Causeway Coast and Glens Borough Council

Internal Audit Report
ICT- Working from Home

June 2021

MOORE

INTERNAL AUDIT REPORT

ICT – Working from Home

Executive Summary

This internal audit was completed in accordance with the approved annual Internal Audit Plan for 2020/21. This report summarises the findings arising from a review of ICT.

The table below summarises the key risks reviewed:

Risk	Number of recommendations & Priority rating		
	1	2	3
In the change to remote working critical Council processes may cease to be performed or cannot operate appropriately and critical processes may not be able to be monitored within a remote working environment, leading to processes not being completed and potential financial loss and/or reputational damage to the council.	-	2	1
With the introduction of remote working (or additional remote working) as a result of the Covid-19 pandemic there may be an increased risk of inappropriate access to the Council network and/or data, or changes to the network may not be properly requested, documented, approved, and executed, leading to potential non-compliance with data security regulations, and reputational damage.	-	6	-
The servers may be unable to handle the increased workload of those working from home leading to potential system failures and downtime, loss of productivity and financial loss for the council.	-	-	1
Total recommendations made	**0**	**8**	**2**

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.

Table of Contents

Auditor:	Catriona McHugh
Distribution:	Audit Committee Chief Executive Director of Corporate Services Head of ICT

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 management and considered the main risks facing ICT resulting from the majority of staff working from home and a review of the key systems and controls in place to address these. The objective was to ensure that:

- Access to the network and data on the network is controlled adequately.
- A security framework is in place and working effectively.
- Staff are aware of their responsibilities in relation to GDPR
- Council's has sufficient ICT hardware and software to support the increased number of staff working remotely and remote Council meetings

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.

In March 2020, due to the Covid-19 Pandemic the Government requested all those persons that could work from home should work from home until advised otherwise. This meant that staff/officers were required to carry out their duties from home if they were able to do so.

The ICT support unit played a key role in Council's response to the Covid-19 pandemic. When Government regulations made it essential for employees to work from home where necessary, it was the scaling up of ICT equipment and remote access to Council systems which facilitated this and allowed critical Council service delivery to continue and Council meetings to continue. The scope of this audit was to review the ICT arrangements in place within the Council in relation to remote working and assess if these changes were sufficient or if they compromised the security of the Council's system.

The scope of this audit was to review the arrangements in place within the Council in relation to ICT including the impact of working from home, focusing on the main risks associated with:

- Continuing Council critical operations
- Security and unapproved access to Council Network
- Server capacity

This audit is not designed to be a full security check of Council systems.

3 Risks

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

1. In the change to remote working critical Council processes may cease to be performed or cannot operate appropriately and critical processes may not be able to be monitored within a remote working environment, leading to processes not being completed and potential financial loss and/or reputational damage to the council.
2. With the introduction of remote working (or additional remote working) as a result of the Covid-19 pandemic there may be an increased risk of inappropriate access to the Council network and/or data, or changes to the network may not be properly requested, documented, approved, and executed, leading to potential non-compliance with data security regulations, and reputational damage.
3. The servers may be unable to handle the increased workload of those working from home leading to potential system failures and downtime, loss of productivity and financial loss for the council.

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
- Carrying out a preliminary evaluation of the arrangements and controls in operation generally within the Council
- Testing the key arrangements and controls
- Testing the completeness and accuracy of records.

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.

