Causeway Coast & Glens Borough Council

Internal Audit Report
ICT Environment

November 2016

Final v2

INTERNAL AUDIT REPORT

ICT Environment

Executive Summary

This internal audit was completed in accordance with the approved annual Internal Audit Plan for 2016/17. This report summarises the findings arising from a review of the Council's ICT Environment.

We recognise that integration of ICT systems has been a significant undertaking for the Council and the ICT team. The work has involved taking systems of differing standards, age and specification with the intention of developing a robust ICT infrastructure that meets the needs of staff and the organisation as a whole. The first year priorities of integrated email, telephony, finance/payroll systems and common web access have been implemented and work is now focusing on the next stage of ICT development (security, infrastructure and GIS).

Through our audit we found the following examples of good practice:

- A plan has been identified for the direction of travel for ICT services within the Council and a new ICT staffing structure has been agreed by Council to drive this plan
- There is a process of back-up for the servers in place across the 4 main Council sites
- Access controls are enforced through the password policies set within the domain controller
- New software is tested by ICT to ensure it is robust before it is rolled out across the Council
- Uninterruptible Power Supplies are in place to ensure no immediate loss of data in the event of a power failure at the 4 main Council sites

Some areas where controls could be enhanced were noted during our review:

Priority 1

- There are no documented business continuity or disaster recovery plans and no formal testing of business continuity/disaster recovery arrangements for ICT has been implemented. Disaster recovery currently relies on back-up arrangements, although it is planned that Ballymoney office will become the ICT disaster recovery site.

Priority 2

- A number of ICT Policies and Procedures and a Social Media policy have been prepared but are currently still in draft format. From our review, the draft policies and procedures appear comprehensive and will provide clear guidance to staff but require to be formalised and communicated to staff.

- The Mobile Phone Policy states that any phone (Council-owned or personal) that has access to Council email will have a pin code and remote wipe automatically enforced. To date, ICT have enabled the remote wipe but not the enforced pin code for smartphones. Further, no laptops have been encrypted within the Council. There is therefore a risk of unauthorised access to Council information if a phone or laptop is lost or stolen.
- There is no formal process for notification of leavers to ICT. We found from our testing 3 user accounts that were still enabled where Heads of Service identified that the individuals had left the Council.
- Patch and server updates for Ballycastle are carried out annually however through an external service provider annual review (continuing historical arrangement). We found that the servers tested had all been updated recently and were last updated in May 2016 for Ballycastle. There is a risk however that annual server updates may not be frequent enough to ensure that vulnerabilities in server systems are addressed in a timely manner. We were also advised that server security logs are not generally monitored to identify any unusual access or attempts to access the servers.
- Under a long-standing arrangement, an external service provider completed an annual review of the servers and firewall in Ballycastle in May 2016. The report from the service provider noted that firewall security settings that it would normally recommend to clients were not implemented on the firewall in Ballycastle. We were advised that this has not been followed up to identify where any weaknesses in the security may be.

The following table summarises the total number of findings/recommendations from our audit:

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

Based on our audit testing we are able to provide the following overall level of assurance:

Limited	There are significant weaknesses within the governance, risk management and control framework which, if not addressed, could lead to the system objectives not being achieved

Points for the attention of Management

In addition to the recommendations noted above we have identified a number of system enhancements during the course of the audit which do not form part of our formal findings, but may help enhance the existing controls. These are detailed at Appendix III.

Table of Contents

Executive Summary 2
1 Objective 6
2 Background 6
3 Risks 6
4 Audit Approach 6
5 Findings and Recommendations 7
5.1 Risk 1 – ICT Governance 7
5.2 Risk 2 – Access Controls 11
5.3 Risk 3 – Back-Ups 15
5.4 Risk 4 – Business Continuity & Disaster Recovery 15
Appendix I: Definition of Assurance Ratings and Hierarchy of Findings 16
Appendix II: Summary of Key Controls Reviewed 17
Appendix III: Points for the Attention of Management 19

Auditor:	Camille McDermott / Steven Lindsay
Distribution:	Chief Executive Director of Performance Head of Performance Head of ICT Audit Committee
	November 2016

Audit progress	Date
Audit commenced	14 September 2016
Draft Report issued to senior management for response	29 September 2016
Responses Received	16 & 23 November 2016
Responses Agreed	23 November 2016
Report Issued	24 November 2016

All matters contained in this report came to our attention while conducting normal internal audit work. Whilst we are able to provide an overall level of assurance based on our audit work, unlike a special investigation, this work will not necessarily reveal every issue that may exist in the Council's internal control system.

