INTERNAL AUDIT SERVICE

High Priority Weaknesses Identified

Client	**Director for Corporate Support (Senior Information Risk Officer)**
System	**Corporate Information Management (2010-2011) – Final Audit Report issued September 2010**

Matter Arising	Recommendation	Responsible Officer / Target Date
Information Governance is not recorded consistently as a risk across the Authority. It is identified as a 'Medium' risk in the Council's Strategic Risk Register and in the ICT department's Operational Risk Register. However, although various information-related issues are included in other departmental Risk Registers, information governance itself is not considered to be a risk and does not appear in any of them.	The Senior Information Risk Officer (SIRO) should ensure that this issue is addressed through the Operational Risk Management Group and that Information Governance becomes a mandatory inclusion in every department's operational risk register.	Head of Corporate Risk and Insurance Target Date: 11/11/10

Management Response to Audit Report issued September 2010
Recommendation agreed. A way forward in raising the profile of the risk issues would be to make Information Governance a mandatory risk for inclusion in all directorate/departmental Operational Risk Registers - this would then promote regular monitoring in line with well-established existing processes to DMTs, CMT and Members of Audit Committee. The Council's Corporate Information Manager attended a meeting of the Operational Risk Management Group (ORMG), on 15th October 2010, to take them through the key issues in order to achieve consistency in the way that risks are recorded and monitored. This will be followed up by more detailed guidance at the next meeting of the ORMG in December 2010.

Update as at May 2011
'Information Governance' is now included in all departments' Operational Risk Registers. In March 2011, the Council's insurance brokers (Heath Lambert) provided an Information Governance training workshop for Risk Champions, to clarify what their role was and what action they needed to take. A standard risk assessment template has now been developed to assist Risk Champions in assessing the specific risks within their areas and once this template has been completed, it will be used to identify issues for inclusion in the departmental operational risk registers. The template is scheduled to be completed by the end of June 2011.

Matter Arising	Recommendation	Responsible Officer / Target Date
The topic of Information Management lacks a sufficiently high profile within the Council. i.e. There is no regular monitoring of progress on information management issues at Committee level.	The SIRO should seek to formalise Member and Committee reporting arrangements for the management and oversight of information management across the organisation, in a manner similar to that already in place for topics such as Risk Management and RIPA reporting procedures.	Head of Corporate Risk and Insurance Target Date: Process to commence from 11/11/10

Management Response to Audit Report issued September 2010
Recommendation agreed. Once Information Governance has been included in every department's operational risk register, it will be managed through the existing Risk Management process, which includes regular reports to Audit Committee.

Update as at May 2011
The Audit Committee already receives regular Risk Management reports which now include both strategic and operational information governance issues.

Matter Arising	Recommendation	Responsible Officer / Target Date
Other than the identified 'Caldicott Guardians' in the Adult Health and Social Care and the Children and Young People areas, there are no Information Lead Officers in any of the Council's other directorates.	The Corporate Information Manager should take action to ensure that: a. An Information Lead Officer is identified in each directorate and that their responsibilities are incorporated into their Role Profiles and linked to their Staff Appraisal Objectives. b. Assistant Directors identify all information management roles within their directorates and include them in the relevant Role Profiles and Staff Appraisal Objectives.	Corporate Information Manager Target Date: 31/12/10 Corporate Information Manager Target Date: 31/12/10
Management Response to Audit Report issued September 2010		
Recommendation agreed. The need to identify departmental Information Lead Officers is set out in the Council's approved Information Management Strategy and the Corporate Information Manager will pursue this issue as agreed.		
Update as at May 2011		
The SIRO has written to all Directors, asking them to appoint Information Lead Officers (ILOs), within their service areas, to contribute to a corporate Information Management steering group and also to identify their staff that have a specific role in relation to information systems in use. Work has already commenced on this major task and it is expected that further significant progress will be made throughout the current year. The Corporate Information Manager will agree the 'role' of the ILOs with them at the inaugural meeting of the Information Management Steering Group and ensure that the details are included in their role profiles.		
Matter Arising	**Recommendation**	**Responsible Officer / Target Date**