Risk 1 – Interruption to Critical Council Processes

ISSUE 1 – ICT Business Continuity and Disaster Recovery Planning	
a)	**Observation-** Audit found that ICT has a detailed Business Continuity Plan (BCP) in place which was last updated February 2021. Audit was also provided with a 5-page Disaster Recovery document, which is the beginning of the development of a Disaster Recovery Plan. Aduit notes disaster recovery testing has taken place for the finance system, but that a full prioritised, schedule of disaster recovery testing for all essential Council systems is not in place. Audit was advised that the ICT team are struggling to fill the relevant vacant post which is designed to support the development of a comprehensive and detailed ICT Disaster Recovery (DR) Plan and DR testing.
b)	**Implication-** In the absence of a documented Disaster Recovery Plan, including documented re-start procedures (supported by a DR testing schedule) there is a risk of delay in Council resuming its ICT operations after an unexpected event (e.g. security breach through hacking etc). This may lead to Council being unable to function for a period of time resulting in damage to Council's reputation.
c)	**Priority Rating**- 2
d)	**Recommendation**- ICT should arrange to put in place a comprehensive Disaster Recovery Plan, supporting recovery procedures and a Disaster Recovery testing schedule as soon as possible.
e)	**Management Response-** ICT has focussed resources on minimising the risk of ICT disaster in the first place, as opposed to dealing with the consequences of Disaster. This is in the form of hardware and software equipment such as firewalls and antivirus software and have been successful in providing a viable ICT solution to Council to date. With the Disaster Recovery Plan for Finance system in place, we plan to also document the informal arrangements which currently exist for the other key systems when staff resources allow.
f)	**Responsible Officer & Implementation Date-** ICT Infrastructure & Security Manager, November 2021

ISSUE 2 – VPN Availability and Usage
a) Observation- Audit was advised that the bandwidth and firewalls Council had in place were, in theory, capable of handling 100-200 'typical' VPN connections between them. In the early days of the pandemic the best guide to VPN usage and sufficiency of bandwidth was user complaints. There were reports of the VPN being flooded or slow, but no statistical evidence from Council's systems. ICT has now set up the ability to get a snapshot of current traffic. In theory Council has a 1000Mbps connection, with the firewall able to handle about half that in VPN traffic (and more after an ongoing upgrade). ICT feel they are in good shape to provide a full service going forward and complaints regarding VPN access have now dropped off. Audit found ad hoc monitoring of VPN usage, but no formal process was in place.
b) Implication- In the absence of ongoing formal monitoring, at an agreed frequency (e.g. weekly) and reporting of VPN usage there is an increased risk of issues with demand and sufficiency not being noted and managed in a timely manner.
c) Priority Rating- 3
d) Recommendation- A process of regular monitoring of VPN usage should be put in place to see what trends develop (e.g. peak traffic times) and to ensure the bandwidth continues to be sufficient. The outcome of the VPN monitoring should be reported to the ICT Manager monthly and reported to SLT if issues arise.
e) Management Response- ICT will keep records of regular checks of VPN usage.
f) Responsible Officer & Implementation Date- ICT Infrastructure & Security Manager, June 2021

ISSUE 3 – Council Laptops
a) Observation- In order to facilitate remote working during the pandemic ICT managed the procurement and distribution of over 250 additional laptops, and a number of supporting pieces of equipment (keyboards, mouse, printers etc.) to staff. Audit found a list is retained on Excel by the ICT team of the laptops, serial numbers, and the staff member who received the laptop. The ICT Team are now performing an exercise of physically inspecting each laptop to ensure: • Security updates have properly installed on an ongoing basis • PAT safety testing on each device • The correct manage-engine is installed and operational to allow the ICT remote access to all staff laptops, when required. Audit notes that the laptops issued by ICT had not been tagged. Audit requested a copy of Council's Asset Management Policy (covering portable fixed assets) and found that there is currently no documented policy and no requirement to tag assets.

b)	**Implication-** In the absence of an Asset Management Policy (& supporting procedure) there is an increased risk of ineffective security around assets especially portable & moveable fixed assets.
c)	**Priority Rating**- 2
d)	**Recommendation** – It is recommended that Asset Management Policy & procedure be put in place (for fixed assets other than land and property).
e)	**Management Response-** An Asset Management Policy will be developed for IT and the wider assets (by the Finance Team). ICT will comply with any Asset Management Policy developed by Council.
f)	**Responsible Officer & Implementation Date**- Director of Finance & ICT Operations Manager, December 2021

Risk 2 – Increased Data Security Risks and Non-Compliance with GDPR

ISSUE 4 – ICT Security Policy and Procedures

a) **Observation-** Audit notes that ICT has a number of policies which cover security – each policy is supported by a documented procedure:

i. Encryption;
ii. Attempted Intrusion Detection and Monitoring;
iii. Bring Your Own Device;
iv. Email Communications;
v. Account Privilege;
vi. Removable Media;
vii. Patch Management.