1 Objective

The areas for inclusion in the scope of the audit were determined through discussion with the Head of ICT. The scope of this audit was to review the arrangements in place within the Council in relation to the ICT Environment, focusing on the main risks associated with:

- ICT Governance
- Security and back-up
- Contingency and recovery.

2 Background

Information Communication Technology (ICT) provides the platform for effective delivery of many of the core functions of the Council. Appropriate and effective controls are important to ensuring that the operating and security arrangements of IT systems (and data held on the systems) are functioning effectively. Appropriate security levels should also be applied to ensure the integrity and confidentiality of information held.

3 Risks

The risks identified by Internal Audit relating to the ICT Environment and agreed with management are as follows:

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

4 Audit Approach

Our audit fieldwork comprised:

- Documenting the systems via discussions with key staff
- Consideration of the key risks within each audit area

- Examining relevant documentation
- Testing the key arrangements and controls
- Testing the completeness and accuracy of records.

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

Job title
Head of ICT
ICT Officers
ICT Contractor (Ballycastle)
Head of Finance
Head of Policy, Organisational Development and HR
Head of Performance
Head of Health and Built Environment
Finance Officer

5 Findings and Recommendations

This section of the report sets out our findings in relation to control issues identified and recommendations. A summary of all the key controls that we considered is included in Appendix II to this report.

5.1 Risk 1 – ICT Governance

Recommendation 1 – *ICT Strategy*
a) **Observation**- The focus in the first year of Council has been to deliver on the ICT workstreams identified during transition (concentrating on the priority areas of telephony, email, new website and finance systems), with the majority of workstreams largely achieved. Plans were presented to and approved by the Corporate Policy and Resources Committee in June 2016 setting out the current risks around ICT, review of the approach to date, SWOT analysis of ICT, long-term goals for ICT, benefits to Council from these priorities and the first step to delivering this through a proposal for a new ICT staffing structure. These plans could be further developed into a more formal ICT Strategy document.
b) **Implication-** Without a clear, communicable vision for the ICT architecture and infrastructure there is a risk that ICT remains reactive and that efforts are not focused on priority areas that help ensure the Council meets its overall goals and objectives.
c) **Priority Rating**- 3
d) **Recommendation**- ICT should progress the implementation of its plans set out in the report to the Corporate Policy & Resources Committee in June 2016 so that an integrated

	approach to ICT across all Council sites and legacy systems is put in place. Consideration should also be given to developing a more detailed ICT Strategy (including a roadmap or action plan) which supports the Council's Estates Strategy and demonstrates how ICT will support delivery of the Council's corporate objectives.
e)	**Management Response**- Agreed. The 3 ICT Management posts of Infrastructure, Operations and Digital Services are expected to be appointed in November 2016.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan - 1st April 2017

Recommendation 2 – *Contract*	
a)	**Observation**- ICT support is provided in the Ballycastle area by an external ICT Contractor working on site one day per week. This is a long-standing arrangement through the legacy Council. A formal contract is not in place covering these services.
b)	**Implication-** There may be a lack of clarity with regard to the service level expectations and responsibilities of the ICT contractor.
c)	**Priority Rating**- 3
d)	**Recommendation**- ICT should review the requirement for external ICT contract support in Ballycastle to determine if it is required under the proposed structures. If the arrangement is to continue, a formal contractual arrangement should be put in place to cover the services of the ICT contractor and the responsibilities regarding safeguarding and maintaining confidentiality of Council information.
e)	**Management Response**- Agreed. Issue is currently being addressed, as part of ICT Structure.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan & 1st April 2017

Recommendation 3 – *ICT Policies and Procedures*

a) **Observation**-
A number of ICT Policies and Procedures and a Social Media policy have been prepared but are currently still in draft format. From our review, the draft policies and procedures appear comprehensive and will provide clear guidance to staff.

