Report to Audit Committee

Agenda Item: A.5

Meeting Date:	8 July 2021
Portfolio:	Finance, Governance and Resources
Key Decision:	Not applicable
Within Policy and Budget Framework	YES
Public / Private	Public

Title:	Internal Audit Report – ICT Various Recommendations (Follow-Up)
Report of:	CORPORATE DIRECTOR FINANCE & RESOURCES
Report Number:	RD26/21

Purpose / Summary:

This report supplements the report considered on Internal Audit Progress 2020/21 and considers the follow up review of ICT Various Recommendations.

Recommendations:

The Committee is requested to

(i) receive the final audit report outlined in paragraph 1.1;

Tracking

Audit Committee:	**8 July 2021**
Scrutiny Panel:	**Not applicable**
Council:	**Not applicable**

1. BACKGROUND INFORMATION

1.1 The 2019/20 Internal Audit opinion raised concerns over ICT Services, particularly due to two partial reviews (Firewall and Mobile Devices) and resource constraints through vacant posts resulting in non-implementation of outstanding recommendations.

1.2 A follow-up audit of all outstanding ICT recommendations was undertaken by Internal Audit in line with the agreed Internal Audit plan for 2020/21. The follow-up, appended as **Appendix A** found progress had been made, with 13/38 recommendations implemented and progress made on a further 6. The report includes 16 recommendations (6 high graded). A second follow-up of all these recommendations is proposed in 2021/22.

2. RISKS

2.1 Findings from the individual audits will be used to update risk scores within the audit universe. All audit recommendations will be retained on the register of outstanding recommendations until Internal Audit is satisfied the risk exposure is being managed.

3. CONSULTATION

3.1 Not applicable

4. CONCLUSION AND REASONS FOR RECOMMENDATIONS

The Committee is asked to

i) receive the final audit report as outlined in paragraph 1.1;

5. CONTRIBUTION TO THE CARLISLE PLAN PRIORITIES

5.1 To support the Council in maintaining an effective framework regarding governance, risk management and internal control which underpins the delivery the Council's corporate priorities and helps to ensure efficient use of Council resources.

Contact Officer:	**Michael Roper**	**Ext:**	**7280**
Appendixes	**ICT Various Recommendations (Follow-up) – Appendix A**		

Note: in compliance with section 100d of the Local Government (Access to Information) Act 1985 the report has been prepared in part from the following papers:

- **None**

CORPORATE IMPLICATIONS/RISKS:

Legal – In accordance with the terms of reference of the Audit Committee, Members must consider summaries of specific internal audit reports. This report fulfils that requirement.

Finance – Contained within the report

Equality – None

Information Governance – None

CARLISLE CITY COUNCIL

www.carlisle.gov.uk

Audit follow up of ICT Services

Outstanding Recommendations

Draft Report Issued: 22 March 2021

Director Draft Issued: 07 June 2021

Final Report Issued: 23 June 2021

Audit Report Distribution

Client Lead:	Head of Digital & Technology Lead ICT Officer (T1907)
Chief Officer:	Chief Executive
Others:	Information Governance Manager Revenues & Benefits Operations Manager Workforce Development Manager
Audit Committee	The Audit Committee, which is due to be held on 8 July 2021 will receive a copy of this report.

Note: Audit reports should not be circulated wider than the above distribution without the consent of the Designated Head of Internal Audit.

1.0 Background

1.1. This report summarises the findings from a follow up audit of outstanding recommendations within ICT Services over 5 separate audits. This was an internal audit review included in the 2020/21 risk-based audit plan agreed by the Audit Committee on 30th July 2020.

1.2. The original audits were as follows:

Year	Audit Title	Assurance Level	High	Medium
2017/18	IT General Controls (Grant Thornton)	N/A	-	2
2018/19	Revenues & Benefits Shared Service	Reasonable	1	-
2018/19	Firewall (ICT Specialist Review)	Partial	11	15
2019/20	Mobile Devices (Follow-up)	Partial	2	5
2019/20	Information Security	N/A	-	2

1.3 Management actions plan were completed detailing agreed actions, responsible managers and implementation dates to address the recommendations (Appendix A)[1].. This follow-up report provides an update on progress made against these action plans.

1.4 The 2019/20 annual internal audit report raised concerns around ICT controls due to the two partial assurances and a growing number of outstanding audit recommendations, including slow progress in implementing historic recommendations.

1.5 Remaining planned ICT audit work (IT Strategy / ICT Specialist Audit) was deferred as it was agreed ICT control concerns existed and further reviews would not add more value until these concerns were addressed. It should be noted that continued development of the Council's Information Governance and Records Management is also reliant on the ICT Service

1.6 The ICT Services team had several absences and vacancies, including the long-term absence and subsequent retirement of the Head of Service. There were delays in recruiting a new Head of Service, partially due to the Covid-19 global pandemic, but the post was recruited to in November 2020.

1.7 Internal Audit recognise the hard work, knowledge and dedication of the existing service, including their considerable efforts to ensure the Council could quickly and efficiently adapt to a new way of working through the pandemic.

[1] Two of the audit reviews (IT General Controls/Revenues & Benefits Shared Service) have been followed up since the initial review – action plans reflect the latest agreed dates and actions as a result of these prior reviews

1.8 Internal Audit will continue to work closely with the team to progress implementation of outstanding recommendations and plan to work with the service to devise a new assurance programme going forward into 2021/22.

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 A risk-based audit approach has been applied which aligns to the five key audit control objectives (see section 4). Detailed findings and recommendations are reported within section 5 of this report.

2.3 The Client Lead was asked to provide an update on progress made in 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 scopes were to provide independent assurance over management's arrangements for ensuring effective governance, risk management and internal controls of the Council's ICT Service, including the confidentiality, integrity and security of the Council's electronic information (cyber-security).

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 Each audit review is given an assurance opinion intended to assist Members and Officers in their assessment of the overall governance, risk management and internal control frameworks in place. There are 4 levels of assurance opinion which may be applied (See **Appendix C** for definitions).

3.2 Where the findings of the follow up confirm that actions have been successfully implemented and controls are working effectively, the internal audit assurance opinion may be revised from that provided by the original audit.

3.3 From the areas examined and tested as part of this follow up review we consider the current controls operating within ICT provide **partial assurances**.

Note: as audit work is restricted by the areas identified in the Audit Scope and is primarily sample based, full coverage of the system and complete assurance cannot be given to an audit area.

4.0 Summary of Recommendations, Audit Findings and Report Distribution

4.1 There are two levels of audit recommendation; the definition for each level is explained in **Appendix D**.

4.2 The previous audits included a total of 38 recommendations (See Appendix A) of which:

- 13 agreed actions have been successfully implemented.
- 6 agreed actions have been partially implemented.
- 18 agreed actions have not been implemented.
- 1 agreed action is no longer relevant due to ending of contractual arrangements.

4.3 A number of the outstanding recommendations relate to similar issues, such as a need for various policies to be reviewed. Where possible, this audit has merged relevant recommendations.

4.4 Audit recommendations arising from this audit review are summarised below:

Control Objective	High	Medium
1. **Management** - achievement of the organisation's strategic objectives	1	1
2. **Regulatory** - compliance with laws, regulations, policies, procedures and contracts	-	-
3. **Information -** reliability and integrity of financial and operational information	1	2
4. **Security** - safeguarding of assets	4	6
5. **Value** – effectiveness and efficiency of operations and programmes	-	1
Total Number of Recommendations	**6**	**10**

4.5 Management response to the recommendations, including agreed actions, responsible manager and date of implementation are summarised in Appendix B.

4.6 **Findings Summary:**

Internal Audit acknowledge that progress has been made since ICT controls were last reviewed with a third of recommendations having been appropriately implemented and closed. However, given the number of recommendations not addressed and the six high graded recommendations made in this review there is still significant progress to be made to provide acceptable levels of assurances over cyber-security and other ICT related controls.

The audit reflects that the limited progress made relates to the significant number of vacancies within the ICT team, in particular the long vacancy for a Head of Service. These difficulties have been compacted by the Covid-19 global pandemic with additional pressures placed on the team, who enabled a rapid and wide-spread migration that enabled the majority of Council officers to work from home during the pandemic. This achievement by the team is acknowledged by both Internal Audit and by Senior Management within the authority.

However, now the head of service post has been filled there is a need to ensure remaining vacancies are filled to enable the team to address the outstanding points in this review. It is clear this will need to be measured against any other ICT health and security concerns raised from specialist health checks proposed for the service (see Recommendation 15), with an ongoing review of priorities versus available resource necessary.

The key issues identified from this audit are summarised as follows:

- The full suite of ICT policies needs to reviewed and updated to ensure up to date, accessible and appropriate policies are in place to ensure suitable usage by individuals accessing the Council's network.
- Plans to obtain further assurances over the health/security of the ICT network should be made, including development of existing remedial action plans to ensure actions are identified and addressed swiftly and are appropriately evidenced as complete.
- Risk management arrangements should be reviewed and updated, including identification of risks relating to Information Governance and Information Security and ensuring existing and planned mitigating actions are segregated to avoid false assurances.
- Mandatory cyber-security training should be reviewed to ensure it is up to date. There is also a need to ensure this training is undertaken by all individuals with access to the Council's network (both officers and members)
- Records management arrangements need to be reviewed to ensure all relevant information is accessible to all relevant individuals within the service.

- Data sharing arrangements are required in relation to the shared service arrangements with Allerdale and Copeland for the provision of Revenues and Benefits software. A firewall solution between Allerdale and the Council is also necessary to help ensure a secure connection is established between the two networks.
- Custodian forms should be obtained retrospectively for all device users.
- A regular VFM review of mobile phone usage should be established to ensure any devices no longer required are disposed of.
- An application locker should be obtained for use on mobile devices to prevent downloading of inappropriate software.
- Latest versions of application software should be formally tracked and applied

Prioritisation of outstanding recommendations will need to be considered against wider assurances currently being planned by ICT Services in relation to ensuring the security of the Council's network and information. Higher priority recommendations will need addressing as a matter of urgency, but a number of the medium recommendations cannot be implemented until the team is fully resourced.

Comment from the Chief Executive

I thank Internal Audit for this report. I am confident that renewed and refocussed leadership in ICT Services, couple with a commitment from me to ensure they have the resources they need will enable us to address these pressing issues for the City Council.

5.0 Audit Findings & Recommendations

5.1 Information Security Events

5.1.1 The audit of ICT General Controls recommended implementation of a formal review of security events to detect potential inappropriate or malicious activity on the Council's network. In addition, the Firewall audit recommended that both firewall alerts and key events should be defined and similarly reported and monitored.

5.1.2 In response to the General Controls recommendation, ICT Services procured a managed SIEM (Security Information and Event Management) solution in 2018. A managed service framework was considered to offer the best value for money, meaning a third party was responsible for monitoring and reporting security events on the Council's network. Responsibility for reviewing and resolving identified issues is retained by the Council.

5.1.3 Evidence was provided that relevant monitoring and reporting has been undertaken by the provider (including firewall alerts and key events). Evidence was also provided that events are registered in the Council's service management solution (Remedyforce), including actions taken by ICT officers to review and resolve the reported issues.

5.1.4 The SIEM solution was procured by the previous Head of Service. Officers have been unable to locate the relevant quotes, tender award documentation and original signed contract, raising concerns about the quality of historic records management.

5.1.5 Similar concerns have been identified elsewhere in this review in relation to document retention within ICT services, with further contract information (para 5.10.3) and training records (para 5.2.4) unavailable to the audit. It is recognised that work has started to develop a SharePoint site to improve accessibility of records to all relevant officers. In addition further plans are in place to develop the Council's use of i-Trent for storing personnel records (including training qualifications).

Recommendation 1 – The ICT service's record management structure should be reviewed to ensure officers have access to all relevant documentation, including those relating to contract/procurement and training records.

5.2 Change Management Policies & Procedures

5.2.1 The audit of ICT General Controls recommended a need to document and publish policies and procedures addressing change management processes and related control requirements.

5.2.2 A significant number of outstanding recommendations included in this review relate to the need to update procedures and this issue is addressed in section 5.5.

5.2.3 To address this recommendation it was identified that ICT staff needed to attain accreditation to ITIL (Information Technology Infrastructure Library) to enable suitable change management procedures to be produced and undertaken.

5.2.4 There is evidence on the Council's training and development application that relevant officers have undertaken the accreditation and a copy of the training material has been retained by the service. However, copies of qualification certificates have not been retained by ICT Services, or forwarded to Organisational Development for central filing, making it difficult to evidence accreditation (see section 5.1 and **recommendation 1**).

5.3 SLA/Data Sharing agreements – Shared Service

5.3.1 The audit of shared ICT software provision for Revenues and Benefits recommended that formal data processing agreements are agreed and signed between the three participants (Carlisle City Council, Allerdale Borough Council and Copeland Borough Council) to ensure compliance with data protection legislation.

5.3.2 There have been delays in implementing this recommendation as it was intended to include the data processing arrangements in a revised SLA (Service Level Agreement), which has not been developed (partly due to limited engagement with partners in the service).

5.3.3 The Information Governance Manager has proposed developing a practical law template between the parties to ensure data protection issues are covered while the Council continues to review the content of the SLA. Actions to this re-iterated recommendation have been updated to reflect this proposal (see Appendix B).

Recommendation 2 – The Data Processing Agreements should be checked to ensure compliance with GDPR and should be signed by all parties to formalise the arrangement.

5.4 Cyber Security Training

5.4.1 The audit of mobile devices recommended that the existing mandatory e-learning training for cyber security is updated, including adding sections on maintaining physical security of assets and Council-specific ICT policies.

5.4.2 The mandatory training has not been updated since it was introduced in 2018. The course is still a mandatory requirement for all new starters, with repeat sessions flagged every three years. 93% of registered officers have completed this course within the last three years.