A review of these policies and procedures revealed a number of anomalies (e.g. reference to a Password Policy and ICT Leavers Policy neither of which exist; reference to users signing the password policy, this is not happening; the use of a Security Incident log – audit was advised this was an aspiration but is not in place) and some gaps in the guidance within the procedures (e.g. limited guidance on how to manage passwords).

Audit notes an example of security measures outlined in the ICT procedures which are not fully actioned. For "Comprehensive anti-malware, application white-listing and behavioural analysis to detect unusual behaviour" Audit was advised that Trend ApexOne security agent is installed on all clients and servers. This includes anti-malware and behavioural analysis. However, application whitelisting is an aspiration, which has been delayed due to a staff vacancy.

The Business Plan for ICT 2020-21 refers to the development of an ICT Strategy and budget has been assigned (however there is no targeted deadline). The Business Plan highlights the increasing threat and risk around cyber security and outlines the following steps to be undertaken in the next 12 months:

- Enhanced acquisition of security products – firewalls, antivirus products, PEN (penetration) testing – for both the network infrastructure and for end-user kit.
- Increased training for all ICT systems users- staff and Members - on the threat of cybercrime.
- Recommendation to Members of enhanced policy changes to reflect the seriousness of the cyber threats.
- An awareness campaign for staff and Members of the risks to the whole organization, supported both with initiatives from both other government bodies and from the private sector.

b) Implication- In the absence of a comprehensive ICT Security Policy and ICT Security Strategy which succinctly explains the security goals of Council, there is an increased risk of gaps in the strategies and actions required to mitigate ICT Security threats. If Security measures identified within the existing suite of ICT Policies and Procedures have not been actioned due to staffing issues, there is an increased risk of increased ICT Security vulnerabilities. (see more on staffing in Issue 9.)

c) Priority Rating- 2

d) Recommendation- The current suite of ICT Policies should be reviewed, updated, and amalgamated to create a comprehensive ICT Security Policy which is 1) an accurate reflection of a Council's current security activities and, 2) provides realistic and attainable security goals. Associated procedures should be reviewed, updated, and aligned to the newly developed ICT Security Policy.

In tandem with the development of the ICT Security Strategy an ICT Security action plan should be developed and highlight

- any security measures/actions which are deemed essential, some may already be referred to within the current ICT policies and procedures, but are not yet actioned by Council, some will have arisen as a result of PEN and firewall testing, and some may be outlined in the ICT Business Plan 202-21. Responsibilities, deadlines and costs for addressing these should be recorded in the Action Plan.
- any security measures which are desirable but not essential can be included in the ICT Security action plan but noted as longer term aspirations until staff resources or budget can be made available. Such measures should be removed from the ICT Security Policy & Procedures until such times as they can be implemented.

Where budget or staffing resource is a limiting factor on essential security measures this should be outlined in the ICT Security Action Plan and highlighted to SLT and elected members.

e) Management Response- Agreed.

f) Responsible Officer & Implementation Date- ICT Infrastructure & Security Manager, September 2021 and ongoing