b) **Implication-**
Where policies and procedures are not implemented, there is a risk that staff may not act appropriately (for example with regard to social media or use of removable storage drives) and inadvertently put systems at risk.

c) **Priority Rating**-
2

d) **Recommendation**-
The ICT policies and procedures should be finalised and implemented as soon as possible and ultimately staff should sign the policy acceptance sheet as evidence that they have read and accept these. Training should also be provided for staff on key points within the policies and procedures, particularly where these may be different from legacy practices (eg prohibition of use of personal pen drives and risks of using same, procedures if need a third party to log-on)

e) **Management Response**-
Agreed. Union representatives and other interested parties will be consulted to ensure that we move, in a sensitive manner, from the different legacy policies and procedures to an agreed CGBC configuration. The new policies and procedures must balance the needs of the organisation with the customs and practise of the legacy organisations.

f) **Responsible Officer & Implementation Date-**
Patrick McColgan & 1st February 2017

Recommendation 4 – *Helpdesk*

a) **Observation**-
Requests for ICT support are currently emailed directly to ICT staff via their individual email addresses, telephoned directly to ICT staff or emailed to a general ICT Support email address that has been set up as a central repository of information and to which all ICT staff have access. It is not possible with the current system to determine how many support requests are ‘live’, who is dealing with them, how quickly they were dealt with and whether any common issues are occurring which could indicate other issues that may need resolving.

ICT are currently configuring new software (Microsoft System Centre) which should provide a helpdesk functionality.

b) **Implication-**
ICT support requests may not be processed in an efficient manner leading to frustration for both ICT and wider council staff and the potential that other, broader issues are not identified.

c) **Priority Rating**-
3

d) **Recommendation**-
ICT should continue to progress the configuration of the Microsoft System Centre so that a helpdesk system can be implemented as soon as possible to ensure that there

	is an adequate process for logging and tracking all incidents and identifying similar types of incidents that could indicate other issues
e)	**Management Response**- Agreed. A more informal approach was prevalent in the smaller organisations. The formalised helpdesk is currently being piloted in a controlled manner.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan & 1st April 2017

Recommendation 5 – *Mobile Phone Request Forms*	
a)	**Observation**- The Council has approved a Mobile Phone Policy. Under the policy, new requests for a mobile phone must be made through a form which should set out the business case for issuing a mobile phone, the type of phone required and should be authorised by the line manager. The Mobile Phone Policy also includes a Declaration sheet which staff should sign as acceptance of the Policy and the conditions of use when issued with a mobile phone. We found that 1 of the 7 mobile request forms tested had not completed the criteria section, authorising officer name or date. We also found that one form had been signed by the mobile phone user themselves rather than the line manager. In addition, ICT have not implemented the signing of the Declaration sheets when staff are issued with phones.
b)	**Implication-** There may not be clear rationale or authorisation for issue of mobile phones if request forms are not fully completed. Where Declarations are not completed, there is a lack of evidence to confirm that the staff member understands and accepts the conditions under which they have been issued the phone and their responsibilities with regard to the usage of the phone.
c)	**Priority Rating**- 3
d)	**Recommendation**- Managers should be reminded to ensure that mobile phone request forms are adequately completed and appropriately authorised. ICT should ensure that all forms are centrally stored as part of records management procedures. ICT should also request that all individuals issued with a mobile phone sign the Mobile Phone Policy Declaration as acceptance of the conditions of use. Further, consideration should be given to introducing a similar acceptance sheet for mobile devices such as iPads.
e)	**Management Response**- Agreed. ICT must take a more robust approach both with colleagues to ensure that the relevant paperwork is completed and in internal ICT Section practises. Mobile phone usage was formally the responsibility of disparate departments in the legacy Councils; in CCGBC, the ICT structure reflects the need for a more centralised resource.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan & 1st April 2017

5.2 Risk 2 – Access Controls

Recommendation 6 – *Server Room Access and Administrator Rights*

a) **Observation**-
Access to the server rooms at the 4 main Council sites is controlled by key or keypad and is restricted to ICT staff (and some other key staff who require access to the rooms, such as Caretakers). A log is not kept of access to the server rooms, although we were advised that such logs used to be kept some time ago.