There is no corporate steering group in place to manage the changes needed in order to implement the requirements of the Council's Information Management Strategy and embed its Information Management Principles.	The Corporate Information Manager should instigate the formation of an Information Management Steering Group, comprised of the nominated Information Lead Officers from each directorate (See section 1.4 above) and with formal Terms of Reference, to manage the implementation of the Council's Information Management Strategy and the embedding of its approved Information Management Principles throughout the organisation.	Corporate Information Manager Target Date: 31/12/10
Management Response to Audit Report issued September 2010		
Recommendation agreed. The group will be convened once the directorate Information Lead officers have been identified.		
Update as at May 2011		
The existing Management Information Security Forum (MISF) will become the wider Management Information Steering Group and will include the directorate ILOs as well as other officers who are involved in information governance and security issues. The steering group will also be attended by the Assistant Director for ICT.		
Matter Arising	**Recommendation**	**Responsible Officer / Target Date**

The principles of the Council's approved Information Management Strategy have not yet been fully embedded throughout the organisation.	The Corporate Information Manager should ensure that the Action Plan, attached to the IMS, is updated and should then gain the approval and commitment of CMT for the allocation of the corporate and directorate budgets (and other resources) needed in order to ensure its completion.	Corporate Information Manager Target Date: 30/4/11

Management Response to Audit Report issued September 2010
Recommendation agreed. The action plan will be updated and approval sought.

Update as at May 2011
New target dates for the Action Plan will need to take into account the results of the departmental information risk assessment exercise, which is currently underway. Once this exercise has been completed, at the end of June 2011, the Corporate Information Manager will then update the Information Management Strategy Action Plan. A number of budget and resource allocations have already been agreed for 2010/11 and 2011/12, examples of which are shown below: The Corporate Accommodation Strategy – including the provision of a new data centre. Investment in Carefirst – including improved system administration. Improvements in data management e.g. HR/Payroll and Housing systems. The new telephone and 'hot desking' technologies.

Matter Arising	**Recommendation**	**Responsible Officer / Target Date**

Information Management is not covered as a specific topic in the Council's corporate induction process and there are no formal training courses available in-house in respect of information management (except for the e-learning course for Government Connect email users, which is only taken by a limited number of staff).	The SIRO should ask the Assistant Director for HR and Organisational Development to amend the corporate induction programme to include coverage of the aims, objectives and requirements of the Council's Information Management Strategy.	This issue will need to be actioned by the Assistant Director for HR and Organisational Development and a target date agreed.

Management Response to Audit Report issued September 2010
The Assistant Director for ICT and the Corporate Information Manager both agree that the recommended action is necessary and important but its implementation has not yet been confirmed by the Assistant Director for HR and Organisational Development. This issue will be pursued and an update provided to the next Audit Committee.

Update as at May 2011
The corporate induction programme is currently being reviewed with the aim of improving its content, the way in which it is delivered and its overall effectiveness. The Assistant Director for HR and Organisational Development has agreed that the subject of information management will be addressed as part of this process. The new procedure will commence in July 2011 after which, the results of the trial will be assessed and any required changes will be reported to CMT for approval.

Matter Arising	**Recommendation**	**Responsible Officer / Target Date**

Comprehensive written policies, procedures, instructions and user guidance notes, covering all aspects of information management, are readily available to all computer users via the Document Library on Staffroom. However, they are not so readily available to non-computer users who may also handle equally valuable physical forms of information. Furthermore, staff do not acknowledge receipt and understanding of Council policies and procedures, etc	The SIRO should ask the Assistant Director for HR and Organisational Development to ensure that all departmental induction programmes are amended to include a section covering of the aims, objectives and requirements of the Council's Information Management Strategy and of the Council's information management policies and guidelines, etc. e.g. the Information Security Policy.	This issue will need to be actioned by the Assistant Director for HR and Organisational Development and a target date agreed.