ISSUE 5 – Guidance on ICT Security and GDPR Compliance for Remote Working	
g)	**Observation**- Audit found that a number of reminders were issued to staff via e-mail during the pandemic in relation to data security and GDPR while working from home. Council's Human Resources unit was developing a Working from Home policy prior to the pandemic. A new 'Agile Working Policy' is now under development and will supersede the draft Home Working Policy. The Agile Working Policy has recently been provided to Heads of Service for their feedback and input. Audit has been advised this new policy will include guidance on ICT and data security during periods of remote working.
h)	**Implication-** Staff are the last line of defence in the fight against cyber-attacks, which are on the increase. In the absence of a Working from Home Policy there is an increased risk of staff not being as vigilant around ICT and data security rules and procedures when working remotely. This increases the risk of cyber-attack and possible non-compliance with GDPR regulations.
i)	**Priority Rating**- 2
j)	**Recommendation**- HR should finalise and issue the Agile Working Policy as soon as possible and issue this to all staff. HR and ICT should ensure up to date guidance on ICT Security is included in the new policy.
k)	**Management Response-** HR is making all efforts to finalise the Agile Working Policy. ICT will scrutinize the Draft Agile Worling Policy to ensure that it includes appropriate ICT security measures.
l)	**Responsible Officer & Implementation Date-** Head of ICT, ODHR Business Partner Organisational Development/ Head of Policy and Community Planning, November 2021

ISSUE 6 – Training for Staff on ICT Security	
a)	**Observation**- Audit found that no mandatory ICT security training has taken place for staff. However Audit notes that the ICT Business Plan 2020-21 includes the following actions: • Increased training for all ICT systems users- staff and Members - on the threat of cybercrime • An awareness campaign for staff and Members of the risks to the whole organization from cyber crime Audit was advised that the ICT team is already in discussion with a local firm who offer Cyber security training and consulting advice.

b)	**Implication-** Cyber-attacks continue to develop and evolve. ICT Security measures such as firewalls etc. cannot 100% prevent hackers or scammers, staff are the last line of defence. Training raises awareness and encourages staff to remain vigilant. In the absence of mandatory recurring training there is a much higher risk of staff becoming complacent, not fully understanding the important role they play in preventing cyber-attacks, and not knowing the danger signs to look out for.
c)	**Priority Rating**- 2
d)	**Recommendation**- Mandatory cyber awareness/ICT Security training for staff and testing of effectiveness post training should be introduced immediately.
e)	**Management Response-** Agreed. ICT will seek SLT approval to make training mandatory.
f)	**Responsible Officer & Implementation Date-** Head of ICT

ISSUE 7 – Training for Staff on GDPR	
a)	**Observation**- Audit found that the following training relating to GDPR, and records management training has taken place in recent years: • in 2018 to 389 staff • in 2019 to 15 staff • Records Management Training provided in 2020 to 154 staff No mandatory GDPR refresher training is taking place on an annual basis.
b)	**Implication-** In the absence of sufficient GDPR training if a major cyber-attack or data breach resulted in leaking of personal data there is an increased risk of non-compliance with GDPR regulations and a much higher likelihood of a large fine from the ICO.
c)	**Priority Rating**- 2
d)	**Recommendation**- Mandatory annual GDPR refresher training should be introduced immediately.
e)	**Management Response-** A business case for a Data Protection Officer is currently before Council for decision. One of the responsibilities envisaged for this proposed post will require the postholder to undertake appropriate training for Councillors and staff on data protection/GDPR issues. A requirement to provide annual refresher training for staff can be included as a specific requirement in the job description. The postholder would liaise with the HR Business Partner for organisational Development in relation to the organisation and provision of such training for staff. If the DPO post is not agreed by Council, then discussion would have to take place with OD/HR on suitable providers and arrangements for such training.

f)	**Responsible Officer & Implementation Date-** HR Business Partner Organisational Development/ Head of Policy and Community Planning - September/October 2021