In addition, Administrator rights are currently accessed through one Administrator logon identity and password which all ICT staff use. It is not possible therefore to identify who has used the Administrator access within the system.

b) **Implication-**
There is no audit trail of who accesses the server rooms or uses Administrator logons and therefore a risk of reduced accountability.

c) **Priority Rating**-
3

d) **Recommendation**-
Consideration should be given to reinstating the sign-in logs for each server room so that an adequate record is maintained of who accesses the server room and when.

Consideration should also be given to implementing individual ICT Admin accounts to enable greater tracking, if required, of actions taken at an ICT Admin level.

e) **Management Response**-
Agreed. The security recommendations will be reviewed as part of the ICT Security policy.

f) **Responsible Officer & Implementation Date-**
Patrick McColgan & 1st April 2017

Recommendation 7 – *Protecting Data on Mobile and Portable Devices*

a) **Observation**-
In relation to mobile phones, the Mobile Phone Policy states that any phone (Council-owned or personal) that has access to Council email will have a pin code and remote wipe automatically enforced. To date, ICT have enabled the remote wipe but not the enforced pin code for smartphones.

In relation to laptops, no laptops have been encrypted within the Council.

b) **Implication-**
Unauthorised access may be gained to Council information through the email if a smartphone is lost or stolen and there is no access control enforced on the phone. Unauthorised access may also be gained to Council information if a laptop is lost or stolen and staff are keeping data on their local laptop drives.

c) **Priority Rating**-
2

d) **Recommendation**-
Pin code or pattern access should be automatically enforced on Council-issued smartphones to prevent unauthorised access to Council email or information. ICT

	should also review the arrangements for staff accessing their Council email account on their own devices to ensure that any remote management policies that are applied on Council-issued devices can also be applied for user-owned devices. Further, consideration should be given to encrypting laptops to prevent unauthorised access to Council data in the event that a laptop is lost or stolen. In the meantime, staff should be reminded that information held on a laptop may be at risk if the laptop is lost or stolen and to therefore take care of the security of their device.
e)	**Management Response**- Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan & 1st February 2017

Recommendation 8 – *Notification of Leavers*	
a)	**Observation**- ICT staff are notified by line managers of new users through a new user form. There is no formal process for notification of leavers to ICT. We selected a sample of 10 leavers and found that all but 1 had their account disabled. We were advised that the enabled account had been disabled and passwords re-set but then had to be re-enabled to allow remaining staff to access email (the original user would not be able to access the account). We also selected a sample of 5 folders held on the Council's servers and reviewed the current user permissions for these folders with the relevant Head of Service. We identified for 2 of the 5 folders tested that there were 3 accounts still enabled where the Head of Service was able to confirm that these staff were no longer employed.
b)	**Implication-** Staff may continue to gain access to Council information after they leave the Council's employment if ICT are not informed in a timely manner of leavers.
c)	**Priority Rating**- 2
d)	**Recommendation**- A process for notifying ICT of leavers should be introduced to ensure that accounts can be disabled once the individual leaves or passwords reset if accounts require to remain enabled for any reason. Consideration should be given to ICT staff signing and dating any leaver forms developed as evidence of when the accounts and Outlook Web Access were disabled.
e)	**Management Response**- Agreed. ICT must work in partnership with HR and HoS to ensure its implementation
f)	**Responsible Officer & Implementation Date-** Patrick McColgan and Brid Lofthouse & 1st February 2017

Recommendation 9 – *Server Monitoring*

a) **Observation**-
Servers across the 4 main sites are monitored by ICT staff. Patches and updates to servers are not automatically applied in case they may contain issues but are generally applied within 2 or 3 months of the patch or update being released. Patch and server updates for Ballycastle are carried out annually however through an external service provider annual review (continuing historical arrangement). We found that the servers tested had all been updated recently and were last updated in May 2016 for Ballycastle.

