CARLISLE CITY COUNCIL

www.carlisle.gov.uk

Audit follow up of IT General Control

Draft Report Issued: 23 February 2018

Director Draft Issued: 23 February 2018

Final Report Issued: 02 March 2018

Audit Report Distribution

Client Lead:	ICT Services Manager
Chief Officer:	Chief Executive
Audit Committee:	The Audit Committee, which is due to be held on 19th March 2018 will receive summary findings and recommendations from this audit.

Executive Summary

1.0 Background

1.1. This report summarises the findings from a follow up audit of IT General Controls. This was an internal audit review included in the 2017/18 risk-based audit plan agreed by the Audit Committee on 16th March 2017.

1.2. The original audit was carried out by the Council's external auditors (Grant Thornton) in March 2017, resulting in 8 recommendations. A management action plan was completed detailing agreed actions, responsible manager and implementation dates to address the recommendations (**Appendix A**). This follow-up report provides an update on progress made against this action plan.

2.0 Audit Approach

Audit Objectives and Methodology

2.1 Compliance with the mandatory Public Sector Internal Audit Standards requires that internal audit activity evaluates the exposures to risks relating to the organisation's governance, operations and information systems.

2.2 Detailed findings and recommendations are reported within section 5 of this report.

2.3 The ICT Services Manager was asked to provide an update on progress made implementing the agreed actions. Internal Audit then undertook testing as necessary to confirm that actions have been fully implemented and that controls are working as intended to mitigate risk.

Audit Scope and Limitations.

2.4 The original audit was performed by Grant Thornton to provide independent assurance over management's arrangements for ensuring effective IT related internal controls are in place.

2.5 It is the responsibility of management to monitor the effectiveness of internal controls to ensure they continue to operate effectively.

2.6 There were no instances whereby the audit work undertaken was impaired by the availability of information.

3.0 Assurance Opinion

3.1 The original audit was performed by the external auditors and therefore did not include an assurance opinion in line with the definitions specified by Internal Audit. This review solely follows up progress of those recommendations made in that review. It is therefore not appropriate to include an assurance opinion for this audit.

4.0 Summary of Recommendations, Audit Findings and Report Distribution

4.1 The previous audit included 8 recommendations (See **Appendix A**) of which:

- Four agreed actions have been successfully implemented.
- Four agreed actions have been partially implemented.

4.2 The four recommendations in progress will be documented on Internal Audit's register of outstanding recommendations and reviewed again in Q3 2018/19. Progress will be reported to Audit Committee as part of the routine monitoring of the implementation of outstanding audit recommendations.

4.3 **Findings Summary:**

Good progress has been made against the action plan, with four of the recommendations now implemented. Progress has been made in implementing the four remaining recommendations. Processes have been put in place to monitor network access and activity on a regular basis and testing of application recovery has been scheduled to take place throughout 2018.

ICT Services have pro-actively provided advice and guidance over recent months and are in the process of purchasing a cyber-security training module as part of the e-learning facility. Training will be mandatory for all staff.

As part of the Budget approval process for 2018/19 ICT Services have had additional funding approved to recruit a Cybersecurity Architect and purchase additional software. This approval should ensure all outstanding recommendations are fully implemented.

Comment from the Chief Executive

I thank Internal Audit for this Review. I am pleased to see that plans are in place to fully implement the previous recommendations.

5.0 Summary of Recommendations, Audit Findings and Report Distribution

Recommendation 1 – IT Disaster Recovery

4.1.1 The original report highlighted that while an IT Disaster Recovery plan was in place, there had been no testing carried out to validate the effectiveness of recovery arrangements.

4.1.2 An ICT Disaster Recovery Management Framework was approved in January 2018. The Framework defines the type and frequency of testing to be carried out, based on the system's priority for recovery.

4.1.3 Testing of applications has been scheduled within Remedy Force (change management scheduling database) in line with the defined priorities. The first testing due to be carried out in April 2018.

