Audit Summary Report

26/06/2007

IT Risk Assessment

Lancaster City Council

Audit 2007/2008

External audit is an essential element in the process of accountability for public money and makes an important contribution to the stewardship of public resources and the corporate governance of public services.

Audit in the public sector is underpinned by three fundamental principles:

- auditors are appointed independently from the bodies being audited;
- the scope of auditors' work is extended to cover not only the audit of financial statements but also value for money and the conduct of public business; and
- auditors may report aspects of their work widely to the public and other key stakeholders.

The duties and powers of auditors appointed by the Audit Commission are set out in the Audit Commission Act 1998 and the Local Government Act 1999 and the Commission's statutory Code of Audit Practice. Under the Code of Audit Practice, appointed auditors are also required to comply with the current professional standards issued by the independent Auditing Practices Board.

Appointed auditors act quite separately from the Commission and in meeting their statutory responsibilities are required to exercise their professional judgement independently of both the Commission and the audited body.

Status of our reports

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any member or officer in their individual capacity; or
- any third party.

Copies of this report

If you require further copies of this report, or a copy in large print, in Braille, on tape, or in a language other than English, please call 0845 056 0566.

.

For further information on the work of the Commission please contact:
Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ
Tel: 020 7828 1212 Fax: 020 7976 6187 Textphone (minicom): 020 7630 0421
www.audit-commission.gov.uk

Contents

Introduction

1 The Audit Commission is required to undertake work to ensure compliance with the International Standards for Auditing UK and Ireland (ISA+ or ISA (UK&I)). These standards require us to obtain an understanding of the organisation, including its internal controls, sufficient to identify and assess the risks of material misstatement of the financial statements whether due to fraud or error.

2 ISA (UK&I) 315 in particular requires us to gain an understanding of the IT environment and the impact this has on the information systems used for financial reporting. These include general controls over data centres, network operations, system software acquisition, change and maintenance, access security and application system acquisition, development and maintenance.

Background

3 The IT Risk Assessment (ITRA) is the methodology used to document our understanding of the IT environment at an organisation wide level. The primary objective of the assessment is to determine whether we can seek to rely upon the IT control environment and therefore gain assurance that the IT or automated controls will operate as intended for the period under audit.

Audit approach

4 An interview was held with the Head of IT and documents were reviewed.

Overall conclusion

5 Overall we can rely on the IT control environment but there are some areas of weakness and controls could be further improved by taking action on the recommendations in this report.

Main conclusions

Inaccurate data processing

6 All the major applications have test systems for the implementation and testing of upgrades and software patches. There is some guidance on the use of test and live systems, data validation, security controls and audit trails in the security policy. We did not look at the testing methodologies used by the system administrators of the application systems.

7 The Corporate Performance Officer is responsible for the Corporate Data Quality Policy which was approved in March 2007. Each service area takes responsibility for its own data and there is an Information Management Group which now includes the Corporate Performance Officer.

8 Each Service area has an 'Information Custodian' who has defined responsibilities including authorising changes to data. Work is currently in progress to include data quality and information management in the Information Custodians' job descriptions as part of a pay and grading review. The Information Custodian is also the System Administrator.

Unauthorised access

9 Access to the network requires a password which is a minimum of six characters. Enforced changes are in place for all users with the exception of remote users. Where enforcing the change is not in place, work is going on to address this. In all cases users are locked out of the system after three failed attempts.

10 New starters are not given access until a new starter form is received, signed by an appropriate manager. A Leavers' Report is received monthly from HR, and the leaver's login is disabled. The Helpdesk emails the line manager for instructions on how to deal with any data left by the leaver. The security policy states clearly that *'access rights must not be set up in advance of requirements and must be removed immediately for users who have changed jobs or left.'*

11 There is no written policy for controlling which IT staff have access to which systems and data and how they are supervised. No IT staff have logins to live application systems although they do have access to the data tables, but not to any DBA tools. The network and technical teams all have administrator access to servers, routers and other network equipment.

12 Lancashire County Council Internal Audit staff have carried out a BS7799 (ISO27001) gap analysis and this is currently being worked through by officers, although there is no intention to go for accreditation. There has also been an audit by the local police Crime Prevention Unit of building security which has identified some concerns.

