| | AUDIT AND ACCOUNTS COMMITTEE 25 MARCH 2010 | **ITEM 16** |
|---|---|---|
| DERBY CITY COUNCIL | Report of the Head of Audit and Risk Management | |

---

**MANAGER RESPONSES - NON IMPLEMENTATION OF RECOMMENDATIONS**

---

**RECOMMENDATION**

1.1     To note the current situation with regard to those Internal Audit recommendations reported to the December 2009 meeting as not implemented.

**SUPPORTING INFORMATION**

2.1     At the meeting on 3 December 2009, members requested that explanations were sought from the Manager responsible for the non-implementation of 2 internal audit recommendations made in respect of leisure centres.

2.2.    Following the meeting, further clarification was sought from the Chair of the Committee in respect of what would need to be recorded for each case of non-implementation of recommendation s highlighted to Committee. The view of the Chair was where Members felt that the issue of non-implementation of an audit recommendation needed to be pursued, then Committee would ask the manager responsible for a written response. If this response was not forthcoming then the manager would be asked to attend the next meeting of this Committee to provide an explanation for the non-implementation.

2.3     The Head of Audit and Risk Management has reviewed those internal audit recommendations that were categorised as "Not Implemented" in the December 2009 report and has sought written explanations from 2 Managers on their decisions to not implement internal audit recommendations.

2.4     The status on the 2 recommendations for the leisure centres that had not been implemented has now changed. The recommendation regarding the alarming of the "jumbo" doors at Moorways Leisure Centre has now been implemented. The recommendation in respect of the introduction of a key lock for the safe at Springwood Leisure Centre will be implemented in the next 4 weeks. Internal Audit will follow this up in April 2010. The response from the Manager is attached at Appendix 2.

2.5     The status of the implementation on the signing and dating of creditor and debtor control account reconciliations has now changed. Internal Audit agrees that the recommendation has been superseded by the implementation of actions to satisfy a

recommendation made in another audit report (see Appendix 3). In respect of the recommendation on sharing the username 'sysadmin', Internal Audit has discussed this with the Head of Business Systems and the solution being proposed on the use of individual log ins (see Appendix 3) is acceptable.

| | |
|---|---|
| **For more information contact:** | Richard Boneham, Head of Audit and Risk Management, 01332 255688 richard.boneham@derby.gov.uk |
| **Background papers:** | |
| **List of appendices:** | Appendix 1 – Implications |
| | Appendix 2 – Update from Principal Sports Centre Manager |
| | Appendix 3 – Update from Head of Business Systems |

| IMPLICATIONS |
|---|

**Financial**

1.      None directly arising

**Legal**

2.      None directly arising

**Personnel**

3.      None directly arising

**Equalities impact**

4.      None directly arising.

**Corporate objectives and priorities for change**

5.      The functions of the Committee have been established to support delivery of corporate objectives by enhancing scrutiny of various aspects of the Council's controls and governance arrangements.

**Extract from Audit Report – Moorways Sports Centre Security – Issued July 2006**

3.1.5  We expected that intruder alarms would be fitted throughout the Sports Centre, which were regularly tested and maintained in accordance with the manufacturer's guidelines.

From our inspection of the Sports Centre, we established that all appropriate areas were connected to the alarm system. When external doors (other than the main entrance) are opened, during opening hours, the alarm system alerts reception.

However, the double doors in the sports hall and the two fire doors in the bar were not connected to this system. There was an official register of testing confirming the date, key holder, ADT Technician name and brief details of inspection.

If all external doors are not connected to the alarm system, there is a risk that unauthorised access could be gained or equipment could be carried out without staff being alerted.

**Recommendation**

**Rating: Merits Attention.**

Not all external doors were connected to the alarm system, and therefore did not alert reception when opened.

We recommend that the double doors in the sports hall and the two fire doors in the bar, be connected to the system which alerts reception when security doors are opened during opening hours.

**Response from Wayne Sills, Principal Sports Centre Manager.**

Issue Accepted

Action Details: Quotes will be obtained to connect all external doors to the alarm system. We will then see how this work can be funded.