4.2 Recommendation 2 – Information Security

4.2.1 The original report highlighted that new members of staff do not receive any training for information security.

4.2.2 Following approval of funding, ICT Services are in the process of procuring training modules to include on the Council's e-learning software (Skillsgate) to cover i) ICT hardware security and ii) cyber security. The modules will be mandatory for all officers to complete annually.

4.2.3 ICT Services have provided e-mail advice and guidance as and when the need arises (E.g. after recent successful cyberattacks on other local authorities).

4.3 Recommendation 3 – Privileged access to Civica

4.3.1 The original report highlighted two users with an unnecessarily high level of access. It was recommended that access levels are reviewed.

4.3.2 The Finance Officer (Systems, Controls & Development) reviewed access levels in November 2017 (though responses are overdue from some departments). The Finance Officer also receives regular leaver reports to check against Civica access.

4.4 Recommendation 4 –Inactive accounts

4.4.1 The original report highlighted that there was no process to monitor inactive network accounts.

4.4.2 The ICT Services Manager now receives a monthly report of all accounts that have been inactive for 30 days and reviews the reasons for this. Accounts no longer required are disabled.

4.5 Recommendation 5 – Network Administrator

4.5.1 The original report highlighted that a supplier user account had unnecessary system administrator access to the network. It was recommended that privileged access is restricted.

4.5.2 The ICT Services Manager now receives a monthly report of all administrator accounts and reviews whether the access is still relevant. Where not action is taken to remove/restrict access.

4.6 Recommendation 6 – Proactive Reviews of Logical Access within Active Directory

4.6.1 The original report highlighted that user accounts and associated permissions were not being formally, proactively reviewed for appropriateness. It was recommended that these were reviewed on a regular basis.

4.6.2 ICT services have embarked on a wider project to achieve and maintain PCI-DSS compliance. As part of this project the ICT Services team are looking to purchase a software product that, among other things, will perform live and continuous audits of the active directory.

4.6.3 In addition, ICT Services have had permission to recruit a Cyber-security post; the role will take a lead in this area.

4.7 Recommendation 7 – Review of Information Security Logs Created by Active Directory

4.7.1 The original audit highlighted that security activity within the Active Directory is not formally, proactively and routinely reviewed.

4.7.2 As part of the PCI-DSS compliance project (as above) ICT Services are also in the process of procuring Security Information and Event Management) software that will routinely monitor security activity and flag potential issues for further investigation (for example, if a user was logged in at two different locations at the same time).

4.7.3 The Cybersecurity Architect will also take a lead in this area.

4.8 Recommendation 8 – Change Management Policies and Procedures

4.8.1 The original audit highlighted that documented policies and procedures had not been formally established addressing change management processes and related control requirements within key applications.

4.8.2 A policy has now been drafted and ICT Services have already adopted this for application upgrades and will be rolled out for infrastructure changes from March (though the schedule has not been agreed with system owners to date).

Appendix A – Original Management Action Plan

Summary of Recommendations and agreed actions						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 1: The Council should produce a test strategy for the critical services recovery plan. Key elements of this plan should be tested at least on an annual basis to validate the effectiveness of the recovery arrangements.	N/S	There is a risk that the Council IT systems could not be restored within a reasonable timescale should a disaster affect the server room at the Civic centre. This could have a detrimental impact on the Council's ability to provide services or lead to reputational damage.	I will implement an annual test of our critical services recovery plan as recommended.	ICT Services Manager	31 October 2017	Yes
Recommendation 2: We recommend that the Council provides new members of staff with information security training. In addition, members of staff should attend some information security training on a regular basis to remind them of their responsibilities regarding data and IT assets. Evidence from training attendance should be retained.	N/S	Although users are reminded of the internet code of conduct when they log onto the network, there is a risk that users adopt inadequate information security practices when using IT assets escalated.	Currently, training is not of part Digital and Information Services remit. I will follow up this recommendation with our training unit.	ICT Services Manager	31 December 2017	In progress