ISSUE 8 – New Starts and Staff Leaving Council Employment	
a)	**Observation**- Audit testing of a sample of 5 leavers and 2 new starts (July 2020-September 2020) revealed • For 1 employee who had left in July 2020 had not had the relevant account disabled • For 1 employee although Audit was advised the account had been disabled, for an employee who left in July 2020, there was no audit trail to identify exactly when this had been actioned On further investigation it was found that ICT had not been informed by ODHR of the staff leaving Council's employment .
b)	**Implication**- If there are delays in disabling the IT accounts of staff leaving Council there may be an increased risk of inappropriate access to the Council network and/or data.
c)	**Priority Rating**- 2
d)	**Recommendation**- ICT and ODHR should jointly agree a process for ensuring ICT is informed in a timely manner when there are staff changes (which affect the right to access council's IT systems and data)
e)	**Management Response -** Agreed and HR will issue an email to all HR staff to remind them regarding of the process of issuing leavers email.
f)	**Responsible Officer & Implementation Date-** ICT Operations Manager**,** HR Business Partner Organisational Development, September 2021

ISSUE 9 – ICT Security – External Testing	
g)	**Observation**- Audit found a good level of external security testing. Annually there is an external test of the Council's firewall and there are also firewall penetration tests performed. Audit reviewed the last Penetration Test Report from July 2019. The report revealed no significant vulnerabilities or security issues; however for 2 of the medium risks identified ICT advised audit that there is a delay in implementing the fix required, as a result of staffing resources. These 2 issues are not significant risks. Audit reviewed a report from May 2021 summarising the most recent Firewall Test. There were 4 critical findings. ICT has advised that 2 of the findings will be resolved

	immediately as result of a firewall refresh. The other 2 issues are internal processes that require updating. Audit was advised that these processes will be altered when additional staff resources allow. As mentioned earlier in the report there is a vacancy within the ICT team which Council has struggled to fill. There has been 1 unsuccessful recruitment drive in the open market and Council's recruitment agency was also unable to source a suitable candidate. A second recruitment drive is currently underway.
h)	**Implication**- A firewall is how ICT protects Council systems from the outside world. It is a key factor in network security. Any weaknesses in the firewall require immediate attention. Any delay in addressing any critical issues highlighted by firewall testing increases the risk of malicious or unauthorised access.
i)	**Priority Rating**- 2
j)	**Recommendation**- Council should ensure ICT staffing is sufficient to ensure security issues are promptly addressed. If difficulties persist in filling the relevant vacancy in the ICT team the following should be considered: • A review of the job description and pay scale of the post; or • Temporary hiring of an external expert to address urgent ICT Security matters.
k)	**Management Response-** Agreed.
l)	**Responsible Officer & Implementation Date-** ICT Infrastructure & Security Manager, November 2021

Risk 3 – Council Servers Unable to Support Remote Working

ISSUE 10 – Back-up of Council Information	
g)	**Observation-** Audit was advised that there is a process to facilitate back-ups. A system called Veeam is used and operates automatic incremental and full back-up in line with a pre-set schedule. Although there is regular reviewing of the back-up status reports no evidence is retained of this check.
h)	**Implication-** Without an audit trail to evidence the review of back-up status reports there is a risk of issues with back-ups being overlooked or not resolved in a timely manner.
i)	**Priority Rating**- 3
j)	**Recommendation** – It is recommended that a record of checks on back-ups is retained. Consider introducing a checklist of ICT Security actions (such as back-ups) including their frequency and record initial and date of who performed the check
k)	**Management Response- Agreed.**
l)	**Responsible Officer & Implementation Date-** ICT Infrastructure & Security Manager, November 2021

6 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.