Responsible Officer: Assistant Manager - Quality Control

Action Date: End July 2006

**Update Position from Wayne Sills, Principal Sports Centre Manager.**

**Not Implemented**

Nov 09 - Funding used for another project. Quotes have been obtained for this work and funding obtained from Community Safety Engagement Partnership. However, this funding was then withdrawn. From some reserve funding Sports Centre Management has £10,000 has been allocated to Moorways to address some of its security issues. A list of priorities is being drawn up by Centre Management.

**Response from Wayne Sills, Principal Sports Centre Manager – March 2010**

The double 'jumbo' doors in the main sports hall and the doors in the Bar are now alarmed.

**Extract from Audit Report – Springwood Leisure Centre: Security – Issued May 2006**

3.3.1   We expected that responsibility for the contents of the Centre's safe would be clearly attributable to one officer at any point in time.

The Duty Manager is responsible for the Centre's safe during their shifts. It is the working practice that during their shift, the Duty Manager should be the only person that accesses the safe, even if the Centre Manager is also on duty.

However, access to the safe cannot be physically restricted to one officer, as the safe is accessed via a numbered keypad and it does not require a key to gain access. The access code number is changed every few months, but is known by the Centre Manager and each Duty Manager. Accordingly, when more than one officer (who knows the access code number) is on site, then effectively neither officer can be held responsible for any discrepancies that may occur with the safe's contents. There is always the risk of unauthorised persons becoming aware of an access code without management's knowledge, whereas access via keys can be controlled and each key can be clearly accounted for.

Records are maintained of deposits in, and withdrawals from, the safe, but the transfer of the responsibility for the contents of the safe is not formally recorded at the end of each Duty Manager's shift. Content records are of little use if responsibility cannot be formally demonstrated.

When access cannot be appropriately restricted and responsibility for discrepancies cannot be determined, there is an increased risk of fraud, theft or the misappropriation of funds.

**Recommendation**

**Rating: Significant.**

Access to the Centre's safe is via an access code number, rather than a key. Accordingly, access to the safe cannot be appropriately restricted to one responsible officer at any one time.

We recommend that the safe is replaced with one which is accessed with a key. The number of keys in general circulation should be strictly restricted to a working minimum. The transfer of safe keys between officers should be formally recorded. Safe keys should be carried on the person of the responsible officer(s) at all times.

**Response from Wayne Sills, Principal Sports Centre Manager.**

Issue Accepted

Action Details: The Centre Manager will obtain a cost to have a key lock installed for the safe.  Once a cost is obtained then this will be looked at in more detail. However, we propose not to change the current system at present as there are concerns regarding the use of a key and cost.  It will mean additional secure key safe will be required on site to have the key locked in over night.  As the safe and the key safe would be within very close proximity to each other for operation reasons and that this would be on ground level, the risk could be greater than at present.

Responsible Officer: Manager - Springwood Leisure Centre

Action Date: 31 August 2006

**Update Position from Wayne Sills, Principal Sports Centre Manager.**

**Not Implemented**

Cost to have the safe changed over to a key system is £300. The Centre does not have any unallocated budget to do this work. The Safe is now operated by a PIN code which is changed every six months. Only designated staff have the number.

**Response from Wayne Sills, Principal Sports Centre Manager – March 2010**

I have spoken with John Brown, Head of Sport and Leisure regarding this recommendation.

The recommendation is to change the Springwood Leisure Centre safe 'combination' lock to a key for the safe.

In the latest Audit Report – Leisure Centre Income, audit have raised concerns over the current safe key system in operation at other sports centres.

I met with auditor Marcus Cale, 3 March to discuss this and we have come up with a system that will now satisfy audit and is practical to operate.

The combination lock at Springwood Leisure Centre is being changed to a key lock system. This will be completed within the next four weeks.

**Extract from Audit Report – Financial Systems: Control Accounts issued April 2006**

3.1.2 We expected that creditors and debtors control account reconciliations would be signed and dated in order to identify the officer responsible for their completion and to demonstrate that the reconciliations were completed in a timely manner.

Creditors control account reconciliations are completed on a quarterly basis. We checked the 3 quarterly creditors control account reconciliations completed in the 2005/06 financial year and found that only the second quarter's reconciliation had been signed by the Financial Systems Manager upon completion, and none had been dated.

Debtors control account reconciliations are completed monthly. We checked the 10 monthly control account reconciliations completed in the 2005/06 financial year and found that all had been signed by the Financial Systems Manager upon completion, but only 1 had been dated.

