



**Manchester City Council**

**Audit 2007/08**

**Information systems controls review**

**15 October 2008**

## Executive summary

### Scope and purpose of the report

- 1.1 We carried out a review of the Council's information systems controls to support our audit of the 2007/08 accounts. This included general IT controls and SAP specific controls work.
- 1.2 This report summarises the principal matters arising from our review for those charged with governance. The issues raised have been discussed with the City Treasurer and other officers as appropriate.

### Key findings

- 1.3 Overall, we assessed the Council's IT control environment as sufficient to support our planned approach to the audit of the 2007/08 accounts.
- 1.4 However, in order to obtain this assurance, we performed some additional work with the Council to assess and quantify the potential impact of identified control issues and to identify compensating controls.
- 1.5 The areas where the Council needs to improve IT controls include:
  - implementing an IT disaster recovery plan and IT strategy
  - removing enhanced user accesses that are no longer required now that SAP has been implemented
  - strengthening controls and audit trails for setting up new SAP user accounts
  - ensuring more consistent application of change control processes for SAP and other systems.
- 1.6 We agreed a detailed report and action plan with management to address these issues. A summary of the action plan is included at Appendix A.

### Next steps

- 1.7 The Audit Committee should monitor implementation of the recommendations arising from this report.

### Acknowledgements

- 1.8 We would like to record our appreciation for the co-operation and assistance provided to us by the Council's officers during the course of this review.

**Grant Thornton UK LLP**  
**15 October 2008**

## Appendix A Summary of the action plan agreed with management

Recommendation	Management response	Implementation details
<p>We recommend establishing and formalising the business continuity and disaster recovery processes, detailing the critical systems that need to be recovered and defining how the recovery process should be actioned.</p> <p>The disaster recovery plan should be tested on a regular basis (minimum of once every 12 months) and clearly define what areas are to be given priority in the event of a disaster.</p>	<p>Objective 7 of the ICT Business Plan has the action to “Implement an ICT Business Continuity Plan”</p> <p>Consequently a great deal of work has been undertaken. The finalisation of the Disaster Recovery Plan is dependent on the documentation of processes necessary to bring each software application back on line. Lack of staff has prevented this work from being undertaken and will begin following the appointment of staff to the new organisational structure.</p> <p>In addition the statutory requirement of holding the data offsite is in place &amp; has been achieved by replicating the data to the BX45 computer suite at the Town Hall.</p>	<p>Head of ICT Service &amp; Unit Management Team</p> <p>September 2009</p>

Recommendation	Management response	Implementation details
<p>An ICT strategy document should be created. ICT should consider the wider requirements of the business, both operationally and strategically, and determine the steps required for ICT to fulfil these requirements in an efficient and coordinate manner.</p>	<p>Objective 6 of the ICT Business Plan has an action to develop and ICT Strategy. The work is being progressed the time target will be achieved.</p> <p>The ICT strategy will include the development of ICT governance across the organisation.</p>	<p>Head of ICT Service October 2008</p>
<p>As the SAP implementation is now complete, SAP standard profiles should be revoked.</p> <p>Appropriate roles should be developed for all users with the necessary (minimum) access that they require in order to perform their daily functions. Furthermore, access permissions should enforce an appropriate segregation of duties, in line with the organisation's requirements.</p> <p>If the business still believes that it is necessary to continue use of the SAP standard profiles, additional compensating controls (such as full session audit logging) should be implemented to ensure that risks associated with these users' activities can be managed.</p>	<p>All "SAP_ALL/NEW" profiles have been removed for the following accounts and other profiles updated to improve controls.</p>	<p>Applications Manager Completed</p>

Recommendation	Management response	Implementation details
<p>To ensure unauthorised changes cannot be made to the SAP software, SAP 'client and transport' settings should be configured to prevent direct changes being made (eg by developers).</p> <p>We found two SAP clients that were not appropriately configured. These clients should be re-configured to prevent direct changes being made.</p>	<p>Both 001 &amp; 066 clients have now been changed to the following:-</p> <p>Changes and Transports for Client-Specific Objects – No Changes allowed</p> <p>Cross-Client Object Changes – No changes to Repository and cross-client Customizing Objects</p> <p>The ICT Service is working closely with Internal Audit to improve and monitor client administration settings on an ongoing basis.</p>	<p>Applications Manager</p> <p>Completed</p> <p>Ongoing</p>

Recommendation	Management response	Implementation details
<p>The user management team should review the process for creating users. The revised process should ensure that all information that will assist with the overall management and validation of users is captured.</p> <p>A monitoring process should be developed to ensure that the agreed naming convention is adhered to.</p>	<p>There has been significant work undertaken by Internal Audit in this area and ICT Service is working closely with Internal Audit to ensure the controls in place for User Authorisation are strong.</p> <p>The recommendations fall with the responsibilities of the SAP Security Architect. There have been difficulties recruiting a suitable person. The post is currently out to advert.</p> <p>On appointment, undertaking the work to comply with the recommendations will be the post holders priority work.</p>	<p>Technology &amp; Infrastructure Manager &amp; Applications Manager</p> <p>May 2009</p>
<p>Change policies over SAP should be reviewed and strengthened. Different types of changes will vary the change procedures, however change control policies must be applied to all changes.</p> <p>Attention should be paid on the different types of change requests and how authorisation of the different changes must be recorded and stored.</p>	<p>The recommended actions are agreed and have now been implemented.</p>	<p>Applications Manager</p> <p>Completed</p>

Recommendation	Management response	Implementation details
<p>A formal system change policy should be created and applied to all changes in operating systems and databases.</p> <p>The policy should be based on a recognised good practice standard (such as ITIL) and should outline the life cycle that each change to the system must follow. This life cycle must incorporate scoping the changes objectives, documenting what changes have been made, appropriate authorisation, and testing. Each of these steps should be fully documented.</p>	<p>A change control process is now in place for file servers and patching is included in the process. Records are kept of all changes made to file servers.</p> <p>Control of the operating system is through the ICT Services' Change Control Process.</p> <p>A separate formal change control process is used for SAP databases. Proposed changes are submitted to the business and the Change Advisory Board.</p> <p>When staff have been appointed to the new organisational structure a review will be undertaken by the Technology and Infrastructure Manager to ensure that the processes, above, comply with good practice as set out in ITIL.</p>	<p>Technology &amp; Infrastructure Manager</p> <p>Completed</p> <p>April 2009</p>



# Grant Thornton

**[www.grant-thornton.co.uk](http://www.grant-thornton.co.uk)**

© 2008 Grant Thornton UK LLP. All rights reserved.

"Grant Thornton" means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton UK LLP is a member firm within Grant Thornton International Ltd ('Grant Thornton International'). Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered by the member firms independently.

This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication