Executive Summary

1. As part of our 2005/06 audit of Argyll and Bute Council, we conducted a high level overview of the overall arrangements for the provision of Information Communications Technology (ICT) services within the Council's Education Department. The review covered:

   - ICT strategy;
   - organisational structure;
   - installation management;
   - service delivery;
   - asset protection;
   - business continuity/contingency; and
   - networking.

Conclusion

2. Overall, provision of the ICT Service within the Education Department appears satisfactory. Our audit work has, however, identified several areas where further improvements could be made. A summary of these areas is included below, with details included as part of the action plan at section 2.

Main audit findings

3. The main areas for improving the management and operation of the ICT within the Education Department include:

   - a process for procuring software and hardware involving both teaching and ICT staff should be developed;
   - all software and hardware installed within the Education Department should be carried out by suitably trained ICT technicians or other trusted employees (trusted employees is Council terminology);
   - updating the ICT strategy for the Education department to include timescales, indicating when and by whom will monitor and review it; and
   - developing appropriate business continuity plans for ICT services within the department.

Management action

4. Detailed recommendations on those areas where controls could be improved are noted in the action plan that follows. The action plan also describes under the 'risk exposure' column the possible consequences of our audit finding. The factual accuracy of the report and the timescales for implementing our recommendations has been agreed with officers.

5. This report to management sets out our findings from the review carried out. The weaknesses outlined are only those which have come to our attention during the course of our normal audit work and are not necessarily, therefore, all of the weaknesses which may exist.

6. Although we include a number of specific recommendations in this report to strengthen internal control, it is the responsibility of management to determine the extent of the internal control system appropriate to the Council. We would stress, however, that an effective internal control system is an essential part of the efficient management of any organisation.

7. The assistance and co-operation we received during the course of our audit is gratefully acknowledged.

Section 2 – Action Plan

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
1	ICT staff highlighted major security concerns in relation to two software applications (NETIDME and Truancy Call) which some schools planned to install. Testing by ICT staff identified security issues with these applications. Our review identified that no formal process exists for procuring software or hardware within the Education Department. Since the audit the Council has developed a procedure for procuring software (and hardware). However, this procedure has yet to be used.	Purchasing software without involving specialist ICT staff can result in the purchasing of a badly performing application (for example the current network capacity could be insufficient to support the application). In addition, the application could have weak security or may have an unsuitable licence. ICT staff should therefore ensure that any new hardware complies with corporate standards and that they have the necessary level of expertise to support it.	A procurement process should be developed involving both teaching and ICT staff. Teaching staff should identify the software application and ICT staff should check that the software and hardware • complies with the appropriate corporate standards; • the impact of the new application on the network performance; and • the security of the application. ***Priority : High***	**Action:** Apply the recently developed procedure to procurement of any new software and hardware. **Responsibility:** ICT Development Manager **Date:** December 2006	The ICT Development Manager has reported to Internal Audit that there is ongoing progress with implementation.

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
2	Currently many staff with the Education Department can install software on the schools networks.	Allowing a lot of staff to install software on the schools computers can potentially result in poorly configured applications, badly performing applications and weak security. Staff who install the software many be unaware of the licensing restrictions which can potentially lead to legal action against the Council if software is installed against the licence arrangement or if illegal software is installed.	Any software installations on the schools network should be handled or carried out under the supervision of the ICT technicians or other trusted employees. ***Priority : High***	**Action:** Management procedures are being developed as part of the identified Information Security (IS) Policy for Education. **Responsibility:** ICT Development Manager **Date:** Initial draft of policy will be available by December 2006	The ICT Development Manager has reported to Internal Audit that there is ongoing progress with implementation.
3	The future strategy for ICT within the Education Department is outlined in ICT Strategy for Education Overview. Whilst this document outlines the plans for the future it does not include appropriate timescales. Nor does it indicate when it will be reviewed and by whom or who is responsible for monitoring progress against the strategy.	Developing a strategy for ICT within the Education Department is to be commended. However without indicating timescales for implementation or the review and monitoring mechanisms installed restricts understanding among management and staff and is likely to reduce the effectiveness of the strategy.	Update the existing strategy by adding timescales, review and monitoring mechanisms. ***Priority : High***	**Action:** The strategy will be further developed in conjunction with colleagues in the Education Service. **Responsibility:** ICT Development Manager and Quality Improvement Officer - ICT **Date:** Initial draft will be available by August 2006	As above.