5.4.3 There is a risk the training is out of date and does not include new relevant issues (particularly in relation to phishing attacks and other threats to cyber security) and the training still does not include anything relating to physical security of assets or Council policies.

5.4.4 In October 2020 all Council officers were asked (via a corporate communication) to undertake additional training provided by the NCSC (National Cyber Security Centre), which includes up to date information relating to phishing and other cyber-security issues. Completion of training is monitored by a declaration within Skillsgate, which is being monitored by Organisational Development. Only 25% of registered officers had completed the course as at the time of the audit,

5.4.5 It was intended to make this supplementary training mandatory as the NCSC is recognised as providing best practice guidance in relation to cyber-security guidance. Organisational Development confirmed this training is not currently registered in Skillsgate as mandatory, so no reminders were flagged with officers of managers. It is likely this has contributed towards the low completion rate. It is noted that reminders have been issued post-audit and this has seen the completion rate increase to 42%.

5.4.6 There is also a slight discrepancy between those officers registered on each training course. The audit identified eleven officers with an e-mail account (who therefore are likely to be exposed to cyber security risks at some point) that were only registered on one of the courses. It is thought this may relate to officers being allocated an e-mail account after initial mandatory courses were set-up – Organisational Development are investigating this anomaly.

5.4.7 ICT services have also undertaken a series of drop-in sessions for staff to attend providing information on security awareness.

5.4.8 The audit of mobile devices also recommended that action was taken to ensure all elected members receive appropriate cyber-security training.

5.4.9 Of the current 37 members only 22 have access to Skillsgate and have been registered to complete the course. Members were given the option to retain a Skillsgate account and the remaining 15 elected not to do so.

5.4.10 Of those 22 members registered on Skillsgate 10 (27% in total) have completed the original e-learning and 2 (5 % in total) have completed the recent NCSC training.

5.4.11 There is no mandatory requirement for Members to complete the training and no responsibility is established to ensure members are encouraged to complete the training.

5.4.12 Given Members are likely to engage in external communications, they are potentially exposed to cyber-security risks such as phishing attacks, making it vital they receive the necessary guidance and training to reduce the potential for successful attacks on the Council's network.

5.4.13 While both ICT Services and Internal Audit have indicated it would be best practice for Members to have the same training as other individuals accessing the Council network, this is not currently possible as not all Members have access to Skillsgate. Organisational Development are currently discussing provision of training to members in relation to ICT security, including provision of one to one sessions.

5.4.14 ICT services have cited recent incidents of both officers and members having had their information compromised. Conversely individuals who have undertaken the training have been found to appropriately report suspicious e-mails they have received, suggesting both the requirement for this training and how effective it can be in preventing attacks.

5.4.15 The above findings strengthen the need to ensure mandatory training is taken by all individuals with access to the Council's network and information, in order to appropriately manage the risk of the Council's network and information becoming compromised. The cost of the cyber-attack in Copeland has been reported as exceeding £2M, highlighting the impact such a risk could impose.

Recommendation 3 – Cyber-security training provided should be reviewed on a regular basis to ensure it is up to date and includes relevant issues, including physical security of Council assets and (once updated) Council policies.

Recommendation 4 – Completion of all mandatory cyber-security training should be monitored, with line managers required to follow up outstanding completion on a timely basis. This process should be supported corporately to ensure a consistent approach is adopted across the full Council.

Recommendation 5 – Provision of cyber-security training should be reviewed to ensure anomalies identified are remedied to ensure all officers with access to the Council's network are registered for all mandatory training.

Recommendation 6 - Action should be taken to ensure all Members have access to suitable cyber-security training

5.4.16 In addition to cyber-security training ICT Services provide regular corporate communications informing officers of specific cyber-security concerns as and when issues arise.

5.5 Policies

5.5.1 Several outstanding recommendations relate to updating, publication, approval and availability of various ICT policies:

- Mobile Devices (R2) - device users should confirm they have read ICT policies on an annual basis.
- Firewall (R1) - the Firewall Management Procedure should be updated to include key issues such as procurement, frequency, completion and management of independent penetration testing, conditions for and completion of internal vulnerability testing, checks including monitoring, results and action taken.
- Firewall (R2) - a change management policy should be produced.
- Firewall (R3) - all ICT Policies should be approved by Senior Management.
- Firewall (R12) - the Incident Management Policy should be reviewed to ensure it is relevant to the Council's structures and operations.
- Firewall (R17) - a firewall incident specific procedure should be documented.
- Firewall (R22) - Firewall security for the FortiGate solution should be reviewed. Management response included preparation of firewall admin account procedures as part of agreed actions.

5.5.2 The service maintains an internal web-page that includes all ICT policies, but it is acknowledged these policies are out of date and not sufficiently developed or specific to Carlisle City Council.

5.5.3 Due to the vacant Head of Service post and significant demands on the service no updates have been made to these policies. Rather than reiterate the above recommendations separately it would add greater value to condense them into one all-encompassing recommendation.

5.5.4 The Council is exploring delivery of Firewall maintenance through a managed service similar to the above-mentioned SIEM solution. This approach may impact which policies will need to be re-produced (though relevant risks will still need managing through strong contract management).

Recommendation 7 – The full suite of ICT policies should be reviewed and updated including those policies referred to in previous audit recommendations and benchmarked against best practice to ensure policies are complete. Once complete, policies should be approved by Senior Management, communicated to all officers and stored in a location accessible to all network users.

5.6 Custodian Forms

5.6.1 The audit of mobile devices recommended that custodian forms were completed by recipients of laptops and mobile phones acknowledging responsibility for the device.

5.6.2 This process has been successfully embedded for all new starters, but work is required on a retrospective exercise for users who were issued devices prior to this process being introduced.

5.6.3 ICT Services have reported issues with equipment not being returned in full (e.g. chargers or cases not returned). Completion of the custodian forms is an important control to ensure officers take responsibility for all equipment provided.

Recommendation 8 – A retrospective exercise should be undertaken to ensure individuals previously assigned mobile devices have completed a custodian form acknowledging responsibility for their allocated device

5.7 Mobile Phone Usage

5.7.1 The audit of mobile devices recommended ongoing monitoring of mobile telephone bills to ensure both appropriate usage and that devices are still required. As a result of the Covid-19 global pandemic the Council has had to procure additional mobile phones to support home working

5.7.2 Suitable information is provided by the Council's two mobile phone contractors to enable analyse of usage for individual handsets, including charges applied, data usage, call time and use of SMS messaging. There is evidence that the ICT Lead Officer carries out suitable monitoring and challenges unusual activity.

5.7.3 Due to other priorities there has not been any review of under-usage to identify devices that are potentially no longer required. While mobile phone usage is relatively low value this would be a useful exercise to undertake, particularly given the full roll-out of Microsoft Teams to all Council officers.

5.7.4 It is acknowledged that mobile phones will still be required by certain officers, but an appropriate level of challenge should be applied to reduce the Council's mobile phone bill where appropriate.

Recommendation 9 – A Value For Money review of mobile devices should be carried out annually to identify any devices no longer required by the Council.