In the absence of the signature of the responsible officer and the date of completion recorded on the reconciliation documentation, the timeliness of completion and the appropriateness of the officer performing the reconciliation cannot be determined.

There is a risk that the responsible officer may not be appropriate or identifiable should the reconciliations come under scrutiny in the future. Reconciliations may not be performed in a timely manner and discrepancies may therefore not be identified, investigated and resolved promptly, increasing the risk of misstatements in the Council's Statement of Accounts.

**Recommendation**

**Merits Attention**

Creditors and debtors control account reconciliations are not always signed and dated.

We recommend that all control account reconciliations are signed and dated upon completion by the responsible officer.

**Response from Lynda Innocent, Head of Business Systems**

Issue Accepted

Action Details: These will be reviewed monthly to ensure they have been signed.

Responsible Officer: Wendy Hooley, Business Systems Manager - Oracle

Action Date: End May 2006

**Update Position from Lynda Innocent, Head of Business Systems (November 2009)**

**Not Implemented**

These are electronically held, therefore it is not practicable to sign these documents. The important issue is that these are properly reconciled and reconciling items are addressed.

*Lynda Innocent's Response on 26/02/10*

I believe this recommendation has been superseded by the recommendation that was made in the Final Creditors Report v1.0 issues on September 2008 which I reproduce below:

Merits Attention

"The Council cannot appropriately evidence that the necessary checks which ensure that reconciliations, between the Accounts Payable and the General Ledger modules of Oracle, have been properly conducted in a timely manner, have been undertaken.

We recommend that until a suitable electronic solution can be found that addresses all the control and evidential requirements of a reconciliation document, hard-copies of the reconciliations between Accounts Payable and the General Ledger should be produced and retained, (signed and dated by the reconciling officer) and these hard-copy reconciliations should in turn be passed to the Group Accountant – Corporate Team for him to check, then counter-sign and date."

Our response to this was as follows:

"The Business Systems Team is going to be trained in the use of "Sharepoint" which will then be used to version control the reconciliations."

This has been implemented and has been in place since at least April 2009.

**Extract from Audit Report – Main Accounting System 2007-8 issued September 2008**

3.1.5  It was noted during the audit and confirmed by the Head of Business Systems that herself, the Financial Systems Manager and Systems Accountant, Business Systems were all sharing the username 'sysadmin' in Oracle for posting feeder systems. This made it impossible to determine who actually posted each systems feed.

Where it is not possible to identify which of the three officers have posted which of the feeder systems, an effective audit trail is not being maintained the integrity of potential evidence is lost.

## Recommendation

**Merits Attention**

The Head of Business Systems, Financial Systems Manager and Systems Accountant, Business Systems Team were all sharing the username 'sysadmin' in Oracle for posting feeder systems.

We recommend that the responsibility (GL Superuser) that allows these officers to post feeder systems under the user name 'sysadmin' be assigned to individual users instead of via a generic administration account.

**Response from Lynda Innocent, Head of Business Systems**

Issue Accepted

Action Details: We will investigate this possibility but there are potential problems with systems administration if we are unable to use the sysadmin account.

Responsible Officer: Financial Systems Manager

Action Date: End October 2008

**Update Position from Lynda Innocent, Head of Business Systems (November 2009)**

**Not Implemented**

We require full access to enable us to undertake our duties for example reviewing the status of concurrent requests and resolving workflow issues.

*Lynda Innocent's Response on 26/02/10*

In order for the 2 Business Systems Managers and me to undertake our duties effectively we need to be able to monitor all concurrent requests that are running on Oracle to allow us to identify any issues that need to be resolved and also correct any workflow errors that emerge. The only way for us to undertake these tasks is by logging into Oracle as Systems Administrator. We have explored alternatives to this but none of these are practical.

*Lynda Innocent's Response on 15/03/10*

We have discussed this again internally and the following will be implemented to safeguard the staff involved.

Sysadmin will continue to be used for rewinding workflow errors and monitoring activity on concurrent requests as there is no other way to undertake these tasks effectively as this is how the application is set up and cannot be changed.

All other changes to the database will be made using individual log ins ie the Business Systems Managers and Head of Service. Once the audit trail is up and running then colleagues in other teams will be in a position to monitor the accuracy of the changes we have made to the database.