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
4	ICT is one area where software applications and environments are rapidly changing. It is important that ICT staff receive the appropriate training in these new developments or at least set aside time to become familiar with any new applications. Council staff recognise this requirement and work is ongoing in development training plans for technicians and introducing a mentoring system.	Without adequate time set aside for training or for familiarisation with the application, ICT staff will not be able to fully support the introduction of new applications and associated the features.	The training plan for ICT staff should be completed and implemented. The planned mentoring scheme should be implemented. When installing new software or hardware appropriate training, if required, should be provided to ICT staff. It is advisable to include this task within the project plan for any new hardware or software. The training provision should be subject to periodic review. ***Priority : High***	**Action:** ICT Training Plan being developed for all ICT Support staff within Community Services **Responsibility:** ICT Development Manager **Date:** Plan established by August 2006	The ICT Development Manager has reported to Internal Audit that there is ongoing progress with implementation.
5	During our audit visit we identified that visitors could enter Inveraray Conference Centre without challenge.	Unauthorised access to council premises should not be permitted as it raises both security and health and safety issues.	All staff should be reminded that visitors should sign in to council premises and if appropriate be escorted. ***Priority : High***	**Action:** Procedures are in place. Closer monitoring of security arrangements is being done.	**Complete.**

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
6	In secondary schools, one network hosts both teaching and administrative computers.	This is a potential security weakness, as in theory, it is possible for pupils to hack into the administrative computer.	A review of the existing network should be undertaken to ascertain if improvements to security of the existing networks is feasible. Possibilities include separating the student and administrative computers into different segments of the network. This approach would help enforce better access controls to the respective computers. ***Priority : High***	**Action:** Closer monitoring of activities will be undertaken as part of implementation of IS Policy for Education. **Responsibility:** ICT Development Manager **Date:** Initial draft of policy will be available by December 2006	The ICT Development Manager has reported to Internal Audit that there is ongoing progress with implementation.
7	In general, most staff were aware of the need to use strong passwords. However, a small number were unaware of this requirement.	Staff use easily guessable passwords, which could allow unauthorised and inappropriate access to the Education Department's computer facilities.	All staff using computers within the Education Department should be reminded to use strong passwords. ***Priority : High***	**Action:** This exists on Corporate Network and will be implements as part of IS Policy for Education. **Responsibility:** ICT Development Manager **Date:** Initial draft of policy will be available by December 2006	As above.

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
8	At the time of audit, the inventory of software and hardware was incomplete. At present the opportunity exists for items to be purchased directly by schools. These items are not reflected on the inventory consistently.	Software licences are included in the council's balance sheet as fixed assets. However, without a detailed count of the software licenses this figure may be inaccurate. Generally software is subject to license agreements, which can be legally enforced. Operating with unlicensed software is an offence. Without a detailed inventory it is difficult to argue that all the necessary steps were taken to ensure that only properly licensed software is used within the schools.	Update the existing inventories to ensure that all software and hardware are included. Consideration should be given to monitoring hardware and software configurations of all networked computers. ***Priority : Medium***	**Action:** This will be implemented as part of IT work plan over the coming year. **Responsibility:** ICT Development Manager **Date:** In place by November 2006	**Complete.**

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
9	We were unable to establish the existence of standard network procedures, security and data protection handbook.	Network procedures describe how various networking administrative tasks are carried out. They are useful in training staff new to the task and in documenting tasks which are generally only undertaken once or twice during the product's lifetime. One of the tasks identified as necessary for the Council to meet BS7799 Information Security Management standard, was for the Education Department to develop a security and data protection handbook. Without such a document the department would find it difficult to comply with this standard.	Develop the appropriate network procedures. Develop security and data protection. ***Priority : Medium***	**Action:** Network management procedures are being developed as part of the identified (IS) Policy for Education. **Responsibility:** ICT Development Manager **Date:** Initial draft of policy and handbook will be available by December 2006	The ICT Development Manager has reported to Internal Audit that there is ongoing progress with implementation.
10	A comprehensive service level agreement (SLA) is an essential requirement for the provision or receipt of any important service. A SLA defines the parameters for the delivery of that service, for the benefit of both parties.	The parameters of the service delivery arrangement are not adequately defined.	Finalise the SLA for National Grid for Learning project.	**Action:** This will be addressed in re-negotiation of contract. **Responsibility:** ICT Development Manager **Date:** April 2006	Management has reported that finalisation of the SLA was delayed due to resolving a hardware issue. A new implementation date of end June 2006 has been provided by management.

No.	Audit Finding	Risk Exposure	Recommendation	Action Responsibility and Date	Update as at 5th May 2006
11	The aim of business continuity planning is to ensure that an adequate service level can be provided if an unforeseen incident occurs. The Progress Report on Argyll and Bute Council Education Information Security Implementation Plan dated February 2005 highlighted several outstanding actions in the area of business continuity planning.	Incomplete business continuity plans will have an impact on the service provision provided by the Education Department should an unforeseen incident occur.	Identify the resources required to complete this action.	**Action:** The Education Management Information System (SEEMIS) will be included incorporate Disaster Recovery Project which accommodates Business Continuity plans. **Responsibility:** ICT Development Manager **Date:** April 2006	**Complete.**