Summary of Recommendations and agreed actions						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 3: We recommend reassessing the users that have full access to the live company in the Civica system. This access should only be granted to personnel that require it to fulfil their job duties.	N/A	a) Bypass of system-enforced internal control mechanisms through inappropriate use of administrative functionality by (1) making unauthorised changes to system configuration parameters, (2) creation of unauthorised accounts, (3) making unauthorised updates to their own account's privileges, or (4) deletion of audit logs or disabling logging mechanisms. b) Internal access to information assets and administrative functionality may not be restricted on the basis of legitimate business need.	**Agreed management action:** I will undertake a review of access to Civica system as recommended	ICT Services Manager	30 June 2017	Yes
Recommendation 4: The Council should implement a process to identify network accounts that have not been used for a period of time. These accounts should be investigated to confirm whether they are still required or they could be disabled	N/S	There is a risk that unnecessary network accounts could remain active. This could lead to unauthorised access to data.	As recommended, I will put in place procedures for the review of inactive user accounts.	ICT Services Manager	31 October 2017	Yes

Summary of Recommendations and agreed actions						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 5: The Council should implement a process to revalidate domain admin user accounts on a monthly basis. Privileged network access should only be granted to users that require it to fulfil their job duties	N/S	a) Bypass of system-enforced internal control mechanisms through inappropriate use of administrative functionality by (1) making unauthorised changes to system configuration parameters, (2) creation of unauthorised accounts, (3) making unauthorised updates to their own account's privileges, or (4) deletion of audit logs or disabling logging mechanisms. b) Internal access to information assets and administrative functionality may not be restricted on the basis of legitimate business need.	As recommended, I will ensure a procedure is implemented to review domain administrative privileges	ICT Services Manager	31 October 2017	Yes

Summary of Recommendations and agreed actions						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 6: It is our experience that access privileges tend to accumulate over time. As such, there is a need for management to perform periodic, formal reviews of the user accounts and permissions within Active Directory. These reviews should take place at a pre-defined, risk-based frequency (annually at a minimum) and should create an audit trail such that a third-party could determine when the reviews were performed, who was involved, and what access changed as a result. These reviews should evaluate both the necessity of existing user ID's as well as the appropriateness of user-to-group assignments (with due consideration being given to adequate segregation of duties)...	N/S	a) Gaps in user administration processes and controls may not be identified and dealt with in a timely manner. b) Access to information resources and system functionality may not be restricted on the basis of legitimate business need. c) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls. d) No-longer-needed permissions granted to end-users may lead to segregation of duties conflicts. e) Access privileges may become disproportionate with respect to end users' job duties.	As recommended, I will ensure a procedure is implemented to review of user accounts and permissions.	ICT Services Manager	31 October 2017	Yes

Summary of Recommendations and agreed actions						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 7: Given the criticality of data accessible through Active Directory, logs of information security events (i.e., login activity, unauthorised access attempts, access provisioning activity) created by these systems should be proactively, formally reviewed for the purpose of detecting inappropriate or anomalous activity. These reviews should ideally be performed by one or more knowledgeable individuals who are independent of the day-to-day use or administration of these systems.	N/S	Without formal, proactive, and routine reviews of security event logs, inappropriate and anomalous security activity (e.g., repeated invalid login attempts, activity violating information security policies) may not identified and/or addressed in a timely manner	I have evaluated a number of products and services which would provide an automated monitoring of logs and network activity as we do not have the resources to do this manually. I will be producing a reporting for consideration by the council's Senior Management Team on how we address this issue.	ICT Services Manager	31 December 2017	In Progress

Summary of Recommendations and agreed actions						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 8: Documented policies and procedures addressing change management processes and related control requirements (such as change testing, approvals, and documentation requirements) within Civica Authority Financials, Trent, and Academy should be established, formally approved by the appropriate members of the organisation, and communicated to relevant personnel responsible for implementing them and/or abiding by them	N/S	a) Change and patch management processes and control requirements may not be formalised or communicated to those within the organisation responsible for observing and/or implementing them. b) Change and patch management may not be effectively administered, leading to loss of data integrity, processing integrity and/or system down-time.	This had already been identified as an issue by the D&IS management team. A process to implement change control within the service will be developed and implemented.	ICT Services Manager	Not stated	In part