5.8 Application Locker

5.8.1 The audit of mobile devices recommended an application locker was applied to all Council devices to prevent users from downloading irrelevant applications (where administration rights are not required).

5.8.2 A process has been put in place for mobile telephones but is yet to be implemented on Council laptops.

Recommendation 10 – The Council should obtain an application locker to prevent device users from being able to download software that does not require administration rights.

5.9 Risk Registers

5.9.1 The information security review identified the need to identify, record, assess and manage corporate risks in relation to Information Governance.

5.9.2 The Council's Information Governance Manager has been leading on the approach to this recommendation and has recently proposed an Information sub-group to help develop a combined corporate approach to risk management including preparation of a draft Corporate risk register relating to information risks. The first meeting is due in April 2021. Until the group has identified and published an appropriate risk register this recommendation remains outstanding.

Recommendation 11 – Corporate risks relating to Information Governance and Information Security should be formally identified, recorded, assessed and managed.

5.9.3 The Firewall audit recommended that planned actions and target dates in the ICT Services Risk Register are reviewed, while the information security review also identified that existing records relating to ICT risks should be revised to clearly identify and segregate current embedded controls from planned actions.

5.9.4 While there have been some updates to the register, including the addition of some new risks further development is still needed, as highlighted below:

- Further risks are required to be registered in relation to ICT's role in maintaining good information governance.
- Existing and further planned mitigating actions are still generally not segregated, increasing the risk of false assurances.
- There is a need to review mitigating actions to ensure they are fully documented and designed to appropriately manage the risk (for example, a mitigating action was identified that merely repeated the original risk with no identified controls).

5.9.5 The service has recognised the need to update the register and have arranged internal meetings to review and update it.

Recommendation 12 – The existing risk register should be reviewed and updated to ensure all relevant risks are documented and that suitable mitigating actions are in place to manage the risks within the Council's risk appetite. This should include segregation between embedded and planned mitigating controls.

5.10 Contract Management

5.10.1 The firewall audit recommended the need to formally agree operational arrangements with the external firewall providers (main and sonic), as well as ensuring contractual arrangements are established with the main firewall provider.

5.10.2 A Service Level Agreement was established to define these arrangements for the main firewall in March 2018 and is still valid. Arrangements for managing the Sonic Firewall have been migrated to the same provider, negating the need for an additional management framework/service level agreement.

5.10.3 It was not possible to obtain signed copies of contracts with providers due to the same records management issues highlighted in section 5.1. This issue has been merged with **recommendation 1**.

5.11 Firewall – Technical documentation

5.11.1 The firewall audit recommended that a change management procedure was prepared (see section 5.5) and that firewall specific testing is formally recorded, as well as any changes to Firewall rules.

5.11.2 Evidence was provided during the audit that both change management and changes to rules are now formally logged within Remedyforce and that the system can provide reports to evidence changes made.

5.11.3 The Firewall audit included two recommendations that the configuration of the FortiGuard application is documented to ensure all agreed settings are known. Evidence was provided that the external provider obtains daily back-ups of the Firewall configuration, which would enable settings to be corrected if required.

5.11.4 The Firewall audit recommended that all connected network devices should be adequately documented and subject to a periodic review. The latest network diagram was provided, which was found to be reviewed in December 2020.

5.11.5 The Firewall audit identified that work surrounding monitoring the Windows Defender Anti-Virus software should be completed. Evidence was provided that showed Defender logs are raised through the SIEM solution and that exceptions and issues are then raised in Remedyforce for remedial action by the council.

5.11.6 The Firewall audit recommended the service should ensure significant network incidents are handled as required via the agreed incident management policy and reported. Evidence was provided that outages are now reported in Remedyforce via the implemented SIEM solution.

5.11.7 The Firewall audit recommended any issues relating to installing the latest version of application software is formally tracked, with any reasons for not installing the latest version formally documented and signed off by senior management. No progress has been made against this recommendation. The original recommendation specifically referred to the FortiGuard software but has been amended to ensure a process is established to address all applications. It is anticipated that this will be appropriately addressed by the proposed managed service going forward.

Recommendation 13 – ICT should ensure the latest version of application software is formally tracked. The reasons for not installing the latest version should be formally documented and signed off by senior management.

5.11.8 The Firewall audit recommended a firewall solution should be established with the Council's network connection with Allerdale Borough Council. No progress has been made against this recommendation.

Recommendation 14 – ICT should look to implement a firewall solution between the Council and Allerdale Borough Council

5.11.9 The Firewall audit recommended security for the firewall solution should be reviewed and action taken to address the weaknesses identified. Other than the completion of a Firewall admin procedure (see section 5.5) the remaining points, such as implementing password controls have been addressed. Settings are documented in the firewall solution.

5.12 Fire Protection System

5.12.1 The firewall audit recommended that action should be taken to ensure the safety of individuals working in the computer suite by preventing the risk of exposure to harmful chemicals used to protect the Council's servers in the event of a fire.

5.12.2 A procedure has been devised to ensure safety of individuals, including introduction of a specific signing in sheet and provision of an information sheet to be read by all visitors. The process enables the system to be switched to manual mode to prevent the automatic release of the chemicals in the event of a fire.

5.13 External Testing

5.13.1 The firewall audit recommended the need to establish a framework for managing the request, completion and action identified for external testing including:

- Managing responses to reports received by highlighting responsibilities, timescales for action(s) identified by category, records to be maintained with evidence, reporting as well as long term monitoring (if applicable).
- Restricting access to reports and action(s) to ICT staff with specific responsibilities for this area.
- Ensuring summary information on outcomes and action(s) taken with reports received are issued to the Senior Management Team and Elected Members accordingly.

5.13.2 The Council receives an annual health check of its PSN network, which has resulted in a number of graded remedial actions. An action plan is in place specifying status of agreed actions, assigning responsibility and timescales for remedial actions. The Council has since passed certification, evidencing that high priority actions have now been addressed.

5.13.3 However, there are many outstanding remedial actions of lower priority to address and it has been recognised that the network reviewed by this health check only accounts for approximately 10% of the Council's ICT estate.

5.13.4 The action plan could be further developed, as the status of actions is not always clearly stated and further improvements could be made by assigning responsibility to individual officers within the Council (including managing external contractors to address their specified actions).

5.13.5 There is no formalised procedure in place to evidence actions undertaken to address identified weaknesses, meaning supporting documentation was not available to validate closed actions.

5.13.6 ICT Services have identified the need for further work to obtain assurances in relation to the security of the Council's network.

5.13.7 The Firewall audit also recommended that internal vulnerability testing should be established, including agreeing and documenting processes and implementing action plans to address identified weaknesses

Recommendation 15 – The Council should formalise plans for future assurances (internal and external) to be obtained for security of the network.

Recommendation 16 – The format of remedial action plans should be reviewed to ensure the status and further action are concisely and clearly documented and that responsibility for each action is assigned to specified officers, as well as ensuring evidence is documented to show actions can be formally closed.