We were advised that server security logs are not generally monitored to identify any unusual access or attempts to access the servers.

b) **Implication-**
Delayed server updates and patches may lead to servers not being as well protected against new threats. In addition, unauthorised or unusual access attempts may not be identified in a timely manner.

c) **Priority Rating**-
2

d) **Recommendation**-
Consistent approaches to server monitoring should be developed to ensure that patches and server updates are applied in a timely manner (in particular in relation to servers in Ballycastle). Server security logs should also be reviewed periodically to identify any unusual server access or attempts to access the server

e) **Management Response**-
Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.

f) **Responsible Officer & Implementation Date-**
Patrick McColgan & 1st February 2017

Recommendation 10 – *Firewall Security*

a) **Observation**-
Under a long-standing arrangement, an external service provider completed an annual review of the servers and firewall in Ballycastle in May 2016. The report from the service provider noted that firewall security settings that it would normally recommend to clients were not implemented on the firewall in Ballycastle. We were advised that this has not been followed up to identify where any weaknesses in the security may be.

b) **Implication-**
The firewall settings (in Ballycastle in particular) may not be up-to-date to meet current threats.

c) **Priority Rating**-
2

d) **Recommendation**-
ICT should review the recommendations from the external service provider's report with regard to the security settings for the firewall in Ballycastle (and across Council's other firewalls) to determine if these should be implemented.

e) **Management Response**-
Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.

f) **Responsible Officer & Implementation Date-**

Recommendation 11 – *Information Governance for Third Party Access*

a) **Observation**-
Third party software providers require access to the Council's servers and data periodically to fix issues in the software (eg for the finance and HR systems). In general, ICT staff monitor the access session given to the Council's systems and access should be restricted to particular servers. We requested details of contracts or service arrangements for the finance and HR system contract providers but staff were not aware of any such contracts.

b) **Implication-**
The confidentiality and data protection responsibilities of third parties in relation to accessing Council data may not be explicitly set out leading to lack of clarity in relation to information governance.

c) **Priority Rating**-
3

d) **Recommendation**-
ICT and Information Governance staff should review whether documented data protection protocols or confidentiality agreements are in place and required for third party contractors who access Council's networks.

e) **Management Response**-
Agreed. This will be communicated to effected HoS to ensure that their respective suppliers adhere to this direction. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.

f) **Responsible Officer & Implementation Date-**
Patrick McColgan & 1st April 2017

Recommendation 12 – *Web Filter Controls*

a) **Observation**-
The firewall settings should ensure that access to inappropriate or risky websites is blocked. We tested this by trying to access two gambling websites from a Council computer and found that both could be accessed. This was investigated by an ICT Officer and an error in the settings was identified and resolved. We re-performed the test and found that both sites were now blocked.

b) **Implication-**
If settings are not reviewed to ensure that they remain correctly set, there is a risk that settings may inadvertently be changed and staff could gain access to inappropriate or risky sites.

c) **Priority Rating**-
3

d) **Recommendation**-
ICT should periodically review the firewall policies to ensure that they remain correctly set.

e)	**Management Response**- Agreed. The enhanced ICT Structure, in the form of a Security Officer, will facilitate this being achieved.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan & 1st April 2017

5.3 Risk 3 – Back-Ups

We have no findings or recommendations to make in this area.

5.4 Risk 4 – Business Continuity & Disaster Recovery

Recommendation 13 – *Business Continuity & Disaster Recovery Planning*	
a)	**Observation**- There are no documented business continuity or disaster recovery plans and no formal testing of business continuity/disaster recovery arrangements for ICT has been implemented. Disaster recovery currently relies on back-up arrangements. It is planned that the Ballymoney HQ will become the disaster recovery site for the main ICT servers in Coleraine and this is currently being tested before server replication goes live.
b)	**Implication-** Without a documented business continuity and disaster recovery plan, and such plans being tested, there is a risk that the expected procedures would not operate effectively. As ICT underpins so much of Council's operations, this risk is particularly significant. There is also a risk that ICT will be delayed in implementing business continuity processes, or that inappropriate or unnecessary actions may be taken, if important information (such as key personnel, business processes and first step business continuity actions) has not been clarified in a formal business continuity plan.
c)	**Priority Rating**- 1
d)	**Recommendation**- A documented Business Continuity and Disaster Recovery Plan should be developed for ICT to provide clear guidance on actions in the event of a business interruption or disaster. In addition, work to develop the disaster recovery site at Ballymoney should be completed as soon as practicable to ensure a smooth transition in the event of any issue affecting the main Causeway Coast & Glens Council severs in Coleraine.
e)	**Management Response**- Agreed. This will be implemented as a matter of priority. The initial scoping exercise will identify the required resources.
f)	**Responsible Officer & Implementation Date-** Patrick McColgan & 1st February 2017

Appendix I: Definition of Assurance Ratings and Hierarchy of Findings

Satisfactory Assurance
Evaluation opinion: Overall there is a satisfactory system of governance, risk management and control. While there may be some residual risk identified this should not significantly impact on the achievement of system objectives.

