevant paperwork is completed and in internal ICT Section practises. Mobile phone usage was formally the responsibility of disparate departments in the legacy Councils; in CCGBC, the ICT structure reflects the need for a more centralised resource. (Patrick McColgan 1st April 2017)	Audit was advised that Business Cases must be completed when making a request for hones or ICT equipment. The Mobile Phone Policy (reviewed by Audit) states that phones will not be issued without appropriate authorization, and all users sign a mobile phone policy declaration when receiving their new phone. There are plans to present a list of all issued ICT equipment regularly to SMT. **Issue addressed**
Consideration should be given to reinstating the sign-in logs for each server room so that an adequate record is	3	Agreed. The security recommendations will be reviewed as part of the ICT Security policy. (Patrick McColgan 1st April 2017)	An ICT Security Policy will be developed by the Security Officer. The ICT Security Officer has only recently been appointed and will take up his post on 1st February 2018.

Recommendation	Priority Rating	Management response & deadline	Position at January 2018
maintained of who accesses the server room and when. Consideration should also be given to implementing individual ICT Admin accounts to enable greater tracking, if required, of actions taken at an ICT Admin level.			Control of access to the server rooms will be considered as part of the development of the ICT Security Policy. No changes have yet been implemented. **Issue not yet addressed** Individual ICT Admin accounts have been created; and audit viewed a list of all administrator accounts which contain identifying details linked to the name of the administrator. **Issue addressed** **Overall issue being addressed**
Pin code or pattern access should be automatically enforced on Council-issued smartphones to prevent unauthorised access to Council email or information. ICT should also review the arrangements for staff accessing their Council email account on their own devices to ensure that any remote management policies that are applied on Council-issued devices can also be applied for user-owned devices. Further, consideration should be given to encrypting laptops to prevent unauthorised access to Council data in the event that a laptop is lost or stolen. In the meantime, staff should be reminded that information held on a laptop may be at risk if the laptop is lost or stolen and to therefore take care of the security of their device.	2	Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved. (Patrick McColgan 1st February 2017)	It is now Council policy to only issue smart phones with pin codes or pattern access in place. Audit observed 3 Council employees accessing their phone and noted that they could only be used until the pattern access or pin code was in place. All mobile phones are set up with a generic passcode but each member of staff is advised to change a personal code. ICT have found that when devices come back for repair that new codes have been created, Mobile device management software has also been put in place which allows internet filtering and control on Council issued smart phones. The software is an add-on application to the Trend anti-virus software which is designed for use with mobile devices. The application was demonstrated to Audit. It allows ICT to maintain a database of all Council issued mobile devices including phones, laptops, tablets etc. Within the database ICT officers can see if there have been any breaches of password security. Policies and procedures for staff accessing Council's e-mail from their own devices has yet to be finalised.

Recommendation	Priority Rating	Management response & deadline	Position at January 2018
			Issue being addressed As noted in earlier progress summaries the ICT Security Officer has only recently been appointed and will take up his post on 1st February 2018. It is hoped that encryption of laptops and other safety measures will be considered as part of the ICT Security Policy. **Issue not yet addressed** **Overall issue being addressed**
A process for notifying ICT of leavers should be introduced to ensure that accounts can be disabled once the individual leaves or passwords reset if accounts require to remain enabled for any reason. Consideration should be given to ICT staff signing and dating any leaver forms developed as evidence of when the accounts and Outlook Web Access were disabled.	2	Agreed. ICT must work in partnership with HR and HoS to ensure its implementation (Patrick McColgan and Brid Lofthouse 1st February 2017)	Audit was advised that ICT e-mailed a request to HR to send details of all leavers to the ICT Support e-mail. Audit was advised that the procedure for ensuring ICT is informed of all leavers has improved but is still not operating properly. Audit obtained a list of leavers for the period 1st March 2017 – 31st December 2017 and tested a sample of 6. ICT had not been formally informed of any of these leavers and Audit was advised that some of these leavers had not been deactivated on CCAG systems e.g. email **Issue not yet addressed**
Consistent approaches to server monitoring should be developed to ensure that patches and server updates are applied in a timely manner (in particular in relation to servers in Ballycastle). Server security logs should	2	The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved. (Patrick McColgan 1st February 2017)	New software was put in place in the summer of 2017 to facilitate monitoring of patches and server updates. Audit viewed the software and observed how the software provides a comprehensive database of all automatic updates and patches to servers (and other ICT equipment such as PCs). ICT