Appendix A – Original Management Action Plans

Summary of Recommendations and agreed actions (IT General Controls)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
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	Funding for an ICT Security Specialist and an Active Directory auditing tools, SteathBits was included in the 2018/19 ICT Services' budget. The ICT Security Specialist post has been job evaluated based on a new job description. I intend to advertise the post in January 2019. The current issues with recruiting ICT talent for an existing post, has required me to investigation options for making the post more attractive to potential applications, such as adding a market factor supplement and relocation packaged; funding for these needs to be identified. I am also looking at the possibility of converting the post into an apprenticeship. The procurement process for the Stealthbits software will start in December, it anticipated that the software will start monitoring our Active Directory infrastructure in April 2019.	ICT Services Manager	31 December 2017	Yes

Summary of Recommendations and agreed actions (IT General Controls)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
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.	Following an review of change management methodologies and consultation with my senior managers, I have decide to adopt the Information Technology Infrastructure Library (ITIL) Service Management best practice processes throughout ICT Services. The development of an ITIL implementation plan will be completed by the end of December and implementation will begin in January. Change management and incident management will be the first ITIL processes implemented.	ICT Services Manager	Not stated	In part. See Appendix B recs 1 and 7

Summary of Recommendations and agreed actions (Revenues and Benefits Shared Service)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 3 – The Data Sharing Agreements should be checked to ensure compliance with GDPR and should be signed by all parties to formalise the arrangement.	H	Failure to comply with legislation	Sharing Agreement to be check for GDPR compliance and then signed by all parties.	ICT Service Manager	31st July 2019	No. See Appendix B Rec 2

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 1 - The Firewall Management Procedure (policy) should be reviewed to include other key issues e.g. procurement, frequency, completion and management of independent penetration testing review, conditions for and completion of internal vulnerability testing / checks including monitoring, results and action(s) taken.	M	Corporate framework not agreed / followed. Roles and responsibilities not documented.	Update Policies and implement regular reviews around policies, external penetration testing (including remedial actions). Create a centralised log of reviews taking place and actions taken. Create Centralised Calendar for reviews with dates and times accordingly	ICT Services Manager	1 May 2019	No See Appendix B Rec 7
Recommendation 2 - A Change Management policy should be drafted.	M	Corporate approach not agreed / formalised. Roles and responsibilities not documented. Potential for service or system failure if errors introduced.	Update change management policy with a specific policy for firewalls	ICT Services Manager	1 May 2019	No See Appendix B Rec 7
Recommendation 3 - Key ICT policies should be approved by Executive Management and / or Elected Members.	M	Lack of Executive / Elected Member support for key policies affecting use of ICT services.	Seek approval of key policies Executive Management and / or Elected Members	ICT Services Manager	1st May 2019	No See Appendix B Rec 7

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 4 - Review the action(s) planned and the target dates in the ICT Services Risk Register.	M	Actions not appropriate. Dates not applicable or missed.	Carry out regular reviews of the Corporate ICT risk register and send updates to policy & performance who update this.	ICT Services Manager	31 March 2019	No See Appendix B R12
Recommendation 5 - ICT should formally agreed and document operational arrangements with the external supplier (TNP).	H	There is potential key work not undertaken due to misunderstandings of tasks to be completed and responsibilities. Exposure to external threats could be more probable as a result of tasks not being completed.	Speak to TNP and get a written statement of understanding/SLA around support	ICT Lead Officer (Infrastructure)	31 March 2019	Yes
Recommendation 6 - ICT management should ensure an appropriate management framework is established to oversee operations and management of the Sonicwall firewall.	H	There is potential key tasks are not being undertaken by the third party supplier leaving the Council's IT services, systems and data exposed to external threats.	Speak to Elitetele and get a written statement of understanding around support	ICT Lead Officer (Infrastructure)	31 March 2019	No longer relevant

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 7 - Change management procedures should be drafted, approved and implemented. Firewall specific testing should be formally recorded and attached to the Service Desk (Remedyforce) application records.	H	Changes are not undertaken consistently with the potential for unrecorded changes leading to service / system failures because errors are introduced.	Formalise change management procedures for the firewall including roles and responsibilities. Rule checking and testing should be documented and formalised. Formalise rule testing as part of change management	ICT Lead Officer (Infrastructure)	1 May 2019	In part See Appendix B R7
Recommendation 8 - Day-to-day management tasks should be documented and diarised accordingly. In addition to this ICT management should ensure others members of ICT undertake tasks on a rotational basis to aid familiarity.	M	Tasks not identified and therefore not completed as expected. Other staff unable to undertake tasks(s) in the event of the prime individual unavailable.	Update/document all firewall management tasks. Firewall changes to be checked by a 2nd officer once done and signed off in the change management call in Remedyforce	ICT Lead Officer (Infrastructure)	1 May 2019	Yes
Recommendation 9 - ICT should ensure the configuration of the Fortiguard (firewall) application is documented. This documentation would in the event of a need to re-install software ensure all agreed settings are known.	M	Full restore / recovery may not be possible in the event of hardware / software failure.	Document the firewall configuration e.g. ports used connectivity etc and show changed from default config.	ICT Lead Officer (Infrastructure)	1st June 2019	Yes

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 10 - ICT should ensure all connected network devices are documented and subject to a periodic evidenced review.	M	All network devices not known. Devices may not be updated as required.	Document all network devices and configuration for them.	ICT Lead Officer (Infrastructure)	30 September 2019	Yes
Recommendation 11 - ICT should complete the work surrounding monitoring the Windows Defender Anti-Virus software as soon as possible and establish processes for managing any exceptions identified.	M	Errors / failures not reported and addressed.	Continue to deploy Windows Defender ATP on devices and enhance configuration	ICT Lead Officer (Infrastructure)	30 September 2019	Yes
Recommendation 12 - ICT Management review the Incident Management Procedure (Policy) ensuring it relates to the Council's structures and operations.	M	Does not cover all expected issues. Does not link to Council's structure / organisation.	Incident management policy to be reviewed and ensure reporting structure is accurate	ICT Lead Officer (Service Support)	1 May 2019	No See Appendix B Rec 7

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 13 - ICT Management should take steps to put in place a contract for the services provided by TNP.	H	The absence of a contract is in breach of the Council's Standing Orders and makes it difficult to seek legal redress should there be problems with service delivery.	Speak to TNP and Elitetele around a formal contract for support. Support agreement is in place and evidenced but is around support hours etc.	ICT Lead Officer (Infrastructure)	31 March 2019	No See Appendix B R1

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 14 - ICT Management should take urgent action to address leaving the automatic fire protection system in automatic mode when individuals / external suppliers are working in the computer suite unattended. In addition to this logs should be established for access / work completed in the computer suite. On a periodical basis this should be reviewed by management to confirm it is completed and adhered to by all staff and third parties. Finally, server cabinets should be made secure.	M	A health and safety risk exists that staff / external suppliers are exposed to the system activating while they are in the computer suite.	Implement sign in system for external contractors explaining the use of FM200 in the datacentre. Refresh training for ICT staff on FM200 system. Ensure where there is a risk of accidental system activation that it is put into manual during the work period and activated afterwards Computer room is in a secure fob area with CCTV. Cabinet doors won't fit due to newer fibre patch leads more rigid than the older ones. Adjusting door hinges so door will fit and if not possible will look at moving firewall to a different cabinet with lockable door at next refresh in Summer 2019. Implement sign-in system for external contractors. Additional IT only fob on build room/computer room door. Signage on all doors and procedures that no-one can enter without being escorted by ICT Services and approval	ICT Lead Officer (Infrastructure)	31 March 2019	Yes

