Appendix 3: Outstanding Computer Audit Recommendations as at 31st March 2012

Service	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
ICT & Customer Services	Medium	BRK/10.20. – IT Security, Procurement and End User Controls – recommendation 1 Management should conduct a risk assessment of laptop security taking into account such issues as the frequency with which laptops are removed from the Council offices on external Council business, which could mean that laptops are not as secured as they are within the main Council building.	*Original Deadline:* 31 May 2010 *Previous revised deadlines:* 31 May 2011, 30 November 2011	31 March 2012	Specific risk assessment document outstanding although risk is minimal due to processes carried out and security in place for building laptops. ICT security policy describes the responsibility of the user when using mobile devices.	As per the management response, no risk assessment has been undertaken. Furthermore we were unable to locate the section in the ICT Security Policy regarding security for mobile devices.
ICT & Customer Services	Medium	BRK/10.20. – IT Security, Procurement and End User Controls – recommendation 5 Management should ensure that they have a suitable removable media policy and supporting infrastructure in place as soon as possible, preferably before it becomes a mandatory Government Connect requirement.	*Original Deadline:* 30 June 2010 *Previous revised deadlines:* 31 December 2010, 31 May 2011, 30 September 2011	30 June 2012	As the desktop refresh program is rolled out one of the criteria will be to lock out the use of unencrypted removable devices. There is additional information available through the Belarc product which identifies all usb devices and their connection details the enables monitoring by exception easier. Further encrypted devices need to be bought after we	We note management response however the recommendation appears to relate to a Removable Media Policy. This has not been provided as evidence and it is unclear how management response addresses the recommendation.

Service	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
					have established how many are required during the refresh process.	Discussions with JL were held however evidence to confirm implementation could not be provided during the follow up process.
ICT & Customer Services	Medium	BRK/11.16. – Network Infrastructure – recommendation 5 Management should conduct a review into the following findings and take appropriate action: • There are 33 active administrator accounts, which represents about 4% of the total number of user accounts. The number of such accounts should be kept to a minimum; • 411 accounts have passwords set to never expire. These include member accounts, mailboxes and system accounts. Only system accounts should be set to never expire and only if assigned a strong password; • 10 accounts are permitted to operate without a password. Note that this does not mean that these accounts do not have a password, only that the facility exists. Where this is not required the facility should be removed; • There are a large number of accounts that appear not to have home directories, logon profiles or logon scripts applied to them. Consistency should	*Original Deadline:* 30 November 2011	31 March 2012	None provided	This has been partly implemented. The remaining requirements are to: a) provide evidence that there are no members accounts for which the passwords are not set to expire. On inspection of the domain settings, it was confirmed there are still a number of accounts where passwords are infinite. b) either change the built in

Service	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
		be applied where possible; and • There are a number of accounts that appear to be generically named.				administrator account name from Domain Admin to something more cryptic and less easily guessable, and/or to set the domain admin account to have an expiring password. Evidence to confirm implementation was requested, however this was not provided to us during the follow up process.
ICT & Customer Services	Low	BRK/11.16 – Network Infrastructure – recommendation 9 Management should conduct periodic reviews of the services on the Domain Controller to ensure that only required services are available. Where services are not required, they should as a minimum be disabled and preferably removed.	*Original Deadline:* 30 November 2011	31 March 2012	Further investigation required to establish the exact requirement. James Hewitt and Steve Duffy will be required to understand what is required.	From discussion with IT Auditor we are informed that as per recommendation a review of the Device Domain Controller should be undertaken, with a documented review of

Service	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
						services running in the background undertaken to assess whether there are any legacy programmes running whilst are obsolete.
ICT & Customer Services	Medium	BRK/12.15 – Anti Virus, Spyware and Malware – recommendation 5 Management should ensure that the patch management process is restarted as soon as possible.	*Original Deadline:* 31 December 2011	31 March 2012	John Laufs has left the Council but this work has been taken over by James Hewitt. he is reviewing the whole patching process and developing a method of deploying the patches that will make it easier to keep them up to date in future. Resource required within ICT team to complete this work. Further progress has been made but full rollout and process not in place.	Met with John Laufs, with some progress made. Walked through server status. 28 have been upgraded to SP2. There are five further servers which can be patched to SP2 and several than can now be decommissioned. We note management response with progress, no revised deadline has been provided at this time.
ICT & Customer	Medium	BRK/12.17 – Internet and E-Mail – Recommendation 4	*Original*	None specified	3 members of the	Implementation

Service	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
Services		Management should implement cross training in the use of the Firewall, Email and Internet Security applications.	*Deadline:* 31 March 2012		technical response have been working together to cross train on the use of the firewalls, email and internet security.	will be reviewed again in Q1 12/13.
ICT & Customer Services	High	BRK/12.17 – Internet and E-Mail – Recommendation 5 Management should ensure that all relevant firewalls are included within the routine network backup process with immediate effect. In addition, the folder used to store the rules backup files should be moved to a secure location separate to the firewall server itself.	*Original Deadline:* 31 March 2012	None specified	Some firewalls are backed up but there needs to be a sanity check on whether all are covered	Implementation will be reviewed again in Q1 12/13.
ICT & Customer Services	Medium	BRK/12.17 – Internet and E-Mail – Recommendation 6 Management should formally document firewall resilience and recovery procedures and ensure that they are tested periodically.	*Original Deadline:* 31 March 2012	None specified	Reported as outstanding.	Implementation will be reviewed again in Q1 12/13.
Environmental Health	Medium	BRK/12.19 – LalPac Licensing Application – recommendation 2 Management should implement a process whereby a separate reconciliation of licence applications is conducted, possibly by conducting spot checks of licence applications deemed to be complete. The LalPac application's upgraded Auditing tools should also be used as part of the process when the upgrade has been completed.	*Original Deadline:* 29 February 2012	None specified	Auditing of 10% of the work is scheduled to take place every month beginning March 2012 and is going to be rotated by the officers awaiting the appointment of the licensing manager. A form has been developed to record the audit and once the audit has been completed it will be returned to the licensing manager to	Evidence to verify implementation of recommendation was requested during the follow up exercise, however this was not provided by the key contact during this period. Implementation will be reviewed again in Q1

Service	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
					review training etc as seen fit. The team have had the following briefing on the 8th February. As a result this recommendation can be classed as completed.	12/13.
Environmental Health	Medium	BRK/12.19.03 – LalPac Licensing Application – recommendation 3 Management should formally document all LalPac upgrade tests into a test script. This script should cover: • all changes contained within the current release notes; and • Standard tests of the wider application to ensure that the changed application continues to operate within required parameters. Scripts required for each subsequent upgrade should also be documented and combined with the already developed scripts where appropriate. For final implementation to the live environment there should be: • formal sign off of testing results; • formal acceptance of the upgraded application; • formal notification to IT that the upgrade to Live can go ahead; and • back out plans in the event of unforeseen circumstances.	*Original Deadline:* 31 January 2012	None specified	We have an update on LalPac pending with IT. The update has been uploaded to the test LalPac site and testing was completed and has been documented on the 7th November 2011. This is in a pdf document (about 30 pages) and can be provided if needed. Back up plans etc are covered by the IT team as the systems are backed up onto the server daily and therefore this recommendation can be classed as completed.	Evidence to verify implementation of recommendation was requested during the follow up exercise, however this was not provided by the key contact during this period. Implementation will be reviewed again in Q1 12/13.