Recommendation
R1 Consider the recommendations of the local police Crime Prevention Unit.

13 The firewall is maintained internally. Anti-virus and anti-spam software is in place, and there is network management software (Solar Winds). Suppliers access the network via a VPN and there is a procedure, included in the security policy for allowing and monitoring access.

Fraudulent or accidental manipulation of data

14 There is a documented change control procedure in place as part of the security policy. All system changes must be implemented under the formal documented IS Change Control Procedure. The impact on security of all changes to systems must be reviewed and a full risk assessment of the possible impact of changes must be carried out, and contingency plans drawn up, prior to implementation. Whenever system changes could have an effect on performance or capacity, an appropriate review of system specification must be carried out prior to implementation.

15 The applications manager does not allow the use of database editors and believes any changes should be made through normal procedures. This is also written into the security policy. Information Custodians have to sign off any data changes which are made by supplies outside the normal application processing.

16 Audit trails (event logs) are active for system utilities and the operating systems. These logs are allocated a certain amount of space and are circular which means that historic data is not available. There is a separate log for each application and this would be under the control of the appropriate service. It is not known if these are monitored by management and there is no known retention policy.

Recommendation
R2 Develop a retention policy for audit trails, and procedures for monitoring by management.

Loss of data

17 The Veritas backup system is used to take nightly incremental backups and weekly full backups. Tapes are held off site a quarter of a mile away with the disaster recovery box. This is less than the recommended distance and will be considered as part of the Business Continuity Plan which is currently under development as part of the Civil Contingencies work.

18 There is a Disaster Recovery contract which is tested at least annually with different applications. Lessons learned and follow up actions are carried out after each test.

Management

19 There are 21 staff looking after 50 servers and 550 PCs. There has been little staff turnover in the last 12 months. All staff have had IT Infrastructure Library (ITIL) overviews, some have had foundation training and some have completed the Managers Course. The IT Service is working towards BS15000.

20 There is an appraisal process and a training plan. On the technical side training takes place in Microsoft Certification, ITIL and CCNA. The training budget for 21 staff is £3,000 which would appear inadequate and may mean that staff are performing functions for which they are not adequately trained, increasing the possibility of error. Some training is provided as part of the installation of new systems.

Recommendation
R3 Review the adequacy of the IT training budget.

21 Developers do have access to the live environment but all access has to be recorded. There is segregation of duties for IT Staff and users and this is documented in the Security Policy, the operational and development functions within IT are completely separate.

22 IT purchases are from GCAT or other framework agreements. Changes to operating systems and networks are made using the change control procedure.

23 The T-Government Cabinet Liaison Group is responsible for overseeing acquisitions and users are the drivers in relation to software selection. There is currently no corporate guidance on the purchase of software applications.

Recommendation
R4 Develop corporate guidance for users on the purchase of software applications.

24 Implementation is on a project basis and Lancaster has adopted its own version of Prince, the '*Lancaster Approach to Managing Projects (LAMP)*' and this is used for all projects. Internal Audit has been involved in the development.

Appendix 1 – Action Plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
5	R1 Consider the recommendations of the local police crime prevention unit.	3	Transformation Manager	Yes	Some of the work will be incorporated into changes due to building work for air conditioning changes. If further expenditure needed a growth bid will be prepared for Star Chamber.	March 08
6	R2 Develop a retention policy for audit trails, and procedures for monitoring by management.	2	Technical Support Manager	Partial	Modern operating system tend to have space limits on audit trails rather than days - more space could be allocated but there would be a costs and retention for a the recommended seven years (ISA 315) will be as backups. Once policy agreed the changes can be made as systems are reviewed.	March 08
6	R3 Review the adequacy of the IT training budget.	3	Head of ICS	Yes	IT training budget for 2007/08 allocated already. A growth bid will be prepared for Star Chamber.	March 08
7	R4 Develop corporate guidance for users on the purchase of software applications.	3	Procurement Officer	Yes	Would appreciate guidance from Audit on their recommendations for guidance in this area and examples of good practise from elsewhere.	December 07