Management Response to Audit Report issued September 2010
The Assistant Director for ICT and the Corporate Information Manager both agree that the recommended action is necessary and important but its implementation has not yet been confirmed by the Assistant Director for HR and Organisational Development. This issue will be pursued and an update provided to the next Audit Committee.

Update as at May 2011
The departmental induction programmes are currently being reviewed with the aim of improving their content, the way in which they are delivered and their overall effectiveness. The Assistant Director for HR and Organisational Development has agreed that the subject of information management will be addressed as part of this process. The new procedure will commence in July 2011 after which, the results of the trial will be assessed and any required changes will be reported to CMT for approval.

Matter Arising	Recommendation	Responsible Officer / Target Date

Although PCC acknowledges that information is its second most important asset, the Authority does not know what information it actually holds or where it is all stored. Although there are long established inventory procedures in place for recording and controlling physical assets, there is no approved system for recording information assets. As things stand, the Council cannot be sure that it holds an up to date 'single version of the truth' and it cannot ensure that its information assets are being used to their full potential.	The SIRO should initiate the introduction of corporate Records Management capabilities, throughout the organisation, by asking the Corporate Information Officer/Manager to prepare appropriate recommendations for approval, together with proposed timescales for their implementation.	Corporate Information Officer/Manager Target Date: 31/3/11

Management Response to Audit Report issued September 2010

Recommendation agreed. The Corporate Information Manager will prepare a report for the SIRO.

Update as at May 2011

The Council's ICT Strategy already acknowledges the need to implement corporate records management systems.

The Corporate Information Manager's report to the SIRO will need to address any records management issues that are identified as a result of the information risk assessment exercise that is currently underway and it will therefore be compiled after this exercise has been completed at the end of June 2011.

Matter Arising	**Recommendation**	**Responsible Officer / Target Date**

Although responsibility for the security and appropriate use of information assets is clearly set out throughout the Council's Financial Regulations, the general concept of 'Information Ownership' has not yet been embedded throughout the organisation.	The SIRO should write to all Chief Officers to formally remind of their specific responsibilities in respect of information management and security and asking them to identify all of their information systems and pass these details on to the Corporate Information Officer, together with the name of the 'Owner' of each of them.	Corporate Information Officer/Manager Target Date: 1/12/10

Management Response to Audit Report issued September 2010
Recommendation agreed. The Corporate Information Officer/Manager will draft the communication on behalf of the SIRO.

Update as at May 2011
The SIRO has written to all CMT members reminding them that "All Directors are responsible for information as a Council asset" and a briefing session has also been arranged, for Councillors and senior officers, to raise their awareness of the security risks that the Council faces today. Work is underway to identify all of the Council's information systems and to assign an 'owner' to each of them. This is a lengthy task and it is anticipated that further significant progress will continue to be made throughout the current financial year.

Matter Arising	**Recommendation**	**Responsible Officer / Target Date**

Section D.1.20 of Financial Regulations sets out the responsibility of Chief Officers "To ensure that, where appropriate, computer based and other operational systems containing relevant information are registered in accordance with the Data Protection and related legislation, and that staff are aware of their responsibilities under the legislation." However, there is no formal process in place to enable them to do this and this exposes the Council to the risk of 'Failure to comply with statutory requirements'. (See Item R46 on the Strategic Risk Register)	The SIRO should initiate the introduction of a formal Data Protection Act registration system, throughout the organisation, by asking the Corporate Information Manager to prepare an appropriate procedure document, together with proposed timescales for its implementation.	Corporate Information Manager Target Date: Ongoing. (It will not be possible to implement an effective system until an initial information audit has been completed.)

Management Response to Audit Report issued September 2010
Recommendation agreed. However, this recommendation cannot be implemented until an Information Management Steering Group has been established and a full information audit has been carried out. It will then be possible to collate and maintain the data protection registration details from the initial information audit and any subsequent changes to it.

Update as at May 2011
The Information Management Steering Group is being established and work will then begin on an information audit and the implementation of a formal Data Protection Act registration system.