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 15 - ICT Management should establish a framework for managing the request, completion and action(s) identified for external testing completed. Specifically the following should be addressed: 1) Managing reports received highlighting responsibilities, timescales for action(s) identified by category, records to be maintained with evidence, reporting as well as long term monitoring (if applicable). 2) Restricting access to reports and action(s) to ICT staff with specific responsibilities for this area. 3) Ensuring summary information on outcomes and action(s) taken with reports received are issued to the Senior Management Team and Elected Members accordingly.	H	Failure to act as required or consistently could expose the Council's IT services, systems and data to risk from external threats. Key action(s) may not be taken leading to an increased threat. Executive management / Elected Members are not made aware of key risks or action (s) taken. Lack of accountability and governance.	Document the management procedure for external ICT Health check reports / Review and update Remedial actions plans from ICT health check / Folder on K Drive now locked down to specific individuals who need access - ICT Management & infrastructure only. This will be carried forward when moved to SharePoint as it contains Penetration testing reports etc which are security sensitive. / Use Remedyforce for all change management/incidents relating to firewalls and reference this when producing management reports / Implement a governance framework for reporting outcomes and remedial action plans of external testing with SMT	ICT Lead Officer (Infrastructure)	1 May 2019	In Part See Appendix B R15&16

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 16 - ICT Management should ensure significant network incidents are handled as required via the agreed incident management policy and reported.	H	Failure to manage significant / critical incidents appropriately and take action as expected. Senior Management unaware of outcomes, actions and reasons. Lack of good governance and accountability for action(s).	Network core issue in November wasn't raised retrospectively in Remedyforce. Senior management were kept informed and staff were updated accordingly. All incidents will be documented.	ICT Lead Officer (Infrastructure)	1 May 2019	Yes
Recommendation 17 - Management should develop firewall incident specific procedures for such events with first steps clearly documented.	H	Action to stop an incident or escalating not taken. Loss of ICT Services / Systems / Data. Potential breach of Data Protection legislation which could lead to financial penalties and public embarrassment.	Create an incident management process for firewall incidents specifically and ensure staff are aware	ICT Lead Officer (Service Support)	1 May 2019	No See Appendix B Rec 7

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 18 - ICT should ensure the issue relating to installing the latest Fortiguard (firewall) application software is formally tracked. The reasons for not installing the latest version should be formally documented and signed off by senior management.	M	Latest version not installed New / revised functionality not available.	Review console in infrastructure meetings based on FortiGate release schedule. Remedyforce regular task and liaise with TNP over suitable software versions so they are installed promptly / Current version is minor release and TNP advised against it as they had seen issues in their testing and at other clients. /Reviews and reasons need documented in Remedyforce	ICT Lead Officer (Infrastructure)	31 March 2019	No See Appendix B R18
Recommendation 19 - Steps should be taken to ensure the backup process for the Fortiguard (firewall) application is formalised with a copy stored outside of the Fortiguard environment.	M	Full restore / recovery may not be possible in the event hardware / software failure.	Take weekly off-device firewall backups through the console and seek advice from TNP whether this can be automated. Backups are created automatically on the devices but are then not stored off-device. Create a Remedyforce regular task and document procedure.	ICT Lead Officer (Infrastructure)	1 May 2019	Yes

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 20 - ICT should look to deploy a solution relating to the management of network devices and logs produced as soon as possible. A suitable management framework should be in place to report on alerts accordingly.	M	Inability to report on devices in the event of problems. Action not taken regarding significant / key events as alerts not defined which could lead to problems or failures. Management / audit logs of key activity not available for management review or in the event of a problem.	SIEM solution currently being evaluated for central log management/alerting	ICT Services Manager	1 July 2019	Yes
Recommendation 21 - ICT should look to implement a firewall solution between the Council and Allerdale Borough Council.	M	ICT Services, Systems and Data are potentially exposed to external threats. Loss of Council Services / Systems / Data should a breach occur at the partner site and spread to the Council's site. Potential breach of Data Protection legislation which could lead to financial penalties and public embarrassment.	Investigate enabling the ASA's firewall functions on both Allerdale and Carlisle devices already in place, beyond the current IP address limiting functions to control traffic. Need agreement from Allerdale BC and steer on R&BS shared service as this may impact service and replication speeds.	ICT Lead Officer (Infrastructure)	1 September 2019	No See Appendix B R14

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 22 - Firewall security for the FortiGate solution should be reviewed and action taken to address the weaknesses identified.	H	Breach of agreed policy. The potential exists of unauthorised access to the firewall processes. Management unable to review work / tasks completed on the firewall solution.	Implement password changes on all firewalls every 3-6 months and document when they have taken place. Use remedy force regular tasks to ensure regular changes take place / Implement password complexity settings available in firewall /Implement idle time out override to 30 mins / Speak to TNP and get a written statement of understanding around support / Carry out regular reviews of firewall admin accounts and document reviews - Use Remedyforce regular tasks and review same time as password changes / Implement management audit log reporting/alerting via SMTP to Remedyforce / Update procedures for firewall admin account approval - must be signed off by head of ICT Services	ICT Lead Officer (Infrastructure)	1 May 2019	No See Appendix B Rec 7

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 23 - Firewall rule management for the FortiGate solution should be reviewed and action taken to address the weaknesses identified.	H	Rules may exist which undermine the protection of ICT services and systems. / Existing rules may potentially be invalid and therefore increase threats. / ICT staff are not fully aware of the reasons for rules leading to confusion / misunderstandings.	Update descriptions on all rules and review external supplier rules on a regular basis using Remedyforce tasks / Rule rationalisation exercise need to be completed./Update descriptions on all rules as part of rule rationalisation project. / Create a central review repository that is updated when regular reviews take place use Remedyforce regular tasks baseline against last set number of rules. / Document all rules and carry out 6 monthly review to confirm additions/deletions. All changes must go through Remedyforce change control.	ICT Lead Officer (Infrastructure)	31 March 2019	Yes
Recommendation 24 - Alerts should be defined for the FortiGate firewall for any key failures / events. In addition to this ICT Management should consider using visual displays in the main ICT office to alert staff of any key failures / events on the firewall.	H	Action not taken regarding significant / key events as alerts not defined which could lead to problems or failures. / Potential loss of ICT Services, Systems and Data. / Potential breach of Data Protection legislation which could lead to financial penalties and public embarrassment.	Implement SMTP alerts for Critical and High alerts to come to Infrastructure and automatically into Remedyforce for assignment/investigation. Look at an Alert display in the ICT office with the SIEM solution to show alerts.	ICT Lead Officer (Infrastructure)	30 September 2019	Yes

