Derby City Council

AUDIT AND ACCOUNTS COMMITTEE
12 December 2012

ITEM 10

Report of the Strategic Director of Resources

Implementation Of Internal Audit Recommendation

SUMMARY

1.1 This report provides Committee with further information on the progress on implementation of an internal audit recommendation regarding the Chipside system.

RECOMMENDATIONS

2.1 To note the report.

2.2 To request an update on progress at the March 2013 meeting of the Committee.

REASON FOR RECOMMENDATIONS

3.1 The Audit and Accounts Committee is responsible for providing assurance to the Council on the effectiveness of the governance arrangements, risk management framework and internal control environment.

SUPPORTING INFORMATION

4.1 At its meeting on 31 October 2012, Committee requested that further information was provided at the meeting on 12 December 2012 on the progress that is being made with the implementation of the recommendation to address the following control issue:

There was a weak password associated with the local administrative “Administrator” and “Capita” accounts. There were also issues with the local password and account management policy on the Server.

This control issue was given a “moderate risk” rating by the Auditor.

4.2 The audit recommended that management seeks to:

- Review the practicalities of strengthening the passwords associated with the Administrator and Capita accounts, and where practical set the password to a strong, non guessable value which should. Ideally, the password should be over 14 where LM hashes are being stored. Administrators should avoid including dictionary words in the password composition, such as password01, as these are common targets in dictionary attacks.
- Review the practicalities of ensuring that the passwords for Administrator and Capita expire after 90 days.
- Review all accounts on the Server to identify any stale user accounts. Stale accounts should then be disabled. If the accounts are deemed still necessary, conduct a review to the practicalities of whether any local accounts could be replaced with domain accounts, to ensure they are subject to domain group policies.
- Enforce a minimum password length for accounts on Dcc-chipside and ensure that either minimum password age, password history or both are increased to better secure accounts and to ensure that previous passwords can not easily be used.

4.3 The Parking Services Manager agreed to implement the recommendation and he logged a service request with Serco on 5 December 2011 to make the required changes to the Chipside server in line with the recommendation by internal audit. On 22 December 2011 Serco identified that the issues highlighted in the recommendation affected the majority of DCC Servers and stated that they would be looking into addressing the issue across all servers and not just the Chipside server. In March 2012 Serco provided a further response to the Parking Services Manager that stated that they were "investigating the security issue highlighted by the audit team on your Server but as mentioned this also affects all other Servers. Currently we are performing an investigation to look at the impact the changes require may have and how to administrate these changes."

4.4 On 20 June 2012, following agreement with both Internal Audit and the Parking Services Manager, this service request was closed by Serco. On the same day, Serco created a new service request to implement changes that would address the weakness highlighted by this recommendation across all DCC servers, including the Chipside Server.

4.5 Progress has been chased with Serco (via the Service Delivery Manager, the Infrastructure Team Leader and the Service Desk & Desktop Support Manager). As at 19 November 2012, Serco were able to confirm that this service request has been assigned to a Serco engineer and that it is in progress. There are currently about 366 servers that require the changes applying to them. The changes are currently a lower priority than the work Serco is doing for the Council around the infrastructure for the imminent return to the Council House.

OTHER OPTIONS CONSIDERED

5.1 None noted.

This report has been approved by the following officers:

Legal officer	N/A
Financial officer	N/A
Human Resources officer	N/A
Service Director(s)	N/A
Other(s)	Chief Officer Group

For more information contact:	Richard Boneham Head of Governance and Assurance, 01332 643280 richard.boneham@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 None directly arising.

Legal

2.1 None directly arising.

Personnel

3.1 None directly arising.

Equalities Impact

4.1 None directly arising.

Health and Safety

5.1 None directly arising.

Environmental Sustainability

6.1 None directly arising.

Asset Management

7.1 None directly arising.

Risk Management

8.1 Sound risk management practices are a key principle of good governance.

Corporate objectives and priorities for change

9.1 The governance framework includes arrangements to plan and monitor delivery of the Council’s priorities.