Appendix 3

Outstanding Computer Audit Recommendations at 31 March 2010

Service	Responsible Manager	Priority	Recommendation	Management Response	Initial Deadline	Revised End Date	Internal Audit Conclusion
Strategic	Teresa Cannon	High	Report BRK/07/11 – Recommendation 1 Risk Assessment - The corporate Business Impact Analysis and IT risk assessments should be completed at the earliest opportunity.	Business Impact Analysis and IT risk assessments have been completed. These form part of the Service Business Continuity Plans and a sample is attached as evidence. A list of critical IT systems is also maintained by ICT, copy attached for information. A Corporate Business Continuity Plan has been drafted, however, it is essential to maintain the service plans which contain more detailed information. A revised BIA will be developed following the exercise on 26 Feb 10, as part of the review of plans, to ensure all critical information is contained within the plans.	Tues-1-Jan-08	Wed-3-Feb-10	PARTLY IMPLEMENTED We note management's responses but deem this to be partly implemented. When the Business Continuity Plan is complete this will be signed off. Revised deadline 30/06/10.

Service	Responsible Manager	Priority	Recommendation	Management Response	Initial Deadline	Revised End Date	Internal Audit Conclusion
ICT	Kevin Taylor	Medium	Report BRK/08/02 – Recommendation 1 The Council should, through an appropriate management forum, update its IT Security Policy in line with the provisions of ISO27001 and ensure Steria comply with the policy.	Discussed at the Audit Recommendations review clinic on 10 March 2010 this would be implemented by the end of March	Thurs-13-Dec-07	Tues-30-Mar-10	PARTLY IMPLEMENTED: Internal Audit reviewed the recommendation as part of the verification that was requested to take place in March, but this was yet to be implemented. Subsequent to this work, the revised IT Security policy was taken to the Business Improvement Sub-Committee in April 2010, who requested amendments to the sign-off form to confirm and clarify the consequences of failing to sign the policy. Once finalised, this can be circulated to Steria. Revised Deadline – 30 April 2010
ICT	Kevin Taylor	Medium	Report BRK/08/02 – recommendation 6 The Council should develop information security training for all staff.	Discussed at the Audit Recommendations review clinic on 10 March 2010 that the Council would be purchasing software for staff to undertake training	Thu-13-Dec-07	Tue-30-Mar-10	OUTSTANDING: This will be implemented following completion and approval of the IT security policy review. The policy will be communicated to all staff who will be required to sign off their acceptance of the policy, to include a short questionnaire to help prove their knowledge. Revised deadline April 2010 to allow for the policy review to be completed first and then training to be implemented.

Service	Responsible Manager	Priority	Recommendation	Management Response	Initial Deadline	Revised End Date	Internal Audit Conclusion
ICT	Kevin Taylor	Medium	Report BRK/08/02 – recommendation 18 The Council, in collaboration with Steria, should periodically review the continued need for staff, with remote access to the Council's network and infrastructure. The Council should introduce a Remote Access Policy. This would define the security framework and provide a mechanism through which remote access could be governed.	Discussed at the Audit Recommendations review clinic on 10 March 2010 that this would be completed alongside the IT Security Policy	Thu-13-Dec-07	Tue-30-Mar-10	PARTLY IMPLEMENTED: The revised IT Security policy now contains a section on remote access and a separate remote access policy is to be drafted. Revised deadline April 2010.
ICT	Kevin Taylor	Medium	Report BRK/08/20 – recommendation 1 - The use of remote access should be reviewed, documented and confirmed	Discussed at the Audit Recommendations review clinic on 10 March 2010 that this would be completed alongside the IT Security Policy	Tue-1-Jul-08	Tue-30-Mar-10	OUTSTANDING: Examples of authorisation model operating in practice have been requested but not received at the time of writing. Therefore, we are unable to validate this recommendation and considered outstanding.
ICT	Kevin Taylor	Medium	Report BRK/08/20 – recommendation 15 Information Security Policy – Confirmation of Understanding / Compliance	New ICT Security Policy reviewed at Business Imp Sub Committee in April - and will be part of new induction process. Email to be sent to all staff in interim to ensure awareness raised, and referencing proposed Info Sec training	Tue-1-Jul-08	Wed-7-Apr-08	OUTSTANDING: Once the IT Security Policy has been completed, staff will be required to confirm their understanding and compliance – this exercise will complete the recommendation.

Service	Responsible Manager	Priority	Recommendation	Management Response	Initial Deadline	Revised End Date	Internal Audit Conclusion
Strategic	Andrew Grimley	Low	Report BRK/09/15 – recommendation 6 – Clear Desk Policy	Discussed at the Audit Recommendations review clinic on 10 March 2010 that there is still some non-compliance with ensuring a "clear desk" policy	Thu-1-Jan-09	Wed-31-Mar-10	OUTSTANDING Having spoken to the Officer we understand that the Council is taking a phased approach to implementing this recommendation, exact details of implementation date are unclear. Hence Revised deadline of 30/06/10
ICT	Kevin Taylor	Medium	Report BRK/10/18 – recommendation 2 Management should work with Steria to ensure that a periodic review of the software inventory is conducted to ensure that only relevant, legal and up-to-date software has been installed on the Council's systems. We would recommend that a documented annual review may be sufficient.	Recent audit confirmed software licencing being managed well. Have agreed with Steria to initiate annual audit of licences as recommendation	Wed-31-Mar-10	Wed-31-Mar-10	OUTSTANDING: We have not been made aware whether this has been subsequently implemented.
ARP	Rod Urquhart	Low	Report BRK/10/19 – recommendation 4 – Management should work with the user groups to consider requesting an enhancement to the application's login sequence such that no information about the validity of either the username or password is displayed when such an error occurs.	Raised with Product Suppliers at the National User Group in Jan and this functionality may be added to the product in a future major release in 2010/11	Sun-28-Feb-10	Wed-31-Mar-10	OUTSTANDING: We were unable to confirm with the officer whether this has yet to be implemented, although given no further update we have assumed this is yet to be implemented.

Service	Responsible Manager	Priority	Recommendation	Management Response	Initial Deadline	Revised End Date	Internal Audit Conclusion
ICT	Kevin Taylor	Medium	Report BRK/10/20 – recommendation 2 – Management should ensure that a replacement policy supporting the proposals contained within the ICT strategy be drafted and agreed once the ICT strategy itself has been approved. This policy should include formally agreed minimum hardware standards that guide the replacement/procurement of new devices.	Agreed with audit that a statement referencing the need to have kit 'fit for purpose' will suffice, as recognises changes in technology and ability to sweat assests to realised greater efficiency savings.	Wed-31-Mar-10	Wed-31-Mar-10	PARTLY IMPLEMENTED – as above, this will be completed with the formal acceptance of the IT Strategy
ICT	Kevin Taylor	Medium	Report BRK/10/20 – recommendation 7 Management should ensure that an adequate Blackberry security policy that complies with Government Connect requirements is implemented as soon as possible. A review of the available default security policies contained within the Blackberry Server application should also be conducted, with the most feasible hardened option being implemented in the interim.	Mobile device policy now updated to include Blackberrys and laptops.	Sun-28-Feb-10	Wed-31-Mar-10	PARTLY IMPLEMENTED Although the Mobile device policy and the IT strategy make reference to mobile devices, the remaining element of this recommendation refers to the server application review, and as such this is presently completed partly implemented.