Summary of Recommendations and agreed actions (Firewall – ICT Specialist Review)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 25 - Internal vulnerability testing should be established urgently. ICT Management should agree and document the processes and management framework for undertaking internal vulnerability testing, storing and recoding and remedial action(s) as well as securing outputs and evidence.	H	Vulnerabilities are not detected after any changes made to ICT infrastructure / network leading to exposure to external threat. / Potential loss of ICT Services, Systems and Data. Potential breach of Data Protection legislation which could lead to financial penalties and public embarrassment.	Framework to be designed and signed off by SMT / Security folder on K Drive now locked down to specific individuals who need access - ICT Management & infrastructure only. This will be carried forward when moved to SharePoint as it contains Penetration testing reports etc which are security sensitive. Any remedial actions plans need referenced back to Remedyforce.	ICT Services Manager / ICT Lead Officer (Infrastructure)	30 September 2019	No See Appendix B R15
Recommendation 26 - Steps should be taken to review the storage of log information for the Fortianalyzer solution and alerting should be established for significant / key events.	M	Action not taken regarding significant / key events as alerts not defined which could lead to problems or failures. / Storage could be exceeded resulting in loss of key log data.	Check current retention schedules. Speak to TNP to see if auto-archiving can be implemented / Implement SMTP alerts for Critical and High alerts to come to Infrastructure and automatically into Remedyforce for assignment/investigation.	ICT Lead Officer (Infrastructure)	1 June 2019	Yes

Summary of Recommendations and agreed actions (Mobile Devices)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 1 – The mandatory cyber-security e-learning module should be updated to include latest issues/trends relating to cyber security and enhanced to cover both the physical security of assets and the Council's ICT policies	H	Cyber breaches / loss of equipment due to failure to adhere to Council Policy	The Skillgate training module will be updated regularly and mandatory for staff to re-take once refreshed. With members we will highlight key areas during their migration to Windows 10 on an individual basis and then provide a briefing prior to full Council on cyber security, physical security and council assets	ICT Services Manager	April 2020	No See Appendix B Rec 4-6
Recommendation 2- All device users (Officers and Members) should confirm they have read key ICT policies on an annual basis.	M	Cyber breaches / loss of equipment due to failure to adhere to Council Policy	A Skillgate module will be created to use the ICT Policy website and test users on key parts of the policies. This will be mandatory for new starters as part of their induction process and all staff annually. With Members we will work with Legal Services to ensure councillors confirm they have read these policies during the induction/re-election process	ICT Services Manager	April 2020	No See Appendix B Rec 7
Recommendation 3 – An exercise should be undertaken to ensure all individuals assigned mobile devices have completed a custodian form acknowledging responsibility for their allocated device.	M	Users do not take responsibility for mobile devices.	Work underway to retrospectively sign custodian forms for users issued with equipment before the policies were implemented. Custodian forms obtained for all users receiving equipment after policies implemented	ICT Lead Officer (Support)	December 2019	In-part See Appendix B R8

Summary of Recommendations and agreed actions (Mobile Devices)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
Recommendation 4 – Action should be taken to ensure all Members have access to suitable cyber-security training	H	Cyber breaches / loss of equipment due to failure to adhere to Council Policy	With Members we will highlight the key areas during their migration to Windows 10 (commencing October 2019) on an individual basis and then have a briefing prior to full Council on cyber security, physical security and council assets at a suitable meeting	ICT Services Manager	April 2020	No See Appendix B Rec 6
Recommendation 5 – The Council should obtain an application locker to prevent device users from being able to download software that does not require administration rights.	M	Cyber breaches due to unsafe software installed on mobile devices.	Application lockdown policies for Microsoft in-tune will be tested with the new version of Windows 10 (1809/1909) - to be deployed to the Council's devices in Q1 2020 – for compatibility. If not suitable, Application lockdown within Windows 10 will be enabled through group policies on the network to restrict software being installed where admin privileges are not required e.g. browsers	ICT Lead Officer (Infrastructure)	May 2020	No See Appendix B R 10
Recommendation 6 – There should be a regular ongoing review of mobile phone usage to ensure devices are still required.	M	Unused devices not identified resulting in poor value for money (as contract could be reallocated / cancelled) Misuse of mobile phones not detected.	Working with current contract supplier (Social Telecoms) to have them review mobile phone usage for misuse and identify unused devices on a monthly basis	ICT Lead Officer (Infrastructure)	December 2019	In part See Appendix B R9

Summary of Recommendations and agreed actions (Information Security)						
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**	**Actioned**
R1. - A joint ICT and Information Governance document detailing planned and ongoing action to implement Information Security improvements should be created and managed.	Medium	Required improvement actions are not adequately recorded and managed resulting in reduced efficiency and inability to achieve the desired outcome.	A joint ICT and Information Governance Action Plan detailing planned and ongoing action to implement Information Security improvements will be created and managed.	Lead ICT Officer Infrastructure Management/ Information Governance Manager	31 August 2020	In part See Appendix B R11
R3. – Corporate risks relating to Information Governance and Information Security should be formally identified, recorded, assessed and managed.	Medium	Exposure to unidentified/uncontrolled risks.	A review of existing risks and identification of other potential risks will be undertaken to ensure the Council's risk exposure is accurate and up to date.	ICT Lead Officer Infrastructure/ Information Governance Manager	31 August 2020	No See Appendix B R12
R4. - Existing records relating to ICT risks, both Corporate and Operational should be reviewed/revised to clearly identify and segregate current embedded controls from planned actions.	Medium	Current records have the potential to provide false assurance risks are adequately controlled.	Existing records relating to ICT risks will be reviewed/ revised to clearly identify and segregate current embedded controls from planned actions.	ICT Lead Officer Programme and Project Management	31 July 2020	No See Appendix B R12

Appendix B – Management Action Plan

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 1 – The ICT service's record management structure should be reviewed to ensure officers have access to all relevant documentation, including those relating to contract/procurement and training records	M	Inability to refer to appropriate contractual documentation / inability to demonstrate VFM / inability to evidence accreditation / breach of data protection legislation / loss and breach of council documentation.	All contracts and procurement are now recorded in an ICT contracts register and are being reviewed as part of the 2-5 year plan for the service	Head of Digital and Technology	30 July 2021
Recommendation 2 – The Data Sharing Agreements should be checked to ensure compliance with GDPR and should be signed by all parties to formalise the arrangement.	H	Failure to comply with legislation / Legal complications in the event of contractual dispute.	Information Governance Manager pursuing data protection agreements between all parties.	Information Governance Manager	30 August 2021
			There has been a delay on progressing due to limited engagement with partnership organisations. Progress anticipated at start of 2021/22. Once an Options Appraisal is available, the team will consider overall implications for the Partnership and obtain signed agreements where required.	Revenues and Benefits Operation Manager	31 December 2021
Recommendation 3 – Cyber-security training provided should be reviewed on a regular basis to ensure it is up to date and includes relevant issues, including physical security of Council assets and (once updated) Council policies.	H	Successful cyber-attack on council's network as a result of preventable lack of awareness.	Currently identified updated NCSC cyber awareness training course and working with OD to implement through Skillgate. Working with OD to update other guidance documentation for staff so that OD can deliver through Skillgate	Workforce Development Manager & ICT Management team	30 August 2021