7 Appendix II: Summary of Key Controls Reviewed

Risk	Key Controls

In the change to remote working critical Council processes may cease to be performed or cannot operate appropriately and critical processes may not be able to be monitored within a remote working environment, leading to processes not being completed and potential financial loss and/or reputational damage to the council.	• An ICT Business Continuity Plan is in place which contains:
	  ○ a pandemic as an identified risk to business continuity and
	  ○ includes an analysis of all critical Council processes and
	  ○ how they would be accessed during a pandemic
	  ○ roles and responsibilities for step by step set up of remote working
	• An I.C.T Disaster Recovery Plan is also in place
	• Staff have access to appropriate mobile hardware, other ICT equipment and software to facilitate home working
	• A process is in place for prioritisation and approval of additional hardware and software required (this may be outlined in the ICT BCP) to facilitate home working
	• The switch to virtual meetings occurred in a timely and secure fashion.
	• A working from home policy has been put in place which includes advice on how to report ICT issues when working from home and GDPR matters
	• The ICT Helpdesk facility is able to continue operation during periods of remote working
	• The ICT Helpdesk has a plan which ensures sufficient human resource capacity to manage the increased demand during a switch over to home working – this may be covered in the ICT Business Continuity Plan or other document.
	• Adequate 3rd party support for remote workers is in place if needed (i.e Tascomi support)
	• An ICT Security Policy is in place and provides guidance on
	  ○ working from home
	  ○ accessing remote working / virtual private network
	  ○ keeping data secure whilst working from home
	  ○ personal responsibilities of data security – especially the dangers surfing the internet or using unauthorised websites
	  ○ use of personal devices
	  ○ Physical security (multiple persons using the same device)
	• Remote access is monitored by I.C.T for evidence of overload of servers or systems
	• The telephone system can handle the switch to remote working i.e. the general public and other stakeholders can still call and speak to relevant staff as required

With the introduction of remote working (or additional remote working) as a result of the Covid-19 pandemic there may be an increased risk of	• Comprehensive I.C.T Disaster Recovery Plans are in place
	• An ICT Security Policy is in place
	• Guidance has been provided to staff on –
	  ○ working from home
	  ○ accessing remote working / virtual private network

Risk	Key Controls
inappropriate access to the Council network and/or data, or changes to the network may not be properly requested, documented, approved, and executed, leading to potential non-compliance with data security regulations, and reputational damage.	○ keeping data secure whilst working from home ○ personal responsibilities of data security ○ use of personal devices ○ the use of potential threatening websites and how to best protect against viruses • Processes/procedures in place to make changes on the network have continued during working from home including- ○ Requests are made and documented ○ Manager/HOS/director approval is recorded • Processes/procedures in place to requesting and granting access have continued during working from home including- ○ Requests are made and documented ○ Manager/HOS/director approval ○ An audit trail is retained of any change to access levels (including granting of access to new employees and removing access for staff leaving) • VPNs are periodically tested and continue to be monitored • ICT review and ensure that Firewalls and Encryptions are in place and effective when staff are working remotely • For council owned and network connected devices there is adequate antivirus software installed and kept up to date, and guidance is provided to staff on using their own devices and anti-virus software • Staff understand the limitations of firewalls when working remotely • Where necessary individual applications have their own security and back-up such as Microsoft office • Mimecast checks are carried out on email traffic • Personal data is not stored on laptops or external storage devices. In the event that personal data is stored on such devices, they are encrypted, and password protected. • Portable computers (laptops, iPads etc) are encrypted • Portable device (including mobile phones) users should sign a declaration to verify that they have understood and will comply with a usage policy which includes security guidance • Staff are given guidance on what devices (e.g. laptops, external hard drives, USB pens) they should use to store electronic information • GDPR training has been provided to all staff are aware of who the DPO is • Staff have been reminded of the importance of GDPR during the period of the pandemic • The Council has defined procedures for dealing with information security incidents and staff are aware of these • Information security incidents are investigated and appropriately reported to management and to the Information Commissioner if required • Any invalid attempts to access the systems and networks are identified, investigated, recorded and reported appropriately (includes access to servers)

Risk	Key Controls
	• Manual documentation is stored securely even when working from home; and staff have been reminded that all files containing confidential or personal information is stored in locked cabinets
The servers may be unable to handle the increased workload of those working from home leading to potential system failures and downtime, loss of productivity and financial loss for the council.	• Servers are monitored during times of heightened usage/working from home and more frequently during the Covid-19 response • RDS or citrix is used, to cut down on traffic with the server and allow faster working • If the server is hosted in a cloud by a 3rd party there is an adequate contract in place to allow council to monitor performance and request improvement if necessary • There is a process of regular back-up of ICT 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