Audit Summary Report

December 2007

Computer Room Installation Controls Review

Sedgefield Borough Council

Audit 2006/07

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.
- 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, 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 to the council

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 non-executive directors/members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any director/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 0844 798 7070.

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 As part of our annual risk assessment process associated with planning the 2006/07 audit at Sedgefield Borough Council, we have completed a review of the computer room installation controls. The review has been carried out due to the recent upgrading of the computer room infrastructure and to aid our understanding of the Information and Communications Technology (ICT) environment which is required to comply with the International Standards of Auditing.

2 The use of robust IT systems and a controlled IT environment impacts how well an organisation monitors both its financial position and produces its annual financial statements. The Audit Commission considers whether the council has responded adequately to the risks arising from IT by establishing effective general IT and applications controls on material business systems. Controls over IT systems are deemed to be effective when they maintain the integrity of the information and the security of the data such systems process.

3 General IT controls include policies and procedures that relate to many of the key business systems as well as the environment to support their effective functioning. This brief review includes an assessment of the controls in the following areas:

- physical security arrangements;
- environmental controls to support operation of systems;
- disaster recovery; and
- logical access controls (key business systems and corporate network facilities).

Main conclusions

4 The Council provides and manages all of its key business systems in-house. The main physical access and environmental controls are adequate and operating in a satisfactory manner with some minor areas identified for improvement. One of the indicators for a well managed ICT service is the availability of policies and procedures. The ICT department has on-line operational procedures in place but it is weak in the availability of council wide IT usage related policies, for example, an ICT security policy.

5 Logical access controls to the corporate network and some of the key business systems in the main are good and follow best practice suggested in BS17799 (now ISO27001:2) guidance. The only exception is the commonly set parameter for 90 day frequency between password changes which is longer than best practice recommends.

6 The Council is one of very few that has developed an in-house disaster recovery off-site facility for its key business systems. Updated insurance cover for IT equipment/inventory is in progress/complete and there is no history of theft, computer virus attacks or breaches of network security.

7 During 2006/07 Internal Audit reviewed ICT security. We have assessed their findings and our work concurs with some of their reported results. We have therefore not included any recommendations already suggested. Overall, there are no significant threats or concerns to the data processing activities operated by the Council.

Key issues

General environmental controls

8 The general environmental controls covers the following areas:

- physical access;
- air conditioning;
- fire and smoke mechanisms; and
- backup power supply.

Physical access

9 The computer room is located on the ground floor of the main council offices building at Green Lane; adequately remote from public access areas. All business systems servers are centralised in this location which also houses the council's reprographic/print service.

10 Entry to the computer room is through the use of an electronic key fob (a type of security token usually a small hardware device with a built-in authentication mechanism) which automatically opens/closes the computer room door when in close proximity to the sensors. The key fobs are issued on a restricted basis to most ICT staff in the three main service areas (Infrastructure, Development and Customer Support).

11 The physical entry controls are satisfactory, however, only the Infrastructure team has a strong operational need to warrant their presence in the computer room. We note that the standard protocol is to ensure council staff and visitors are not left unsupervised in the computer room. The only minor weakness identified is the absence of an internally maintained log book to formally record visits, for example, service engineers, auditors.

12 An inspection of the computer room focusing on the security features confirmed that the passive infra-red motion detector assumed to be linked to the alarm system was not visible. It was later found to have been placed above the suspended ceiling in a position where it could not perform its security function.

13 The windows of the computer room have internal bars fitted and on initial inspection they seemed to be more of a deterrent feature than an effective barrier to forced entry. A polarised reflective/mirror film has been applied to the windows to aid in preventing IT equipment inside being easily viewed but this feature is not effective close up.

Air conditioning

14 The air conditioning system is regularly maintained and seen to be operating effectively. There is no health and safety issue over noise as Infrastructure team staff normally sits in an adjoining office limiting their exposure to potentially high noise levels.

15 All previous heating pipes have been disconnected. There are no water or moisture detectors in the computer room but no history of any water related damage. There are some plans to install shower facilities near the computer room and the Council has carried out a risk assessment to determine and manage the installation. We have no additional concerns.

Fire and smoke mechanisms

16 The computer room has a fully maintained non-halon fire suppressant and smoke alarm system. The room is not used as an additional storage location for paper or other IT related consumables. A large storage bin is available to collect any waste material for disposal and there is no evidence of any combustible or hazardous materials. The arrangements in place are satisfactory.

Backup power supply

17 The computer room has recently been re-furbished in part to accommodate a larger new uninterruptible backup power supply which can provide sufficient power to enable a controlled closedown of systems and prevent corruption/damage to data in the event of an outage action. We have no concerns about the backup power supply arrangements.