Limited Assurance
Evaluation opinion: There are significant weaknesses within the governance, risk management and control framework which, if not addressed, could lead to the system objectives not being achieved.

Unacceptable Assurance
Evaluation opinion: The system of governance, risk management and control has failed or there is a real and substantial risk that the system will fail to meet its objectives.

Hierarchy of Findings

This audit report records only the main findings. As a guide to management and to reflect current thinking on risk management we have categorised our recommendations according to the perceived level of risk. The categories are as follows:

Priority 1: Failure to implement the recommendation is likely to result in a major failure of a key organisational objective, significant damage to the reputation of the organisation or the misuse of public funds.

Priority 2: Failure to implement the recommendation could result in the failure of an important organisational objective or could have some impact on a key organisational objective.

Priority 3: Failure to implement the recommendation could lead to an increased risk exposure.

Appendix II: Summary of Key Controls Reviewed

ICT Environment

Risk	Key controls
• There may be an inadequate (or no) formal governance structure in place for managing ICT leading to an uncoordinated approach to the development and management of the ICT systems	• ICT Strategy is in place – this is subject to an audit recommendation • There is a clear governance structure for overseeing ICT within the Council • Key staff have been identified in relation to ICT and there are plans in place to address any issues relating to reliance on key individuals • There is a risk register for ICT • ICT policies are comprehensive and up-to-date – this is subject to an audit recommendation • Policies are in place regarding the use of social media by Council – this is subject to an audit recommendation • ICT policies are communicated to staff – this is subject to an audit recommendation • There is a clear process for incident or problem reporting and management – this is subject to an audit recommendation • Software licences are up-to-date and Business Technology staff are aware when licences are due to expire so that they can be renewed in a timely manner • Staff are not permitted to install unauthorised software on their computers • Directories are periodically reviewed to detect if inappropriate or suspicious files are held on Council systems • Downloads from the internet to Council computers and laptops is controlled • Changes to operating systems and application systems are authorised, tested and approved before being made live to users • There are adequate controls over the selection, testing and acceptance of new software packages
• Access to the ICT systems and networks may not be controlled, leading to potential unauthorised access to sensitive information.	• Levels of access are defined and restricted by user types / location / software required etc • Levels of access to systems are authorised by the system or data owners • Permission to make changes to the system is restricted and documented • Access to Council systems and networks is closed in a timely manner once a staff member or approved third party contractor no longer requires the access or leaves Council's employment – this is subject to an audit recommendation • Access to the systems and networks is monitored and invalid attempts to access the systems and networks is identified and reported appropriately – this is subject to an audit recommendation • Remote access to the ICT systems is controlled and monitored – this is subject to an audit recommendation • Internet and email usage is controlled (eg policies on usage, monitoring etc)

Risk	Key controls
	• Access to information held on computer is controlled and restricted by password • Passwords are changed every 160 days • Portable computers (laptops etc) are encrypted – this is subject to an audit recommendation • Access to the ICT server rooms etc is restricted • A firewall system is in place and security settings are updated regularly – this is subject to an audit recommendation • Anti-virus software is installed on all computers and laptops and is regularly updated • Access to the Council's electronic databases by third parties (eg by IT service contractors) is restricted and data protection responsibilities are clearly set out within the service contracts – this is subject to an audit recommendation
• There may be inadequate back-up arrangements in place to protect systems and data, resulting in a potential loss of information and data in the event of a system failure	• There is a process of regular back-up of systems and data • Back-ups are stored separately from the system so that they are not vulnerable to environmental threats that may disrupt the main system • Back-ups are logged and recorded • Checks are made to ensure that back-ups perform correctly – this is subject to an audit recommendation • Access to back-up information is controlled • There are adequate environmental arrangements in place to protect key hardware such as servers (eg from risk of fire and water)
• There may be inadequate contingency and recovery plans in place to enable the system to recover in a timely manner in the event of a failure or disruption to the system	• There is a business continuity plan for ICT – this is subject to an audit recommendation • There is an ICT disaster recovery plan – this is subject to an audit recommendation • Uninterruptible power supplies are in place for each server • There are plans to test (or tests have already been carried out) the business continuity and disaster recovery plans and document lessons learned – this is subject to an audit recommendation • An action plan is developed to address issues arising from testing – this is subject to an audit recommendation