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 4 – Completion of all mandatory cyber-security training should be monitored, with line managers required to follow up outstanding completion on a timely basis. This process should be supported corporately to ensure a consistent approach is adopted across the full Council	H	Successful cyber-attack on council's network as a result of preventable lack of awareness.	OD team to monitor Skillgate courses and follow up non compliance with SMT. Reminders to be issued for non completion. In addition OD will record development sessions and email with read receipt and provide one to one support as part of the OD development support to I.T	Workforce Development Manager	30 August 2021
Recommendation 5 – Provision of cyber-security training should be reviewed to ensure anomalies identified are remedied to ensure all officers with access to the Council's network are registered for all mandatory training	M	Successful cyber-attack on council's network as a result of preventable lack of awareness.	Organisation Development to investigate anomalies identified by the audit and report back findings.	Workforce Development Manager.	30 August 2021
Recommendation 6 - Action should be taken to ensure all Members have access to suitable cyber-security training	H	Successful cyber-attack on council's network as a result of preventable lack of awareness.	Development session courses to be devised and e-mailed to all Members including ICT security (with read receipt to ensure all Members have received updates). One to one sessions with Members also to be developed.	Workforce Development Manager.	30 August 2021

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 7 – The full suite of ICT policies should be reviewed and updated including those policies referred to in previous audit recommendations and benchmarked against best practice to ensure policies are complete. Once complete policies should be approved by Senior Management, communicated to all officers and stored in a location accessible to all network users.	H	Lack of guidance for network users increasing risk of error, misuse, successful cyber-attacks and viruses.	Currently working on updated ICT Policy and Data backup policies that will be presented to SMT for adoption	Head of Digital and Technology	31 October 2021
Recommendation 8 - A retrospective exercise should be undertaken to ensure individuals previously assigned mobile devices have completed a custodian form acknowledging responsibility for their allocated device	M	Users do not understand responsibility for their assigned devices.	Undertaking an internal review of devices that need a signed custodian form	ICT Helpdesk Manager	30 September 2021
Recommendation 9 – A Value For Money review of mobile devices should be carried out annually to identify any devices no longer required by the Council.	M	Council spending money on devices not required.	ICT will look to produce annual management reports on devices no longer used or under utilised through suppliers so that Managers can decide whether to continue with provision of that device (This has been delayed due to global pandemic causing uncertainty over device usage)	ICT Helpdesk Manager	30 November 2021

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 10 – The Council should obtain an application locker to prevent device users from being able to download software that does not require administration rights.	M	Breaches due to malicious software installed on Council devices.	Windows 10 Applocker will be implemented during the Version upgrade of Windows 10 planned this year. Delayed from last year due to Covid	Infrastructure Manager	December 2021
Recommendation 11 – Corporate risks relating to Information Governance and Information Security should be formally identified, recorded, assessed and managed.	M	Exposure to unidentified risks / uncontrolled risks.	Risk register to be regularly reviewed as per the corporate timetable. To be considered further by the Information Governance Assurance Group.	Information Governance Manager	30 August 2021
Recommendation 12 – The existing risk register should be reviewed and updated to ensure all relevant risks are documented and that suitable mitigating actions are in place to manage the risks within the Council's risk appetite. This should include segregation between embedded and planned mitigating controls	M	Failure to appropriately identify, review, mitigate and monitor relevant risks.	Risk register to be regularly reviewed as per the corporate timetable Ongoing updates of risk register done to corporate timetable	Head of Digital and Technology	30 August 2021
Recommendation 13 – ICT should ensure the latest version of application software is formally tracked. The reasons for not installing the latest version should be formally documented and signed off by senior management.	M	Latest version not installed, resulting in potential usage issues and increased risk of successful cyber attacks.	Working with new provider who will manage and install updates to the Network and firewall environment on a quarterly basis as per manufacturer recommendation	Infrastructure Manager	30 August 2021

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 14 – ICT should look to implement a firewall solution between the Council and Allerdale Borough Council	M	ICT Services, Systems and Data are potentially exposed to external threats. Loss of Council Services / Systems / Data should a breach occur at the partner site and spread to the Council's site. Potential breach of Data Protection legislation which could lead to financial penalties and public embarrassment	Working with new provider who will manage the network to implement firewall security between Carlisle and Allerdale	Infrastructure Manager	30 September 2021
Recommendation 15 – The Council should formalise plans for future assurances (internal and external) to be obtained for security of the network	H	Security issues unidentified and unresolved.	Long term plan is full testing of the IT Estate and currently working with the LGA on a pilot testing scheme for councils. Any issues identified as Critical or High are dealt with appropriately and all issues are recorded in an action plan. This plan will be made available to senior management, audit and data protection manager. Engagement of external providers for security monitoring is in place to provide further assurance	Head of Digital and technology	31 December 2021

Recommendation 16 – The format of remedial action plans should be reviewed to ensure the status and further action are concisely and clearly documented and that responsibility for each action is assigned to specified officers, as well as ensuring evidence is documented to show actions can be formally closed.	M	Failure to resolve identified security issues.	Detailed actions plans are already in place as part of the process related to IT Healthchecks. Format to be reviewed as plans are progressed.	Head of Digital and Technology	30 August 2021.

Appendix C - Audit Assurance Opinions

There are four levels of assurance used; these are defined as follows:

	Definition:	Rating Reason
Substantial	There is a sound system of internal control designed to achieve the system objectives and this minimises risk.	The control framework tested are suitable and complete are being consistently applied. Recommendations made relate to minor improvements or tightening of embedded control frameworks.
Reasonable	There is a reasonable system of internal control in place which should ensure system objectives are generally achieved. Some issues have been raised that may result in a degree of unacceptable risk exposure.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently embedded. Any high graded recommendations would only relate to a limited aspect of the control framework.
Partial	The system of internal control designed to achieve the system objectives is not sufficient. Some areas are satisfactory but there are an unacceptable number of weaknesses that have been identified. The level of non-compliance and / or weaknesses in the system of internal control puts achievement of system objectives at risk.	There is an unsatisfactory level of internal control in place. Controls are not being operated effectively and consistently; this is likely to be evidenced by a significant level of error being identified. High graded recommendations have been made that cover wide ranging aspects of the control environment.
Limited / None	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	Significant non-existence or non-compliance with basic controls which leaves the system open to error and/or abuse. Control is generally weak/does not exist.

Appendix D

Grading of Audit Recommendations

Audit recommendations are graded in terms of their priority and risk exposure if the issue identified was to remain unaddressed. There are two levels of audit recommendations used; high and medium, the definitions of which are explained below.

	Definition:
High	Significant risk exposure identified arising from a fundamental weakness in the system of internal control
Medium	Some risk exposure identified from a weakness in the system of internal control

The implementation of agreed actions to Audit recommendations will be followed up at a later date (usually 6 months after the issue of the report).