Recommendations	
R1	*Implement a manual internal log book system to maintain a record of all external visitors to the computer room.*
R2	*Restrict automatic access to the computer room to staff who need to work in it, for example, Infrastructure Team staff who manage the servers and communications equipment.*
R3	*Ensure that the passive infra-red and security alarm system is tested and re-assess the adequacy of the present physical control arrangements to prevent a forced entry to the computer room.*

Data backup and disaster recovery arrangements

18 The data backup backups for all key departmental systems are taken on at least a daily basis and are subject to periodic testing with additional copies stored securely both on and off-site.

19 The Council is one of the very few that has in place a dedicated backup data processing setup providing a good degree of disaster recovery resilience. The backup site is located in one of the rooms on the ground floor of the Central Depot a few miles away. The room is not identified as such, locked (keys retained by ICT staff) with adequate environmental and backup power arrangements. We have no immediate concerns about the Council's disaster recovery arrangements. Corporate business continuity arrangements are the responsibility of each department and these have not been covered in the scope of this review.

20 We note there are no procedures to ensure that data on failed server hard disks has been rendered inaccessible. In the event of a hard disk failing, the failed disk is returned to the supplier for a replacement. Our concern is that suppliers often analyse failed disks to determine reasons for failure. To aid them in this task they use sophisticated tools, which in some instances can recover significant amounts of stored confidential data. Failure to protect data adequately could result in the Council not be meeting its obligations under the Data Protection Act.

Recommendation	
R4	*Ensure that any failed hard disks returned to suppliers are magnetically wiped clean or seek suitable assurance from suppliers that confidential data will not be accessed/wiped clean by them.*

Logical access controls

21 Strong logical access controls provide a mechanism to restrict access to key business systems to authorised staff only. We have reviewed the adequacy of logical access controls through the completion of a self assessment questionnaire sent to system administrators managing the corporate network and departmental systems (Resourcelink - payroll, Agresso main accounting and Northgate SX3: Revenues and Benefits).

Network access controls

22 The procedures for setting up starters/leavers to the corporate network including are satisfactory and meet best practice guidelines. There are only two logical access parameters where there is scope for improvement:

- password change frequency at 90 days is too long; and
- password reuse to prevent re-use of old passwords at only two is low.

We have no significant concerns over the network backup arrangements and general operational management.

Agresso main accounting system

23 The logical access settings for the main accounting system are satisfactory and there are no significant concerns.

Northgate SX3: Revenues and Benefits

24 Overall, the logical access controls are adequate but there is some scope for improvement in the following areas:

- password change frequency at 90 days is too long.

Resourcelink - Payroll

25 The logical access controls for the payroll system are overall quite strong with the following exception:

- password change frequency at 90 days is too long.

Recommendation	
R5	*Password controls should ensure that all passwords are a minimum of seven characters, prevent re-use of the last 10 passwords and enforce changes every 30 to 60 days. Complexity rules for passwords should be activated where this feature is available, for example, capital and numeric characters are included.*

Appendix 1 – Action plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Comments	Date
6	R1 Implement a manual internal log book system to maintain a record of all external visitors to the computer room.	2	Head of ICT	Agreed	Complete
6	R2 Restrict automatic access to the computer room to staff who need to work in it, for example, Infrastructure Team staff who manage the servers and communications equipment.	2	Head of ICT	We have considered this and feel that it may cause problems. The two large Xerox printers are in the computer room and staff can ask for items from these outside of 'normal office hours'. In these instances it is normally 'an emergency' and it would not be appropriate to reduce the level of service so that only some members of the IT Section could deal with this type of request. Therefore we have decided that it is better for the help desk and development teams to have access to the computer room. The server and network cabinets are locked so only the infrastructure team have access to these. However, we will keep the situation under review.	Ongoing.
6	R3 Ensure that the passive infra-red and security alarm system is tested and re-assess the adequacy of the present physical control arrangements to prevent a forced entry to the computer room.	3	Head of ICT	As there has been some major work undertaken on the air conditioning units over the last few months the location of the passive infra-red alarms could not be changed until the work was completed. Now that the work has been finished, this is currently being looked into.	Ongoing.
7	R4 Ensure that any failed hard disks returned to suppliers are magnetically wiped clean or seek suitable assurance from suppliers that confidential data will not be accessed/ wiped clean by them.	2	Head of ICT	Assurances have been obtained from the suppliers that they erase disks returned to them. However, we will look into the costs/benefits of obtaining a disk eraser.	Ongoing.

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Comments	Date
8	R5 Password controls should ensure that all passwords are a minimum of seven characters, prevent re-use of the last 10 passwords and enforce changes every 30 to 60 days. Complexity rules for passwords should be activated where this feature is available, for example, capital and numeric characters are included.	2	Head of ICT	We have reviewed this and consider our existing policy to be adequate. It has been proved that changing complex passwords too frequently can result in users being more likely to write them down. Therefore there is a balance to be drawn between the complexity of the passwords (which in our case our network password complexity is high) against the frequency of it changing. We will however, continue to monitor this.	Ongoing