Appendix III: Points for the Attention of Management

IT Software/Hardware Requisition Form)
The draft ICT policies and procedures document includes a template IT software/hardware requisition form. This form makes reference to it being a draft from Fermanagh and Omagh District Council. Reference to other Councils should be removed from the template.
Management response: Agreed. This will be implemented.

User permissions to folders
ICT has begun some work with Heads of Service to identify new folder structures and permissions to folders to reflect the new organisational structures and information access needs. ICT should continue to work with services to review and ensure that all user permissions to access network folders are correct in light of changes in staffing structures and amalgamation of legacy file systems.
Management response: Agreed. HoS are working in conjunction with ICT to this end. As the staff recruitment process continues, this will be escalated.

Old Servers
We were advised that old servers are located in Ballymoney Town Hall and leisure centre that are not secured in dedicated lockable server cabinets (currently in wooden, lockable cabinets that were made by Council). Whilst the data held on these old servers is not likely to be current, there is a risk that the security of these cabinets may not be as robust as required. ICT should therefore continue to progress its review of its infrastructure. Archive or redundant servers/storage devices should be reviewed to determine if they should remain at their current sites (outside of the 4 main Council offices) or whether they should be moved. If they are to remain in their existing sites, consideration should be given to ensuring that all are in specific, lockable server cabinets.
Management response: Agreed. ICT will continue to work on the disposal/archive of legacy server infrastructure and data.

Back-up Procedures

Back-up procedures have not been documented for all sites and procedures are generally continuing separately based on legacy practices. We found that back-ups were up-to-date and that back-up failures were generally identified and monitored in a timely manner. Testing that back-ups can be restored was not always consistent across all sites and in some cases depended on when ICT staff had time.

Consideration should be given to formally documenting back-up procedures for all servers across the Council's sites so that ICT has an integrated view of the current back-up arrangements and can ensure consistent practice across all its server sites. ICT should also continue to test that its back-ups can be restored and consider making this part of the formalised back-up procedures.

Management response:

Agreed. This is a substantial body of work, and involves increasing our network and in working with internal partners such as Finance and other HoS. The backup documentation will be collated for all sites going forward.

Cloud-based Back-up

A cloud-based service is used to back-up the emails Roe Valley Arts and Cultural Centre. Documentation on the service states that the data is stored in data centres in the USA and Australia. The Data Protection Act 1998 requires that personal information is not hosted in data centres outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Revisions to EU regulations on data protection (expected to be implemented within the next year) are expected to enforce data protection requirements more stringently.

ICT should liaise with Information Governance staff to seek assurance from the cloud service provider that its services will comply with existing and any known planned Data Protection legislation.

Management Response:

Agreed.

Access to Back-up Tapes

Observation-

Full back-ups of Council servers are made to tape in Coleraine and Ballycastle and kept in off-site locations (sports centre in Garvagh and depot in Ballycastle). Tapes are used on a rotation basis with the most recent back-up being stored off-site and other tapes kept in safes in each Council HQ. We were able to physically verify that the back-up tapes were securely stored in locked safes in the main Council HQs and in Garvagh, and were advised that a similar security is maintained in the depot in Ballycastle. We noted however, that one of the full back-up tape sets that should have been in the safe in Ballycastle HQ was not present. After investigation we were advised that this had been sent to a software company used by Council some time ago. We also noted that staff

with access to the safe in the off-site centres will also have access to the full back-ups. There is a risk therefore that access to the full back-ups is greater than required and that missing back-up tapes may not be identified. ICT should therefore review the arrangements for access to the off-site storage of the back-up tapes from Cloonavin and Ballycastle to ensure that access is limited as far as possible and that tape whereabouts is tracked.
Management Response: Agreed as above.