Recommendation	Priority Rating	Management response & deadline	Position at January 2018
also be reviewed periodically to identify any unusual server access or attempts to access the server			monitor ICT websites for news of problems with patches and updates, and regularly monitor (at least weekly) the progress of patches and updates, for servers, via the update monitoring software. The software will record all details regarding the patch and flag any problems encountered when a patch or update was being installed. This allows ICT to see at any given moment the status of all patches and updates and to rectify any issues in relation to server patches and/or updates. **Issue addressed**
ICT should review the recommendations from the external service provider's report with regard to the security settings for the firewall in Ballycastle (and across Council's other firewalls) to determine if these should be implemented.	2	Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.	Audit was advised that since the previous audit changes in the ICT environment mean that all Council e-mail flow through Coleraine. This means that the same firewall is used for all e-mail traffic; and the Ballycastle firewall is no longer required. The Infrastructure Manager demonstrated to Audit how internet/e-mail traffic for Ballycastle is now routed through Coleraine Audit. A trace report was generated showing how a single PC in Ballycastle (172.25.195.251) using www.google.co.uk was routed through Coleraine (172.25.0.) **Issue addressed**
ICT and Information Governance staff should review whether documented data protection protocols or confidentiality agreements are in place and required for third party contractors who access Council's networks.	3	Agreed. This will be communicated to effected HoS to ensure that their respective suppliers adhere to this direction. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved. (Patrick McColgan 1st April 2017)	Audit was advised that this will be formalised as part of the ICT Security Strategy and in preparation for GDPR. **Issue not yet addressed**
ICT should periodically review the firewall policies to ensure that they remain correctly set.	3	Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.	The firewall suppliers carry out an annual review of the firewall.

Recommendation	Priority Rating	Management response & deadline	Position at January 2018
		(Patrick McColgan 1st April 2017)	A member of the ICT team (ICT Security Officer) is due to attend training on firewall protection in the Spring of 2018. **Issue being addressed**
A documented Business Continuity and Disaster Recovery Plan should be developed for ICT to provide clear guidance on actions in the event of a business interruption or disaster. In addition, work to develop the disaster recovery site at Ballymoney should be completed as soon as practicable to ensure a smooth transition in the event of any issue affecting the main Causeway Coast & Glens Council severs in Coleraine.	1	Agreed. This will be implemented as a matter of priority. The initial scoping exercise will identify the required resources. (Patrick McColgan 1st February 2017)	Audit was advised that a lot of testing of disaster recovery processes has taken place e.g. a recent test of TOTAL found that all back-ups were replicated at another Council with no problems identified. The final testing is almost complete and the technology is now largely in place to support Business Continuity and Disaster Recovery. Audit discussed the testing of the TOTAL finance system and found that (non-documented) plans are in place to test if replicated TOTAL can perform specific processes e.g. perform creditors run in a different location; make BACS payments off-site; process payroll. A discussion with the Head of Finance revealed that Finance plan to document the process being tested and the results. No formal documented evidence has been retained of any testing to date but audit was advised that a first draft of the Business Continuity and Disaster Recovery Plan would be in place for ICT by the summer of 2018. **Issue being addressed.**

Appendix I: Hierarchy of Findings

This audit report records only the main findings. As a guide to management we have included the categories of recommendations that were applicable at the time of the prior year audits (note: these were revised in 2016 following guidance from the DFP):

Priority 1: Major issues which require urgent attention and the implementation of agreed audit recommendations in the short term.

Priority 2: Important issues which require immediate attention and the implementation of agreed audit recommendations in the short to medium term.

Priority 3: Detailed issues of a less important nature which require attention and the implementation of agreed audit recommendations in the medium to long term.

Appendix II: Our Approach and Staff Interviewed

Our audit fieldwork comprised:

- Reviewing progress against recommendations via discussions with key staff
- Examining relevant documentation
- Testing controls and accuracy of records.

The table below shows those consulted with and we would like to thank them for their assistance and co-operation.

Job title
Head of ICT
ICT Manager
ICT Officers