Date: 31st March 2010 REF:H/CICT/1/2010

Information and Data Security Management

EXECUTIVE SUMMARY

Context

The loss of confidential information is a growing business risk for organisations. Recent publicity regarding breaches in the Public Sector, and in particular, the security of information being transferred between locations and organisations, has underlined the importance of robust information governance within the Public Sector. Data loss incidents are increasing in number and significance every year. Such leakages are not only costly but also damaging to corporate reputations.

The requirements of ISO IEC 27001:2005, the current standard for information security management present a number of information security challenges to the Council. The Consortium carried out an audit of information security policies in April 2009 and our review did not duplicate any of the areas covered.

The Payment Card Industry Data Security Standard (PCI DSS) must be met by all organisations that transmit, process, or store payment card data. The Council accepts on line and telephone payments from its customers and is therefore required to demonstrate compliance with the requirements of PCI DSS. A high-level review of compliance with PCI DSS was included in the scope of our review.

Overview

The Council has some awareness of current information and data security issues and risks. It has an IT Security Policy and Internet Usage Policy, which have been communicated to computer users using the corporate Intranet. The Council includes information relating to information security in its new starter induction process.

The Council has formal processes for the management of users of its key systems. We understand that some information security training is given to appropriate staff. We were also pleased to note that during 2009, the Council requested a 3rd party information security company, NTA Monitor, to carry out testing of its firewall configurations and other areas of the IT infrastructure to determine its overall compliance with the requirements of the Government Code of Connection (GCSx) as well as PCI DSS.

However

The work carried out by NTA Monitor identified that the Council had a number of vulnerabilities in the configuration of its firewalls and that it was not fully compliant with the requirements of GCSx and PCI DSS. At the time of our review, the ICT Manager informed us that all actions required to address the identified weaknesses had yet to be fully completed.

Our review highlighted that the Council has no approved policy for undertaking network infrastructure penetration testing or for carrying out security vulnerability assessments. This would outline the Councils approach to maintaining a secure and reliable infrastructure. Furthermore, the Councils' IT Security Policy should be updated to include information on PCI DSS as well as referring to ISO / IEC 27001:2005, the latest standard for information

security management. It also has no senior officer with formal responsibilities for information security.

Our review did not include detailed testing of the controls over the use of removable media devices; therefore, we are unable to provide an assurance over the effectiveness of current controls.

These issues are addressed through the recommendations in the report. As a result of these findings, the overall assurance rating is given below.

As only minor risks have been identified and some recommendations made, the assurance rating following this audit is

MARGINAL

Scope

The audit included an examination of the following:

- the extent of corporate policies and guidance on data security and how these are communicated;
- awareness of ISO IEC 27001:2005 and a high level review of compliance with the requirements of the standard. However our work will not constitute a formal assessment of the Council's compliance with the standard;
- whether the Council has appropriately updated security procedures and policies in response to the GCSx Code of Connection requirements. In doing so, we will consider any other related audits in this area;
- steps taken to comply with the requirements of PCI DSS in respect of debit and credit card transaction processing systems;
- use of portable media for data storage; and
- the adequacy of security monitoring processes.

The recommendations are listed on the action plan, followed by the detailed report.

Acknowledgements

The help and co-operation of the Head of Change Management and Support Services, the ICT Manager and other IT staff was much appreciated by the following KPMG IT Advisory staff:

Malcolm Harding, IT Advisory Manager
Wasim Akbar, IT Advisory Analyst

ACTION PLAN

RECOMMENDATION	Section number	Priority	Officer Responsible	Agreed Action and completion date
The Council should formally assign a senior officer with overall responsibility for information security and record the responsibilities in a job description.	1.a	Medium	ICT Manager	Job descriptions will be reviewed and an appropriate officer will be designated responsible. 31st July 2010
The Council should update its IT Security Policy to refer to ISO IEC 27001:2005 information security standard and also include high level information on the requirements of PCI DSS.	1.b	Medium	ICT Manager	The Council has no plans to implement the 27001 standard. Clarification of the most important sections of the standard to include in policies is needed. Once these are received they will be incorporate in the appropriate IT Security Policy (User or Technical) **KPMG Update** This information has now been provided 31st July 2010
The Council should ensure it has a Service Level Agreement with Alliance & Leicester in place as soon as possible. As part of this agreement, the Council should contact them and obtain assurances on the security measures in place to safeguard the personal data of its customers who make on-line payments.	3.a	High	ICT Manager and Head of Finance	The Bill Pay Project is being replaced with a new software solution. 31st July 2010
The Council should ensure that all actual and potential weaknesses identified in the Code of Connection compliance scan are actioned as soon as possible.	3.b	High	ICT Manager	All high priority weaknesses have been addressed and lower risk issues have been considered and addressed as appropriate.

The Council should provide PCI DSS awareness training to appropriate staff.	3.c	High	ICT Manager and Head of Finance	On receipt of PCI DSS guidance from KPMG, training for appropriate officers will be arranged. **KPMG Update** This information has now been provided 31st July 2010
IT Services staff should ensure that an approved policy for network infrastructure penetration testing and for carrying out security vulnerability assessments is fully documented as soon as possible.	5.a	Medium	ICT Manager	Guidance received will be incorporated into the IT Team's operational patching policy. 31st July 2010